

LUCCA DE PAULA FONSECA SILVA

CRIMES CIBERNÉTICOS:
OS DESAFIOS DA SEGURANÇA DIGITAL NO BRASIL

LUCCA DE PAULA FONSECA SILVA

CRIMES CIBERNÉTICOS:
OS DESAFIOS DA SEGURANÇA DIGITAL NO BRASIL

Trabalho de Conclusão de Curso apresentado à
Instituição Pitágoras como requisito parcial para a
obtenção do título de graduado em Sistemas de
Informação.

Orientador: Gryco Holanda

LUCCA DE PAULA FONSECA SILVA

CRIMES CIBERNÉTICOS:
OS DESAFIOS DA SEGURANÇA DIGITAL NO BRASIL

Trabalho de Conclusão de Curso apresentado à Pitágoras, como requisito parcial para a obtenção do título de graduado em Sistemas de Informação.

BANCA EXAMINADORA

Prof(a). Matheus Teixeira Rocha

Divinópolis, dia 06 de junho de 2022.

Dedico esse trabalho ao meu pai Rogério José da Silva, que sempre me inspirou a tentar seguir sempre em frente, por sempre estar meu lado em momentos difíceis me dando dicas de como posso ser melhor tentando melhorar sempre e almejar meus sonhos nessa nova conquista na etapa final da minha vida acadêmica.

AGRADECIMENTOS

Meus agradecimentos a todos meus familiares por sempre serem uma inspiração para que eu nunca desistisse dos meus sonhos.

Também agradeço muito aos meus professores que me acompanharam minha jornada acadêmica desde o início do curso, foram anos de uma experiência incrível onde pude conhecer muitas coisas que eu nunca imaginaria ter conhecido sobre o mundo, por terem sempre me guiado me ensinado como ser um bom profissional.

“Somente os que ousam errar muito podem realizar muito” – John F. Kennedy

SILVA, Lucca, Fonseca de Paula. **Crimes Cibernéticos**: Os desafios da Segurança Digital no Brasil. 2022. 36. Trabalho de Conclusão de Curso (Graduação em tecnologia da Informação) – Pitágoras, Divinópolis, 2022.

RESUMO

A praticidade e a conectividade, oferecidas pela internet, geraram uma série de benefícios à sociedade. Todavia, com a crescente adesão social à tecnologia, surgem novos meios que possibilitam a prática dos crimes cibernéticos. Nesse diapasão, o impacto do avanço tecnológico no ordenamento jurídico brasileiro faz repensar o papel do direito frente à ocorrência dos crimes virtuais ocorridos e os desafios jurídicos em face à tipificação do cibercrime. Nessa perspectiva a problemática desse estudo é: quais são os mecanismos mais utilizados pelos criminosos nos crimes cibernéticos e quais ferramentas podem ser usadas pelos usuários nas interfaces da internet para que garantam segurança de dados e privacidade? Logo, o objetivo geral é expor sobre os delitos cibernéticos e assim analisar o que a legislação pátria regula a respeito. Para alcançá-los, foram traçados os objetivos específicos que são: analisar a evolução tecnológica; discorrer sobre o conceito de delitos cibernéticos; evidenciar as classificações dos delitos cibernéticos cometidos por meio virtual e verificar, à luz do ordenamento jurídico brasileiro e quais ferramentas podem ser utilizadas para ajudar usuários a se protegerem na internet. O trabalho é resultado de uma pesquisa bibliográfica que adotou como procedimento a análise documental, pautada em leis, no sentido amplo, projetos de leis, bem como a revisão bibliográfica nas bases de dados *online*, com consulta a artigos científicos e doutrinas relacionadas à temática. Conclui-se que é necessário regulamentar leis específicas para o combate ao crime cibernético, bem como que haja investimentos de proteção na segurança das informações dos dados dos usuários.

Palavras-chave: Tecnologia. Cibercrime. Segurança de dados. Privacidade

SILVA, Lucca, Fonseca de Paula. CYBER CRIME: the challenges of digital security in brazil2022. 36. Trabalho de Conclusão de Curso (Graduação em tecnologia da Informação) – Pitágoras, Divinópolis, 2022

ABSTRACT

The practicality and connectivity offered by the internet have generated a series of benefits for society. However, with the growing social adhesion to technology, new means appear that enable the practice of cyber crimes. In this vein, the impact of technological advances in the Brazilian legal system makes us rethink the role of law in the face of the occurrence of virtual crimes that have occurred and the legal challenges facing the typification of cybercrime. In this perspective, the problem of this study is: what are the mechanisms most used by criminals in cyber crimes and what tools can be used by users in internet interfaces to ensure data security and privacy? Therefore, the general objective is to expose about cyber crimes and thus analyze what the national legislation regulates in this regard. In order to achieve them, specific objectives were outlined, which are: to analyze the technological evolution; discuss the concept of cyber crimes; highlight the classifications of cyber crimes committed through virtual means and verify, in the light of the Brazilian legal system and which tools can be used to help users protect themselves on the internet. The work is the result of a bibliographic research that adopted as a procedure document analysis, based on laws, in the broad sense, bills, as well as the bibliographic review in online databases, with consultation of scientific articles and doctrines related to the theme. It is concluded that it is necessary to regulate specific laws to combat cyber crime, as well as that there are protection investments in the security of user data information.

Keywords: Technology. cybercrime. Data security. Privacy

LISTA DE ILUSTRAÇÕES

Figura 1 – Crimes Cibernéticos	25
Figura 2 – Principais tipos de ataques por <i>malwares</i>	26

SUMÁRIO

1. INTRODUÇÃO	13
2. EVOLUÇÃO TECNOLÓGICA E O COMÉRCIO ELETRÔNICO NO BRASIL ERRO! INDICADOR NÃO DEFINIDO.4	
3. DELITOS COMETIDOS ATRAVÉS DA INTERNET	15
4. PROTEÇÃO DOS USUÁRIOS NA INTERNET	17
4.1 CRIMES CONTRA A PROPRIEDADE INTELECTUAL ERRO! INDICADOR NÃO DEFINIDO.0	
4.2 ESPIONAGEM ELETRÔNICA	29
4.3 FRAUDES VIRTUAIS.....	34
5. CONSIDERAÇÕES FINAIS.....	35
REFERÊNCIAS.....	36

1. INTRODUÇÃO

Quando a internet se popularizou para uso empresarial e doméstico, em meados da década de 1990, eram poucos os entusiastas que pensavam que ela atingiria os patamares que atingiu hoje na sociedade. Os grandes avanços da sociedade pós-revolução tecnológica acarretaram também na modernização das relações sociais, trazendo maior facilidade e instantaneidade na comunicação e integração. O presente trabalho pretende discutir e analisar algumas relevantes questões relativas à prática dos delitos cibernéticos e os desafios da segurança digital no Brasil.

Em razão da velocidade de transformação da sociedade e das relações interpessoais, com ênfase na sua liquidez, necessária a pesquisa sobre o tema, no intuito de aperfeiçoar o ordenamento jurídico, que, por sua vez, deve organizar e regulamentar o tema, buscando medidas que visam resguardar os direitos fundamentais no meio cibernético. Ademais, se justifica pela modernização dos meios de comunicação, os quais, além de vantagens, trazem maior facilidade no cometimento de delitos cibernéticos virtuais, que vão se aperfeiçoando e evoluindo com astúcia, ao passo que o Estado precisa estar em consonância no seu combate.

Nessa perspectiva a problemática desse estudo é: quais são os mecanismos mais utilizados pelos criminosos nos crimes cibernéticos e quais ferramentas podem ser usadas pelos usuários nas interfaces da internet para que garantam segurança de dados e privacidade?

Logo, o objetivo geral é expor sobre os delitos cibernéticos e assim analisar o que a legislação pátria regula a respeito. Para alcançá-los, foram traçados os objetivos específicos que são: analisar a evolução tecnológica; discorrer sobre o conceito de delitos cibernéticos; evidenciar as classificações dos delitos cibernéticos cometidos por meio virtual e verificar, à luz do ordenamento jurídico brasileiro e quais ferramentas podem ser utilizadas para ajudar usuários a se protegerem na internet.

O trabalho é resultado de uma pesquisa bibliográfica que adotou como procedimento a análise documental, pautada em leis, no sentido amplo, projetos de leis, bem como a revisão bibliográfica nas bases de dados *online*, com consulta a artigos científicos e doutrinas relacionadas à temática. Deste modo, a pesquisa versa

sobre segurança digital, direitos fundamentais e qual o impacto que eles tem sofrido a partir da evolução tecnológica no ordenamento jurídico brasileiro.

2. EVOLUÇÃO TECNOLÓGICA E O COMÉRCIO ELETRÔNICO NO BRASIL

Os avanços tecnológicos e descobertas fizeram com que as distâncias entre as pessoas e as informações, o lazer, os estudos, etc., pudessem ser reduzidas de uma maneira radical, fazendo com que as relações entre as pessoas passassem a ser feitas na maioria das vezes utilizando equipamentos eletrônicos ligados à *internet*. Até mesmo culturas diferentes passaram a se inserir em meio as pessoas e com isso pode interagir com outras culturas através da rede mundial de computadores (GRECO,2005).

O termo computador é definido como uma máquina que pode receber, armazenar e enviar dados e pode realizar sequências pré-programadas de operações aritméticas (como cálculos) e lógicas (como comparação) nesses dados para resolver problemas (BORRI,2021).

A história da tecnologia começou a ganhar forma com o primeiro computador digital eletrônico de grande escala: o ENIAC (*Electrical Numerical Integrator and Calculator*). O computador foi criado em fevereiro de 1946 pelos cientistas norte-americanos John Presper Eckert e John W. Mauchly, da *Electronic Control Company* (GRECO,2005).

Da sua origem até os dias atuais, o homem vem buscando desenvolver ferramentas para facilitar o seu cotidiano, conseqüentemente criou máquinas e junto a elas foi aprimorada a tecnologia, surgindo um novo ambiente no qual grande parte da população mundial moderna faz uso frequente, com o advento da *internet* e do computador, deu-se início ao acesso direto aos ambientes informáticos (GROSSI,2005).

Portanto, o mundo passou por muitas mudanças, entre as quais estão, sem dúvida, a Segunda Guerra Mundial e a Revolução Industrial, que mudaram notoriamente todo o mundo moderno e o modo de vida neste planeta. Isso fornece uma maior interação entre humanos e máquinas (PINHEIRO,2010). A data específica da criação do sistema de rede global (ou em termos populares da *internet*) não foi determinada, mas esse sistema nasceu em meados da década de 1980 (GRECO,2005).

Com as novas relações sociais que um mundo globalizado passou a surgir nesta era digital envolvendo várias culturas diferentes e o Direito deve se adequar à

nova realidade, devendo também caminhar junto com os avanços dessas tecnologias para que desta forma não deixe a sociedade digital e até mesmo a física à mercê da criminalidade (ROHRMANN,2005).

A *internet*, também conhecida como rede mundial de computadores, foi criada na época da guerra fria, possuía fins militares, assim como o computador, ou seja, utilizada como um meio alternativo de comunicação do exército norte-americano caso os meios de comunicação convencionais da época fossem destruídos em ataques promovidos pelos inimigos (CARVALHO,2020). Assim, foi criada a ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançadas), essa foi a primeira rede nacional de computadores , criada no ano de 1969 pelo departamento de defesa dos Estados Unidos da América com a incumbência de conectar os computadores dos centros de pesquisa, universidades e principalmente instituições militares americanas, fazendo assim com que se compartilhasse informações, pesquisas e estratégias militares o ano de 1972 o governo apresentou a *internet* a sociedade (GRECO,2000).

Borri (2021) comenta que esta era atual com que a evolução tecnológica ultrapasse os limites esperados , alcançando uma velocidade sem precedentes , fazendo com que a vida das pessoas tivesse seu cotidiano mudado seja nos campos da sociedade, seja nas formas de comunicação, tudo isto com intuito de tornar a vida das pessoas mais fácil, tanto na agilidade das comunicações , quanto na facilidade de realizar atividades diversas , sendo possível realizar compras de diversos gêneros , realizar transações bancárias , estudar, isto tudo sem ao menos se dirigir a outro local ou sair de casa, devido a praticidade estas ferramentas digitais apresentam ao ser humano imensas oportunidades .

Observa-se que houve uma evolução, muitas vezes considerada lenta, da *internet* no Brasil, na qual, em seu início a utilização da rede abrangia apenas instituições de pesquisa (CARVALHO,2020).

A origem do comércio eletrônico pode ser rastreada até a década de 1970, Mesmo antes do desenvolvimento da Internet, devido ao surgimento da transferência eletrônica de fundos (EFT) e do intercâmbio eletrônico de documentos (EDI), Isso permite que as transações financeiras e a troca de documentos entre a empresa e seus clientes sejam realizadas eletronicamente (RIBEIRO, 2019). Antes que a Internet fosse amplamente adotada e usada comercialmente, os sistemas de comércio

eletrônico baseados em EDI e EFT eram muito caros, principalmente por causa do alto custo das redes privadas. Portanto, sua aceitação se limita principalmente a empresas multinacionais, use sua força financeira para pressionar e persuadir (por meio de subsídios) fornecedores menores a implementar um sistema de EDI. Até então, temos o chamado pré-comércio eletrônico da Internet (MENDES,2018).

A ascensão do comércio eletrônico no começo da década 1990. Um dos pioneiros neste campo é a Amazon.com, e Sediada em Seattle, EUA. No Brasil, o as primeiras organizações que vendem produtos para sites são livrarias, começando suas atividades em 1995, desde então, o *e-commerce* chegou, expandiu e tornou-se cada vez mais popular internacional (OLIVEIRA, 2017). No Brasil, em 2018, seu faturamento foi de aproximadamente 53,2 bilhões de reais, 58 milhões de brasileiros. A previsão é que chegue a 85 bilhões de reais em 2021, o mercado apresentará crescimento constante digital. Mesmo em tempos de crise, o *e-commerce* não parou de crescer. Esses números refletem uma tendência de crescimento do comércio online, buscando adaptar-se à demanda cada vez maior. As lojas on-line não vendem apenas bens de consumo, mas também alimentos prontos, medicamentos, serviços, entre outros (OLIVEIRA, 2017).

A Internet é um fenômeno, muitas pessoas estão conectadas, tantas empresas decidiram participar dessa comunidade. Como as compras e vendas também são feitas pela internet, muitos consumidores passam a entrar em contato mais e a pesquisar os produtos oferecidos pelas lojas virtuais, obtendo preços mais favoráveis e mais tipos de produtos no conforto de suas casas (SANTOS, 2020). Hoje, as empresas buscam oferecer aos seus consumidores as melhores formas de agradá-los, incluindo promoções, sorteios e lojas virtuais, onde os produtos são sempre vendidos a preços mais acessíveis. As lojas virtuais estão começando a mudar a forma de compra e venda, pois hoje quase tudo pode ser feito pela internet, como pagar contas, verificar contas, transações, envio de documentos, etc.

Diante disto, no próximo tópico discutiremos os conceitos e definições do *e-commerce*, suas vantagens e desvantagens e os tipos de *e-commerce* existentes (MORAES,2017). No Brasil, muitas empresas estão obtendo suas páginas na Internet para abrir suas lojas físicas e abrir lojas virtuais para expandir seus negócios e aumentar o número de clientes. O *e-commerce* ou *e-commerce* remonta aos tempos antigos, foi criado para segurança e hoje se tornou sua estratégia de mercado para

compra e venda (RIBEIRO, 2019). A cada dia o *e-commerce* é atualizado e revisado para facilitar o acesso, mais clientes podem utilizá-lo, para que a empresa tenha a oportunidade de ter mais clientes, os clientes possam ter um acesso melhor e mais rápido aos produtos que procuram. Essa evolução é bastante estável, e o número de consumidores online vem aumentando a cada ano porque a empresa espera estreitar seus laços com consumidores, fornecedores, distribuidores e até mesmo concorrentes para ampliar sua participação no mercado (SANTOS, 2020).

Para Drucker (2000), *e-commerce* pode ser classificado como força motriz da Revolução da Informação, segundo ele é um avanço tecnológico que modifica as tradicionais existentes. O comércio eletrônico pode ser definido como transações comerciais ativadas digitalmente entre organizações e indivíduo, ou seja, todas as transações comerciais mediadas pela tecnologia digital. Envolve o uso da Internet, da *World Wide Web* e de aplicativos e navegadores executados em dispositivos móveis para realizar negócios (OLIVEIRA, 2017).

O *e-commerce* nada mais é do que uma transação online na qual você pode comprar e vender, é uma rede onde as pessoas se comunicam e encontram os melhores produtos ou serviços. Desde que tenha um computador com acesso à Internet, o consumidor pode escolher o produto com o preço mais favorável e a melhor forma de pagamento para efetuar a compra. O *e-commerce* não é apenas uma loja virtual, é uma ferramenta onde você pode expor produtos e serviços, além de expor diversos produtos com preços e marcas diferentes. É uma nova era, e tudo o que você procura pode ser encontrado no computador tela. A evolução do *e-commerce* trouxe uma nova forma de compra e venda que utiliza apenas contatos virtuais e possui grande flexibilidade, podendo ser acessada de qualquer lugar, facilitando assim o processo de compra pela Internet. Santos (2020), define *e-commerce* como um processo social e de gestão em que indivíduos ou grupos obtêm o que precisam e querem criando, fornecendo e trocando produtos valiosos com outros. A oferta e troca de produtos já existia mesmo antes de pensarmos em internet, e o *e-commerce* é apenas uma atualização no modo de compra e venda.

Ao longo da "Década de Ouro", várias lojas online foram criadas e empresas físicas começaram a desenvolver operações. A Internet chegou ao Brasil em 1990 e começou a ser comercializada em 1995, condição necessária para as operações de *e-commerce*. Assim, teve início a história do comércio eletrônico brasileiro, que pode

ser dividida nos quatro períodos a seguir (FERREIRA,2020). Com o estabelecimento do negócio online da Livraria, iniciaram-se as atividades de *e-commerce* no Brasil. Três anos se passaram antes que outras empresas começassem a vender seus produtos por meio de sites da Internet. São Saraiva (livros), *Ri Happy* (brinquedos), *Cia Hering* (roupas) e *Sunglass Hut* (óculos). Nos anos seguintes, em 1999 e 2000, dez novos varejistas começaram a dedicar-se ao trabalho de *e-commerce*, produtos que envolvem os mais diversificados setores como eletroeletrônicos, eletrodomésticos, confecções e farmacêutico. Entre 2001 e 2005, no momento de crise mundial, existiam apenas cinco empresas de comércio eletrônico Surgiram o Brasil: Terra dos Pássaros, Lojas KD, Zona Sul Supermercados, Grupo Herval e Novo Mundo. O período de 2003 a 2012 foi denominado "Década de Ouro" do varejo. Caracterizado por expansão das vendas continuam a ser superiores ao PIB e, em termos de *e-commerce*, o crescimento é mais rápido.

Em 2004, a rede social começou quando o Google lançou o Orkut, que mais tarde foi substituído pelo *Facebook*. Em 2011, começaram a aparecer as primeiras *fanpages* da empresa nesta nova rede social. Já existem várias categorias de consumo no *e-commerce* No Brasil, bens duráveis (eletrodomésticos, eletrônicos, Móveis, etc.) para serviços de entretenimento (ingressos Cinema, teatro e espetáculos) e turismo (passagens aéreas e rodoviárias, hospedagem, alimentação). Já começou a expansão do *e-commerce* para o consumo de bens de consumo de grande movimento, como perfumes e cosméticos, medicamentos, bebidas e alimentos não perecíveis.

Segundo Martucci (2020), a pandemia Covid-19 mudou o comportamento de compra dos brasileiros. Com o fechamento dos pontos de venda físicos, os compradores estão se voltando para o *e-commerce*. Essa migração acontece tanto para compradores que já estão acostumados com as compras online, mas também para compradores que nunca experimentaram o canal. Sete em cada dez brasileiros disseram que planejam continuar mesmo após o fim da quarentena. Devido à nova pandemia de Coronavírus, as lojas físicas foram fechadas e os empresários mudaram as vendas para ambientes virtuais. 80% das pessoas optam por vender por meio de grandes sites como Mercado Livre, Submarino e Magazine Luiza. Esses varejistas atuam como "shopping centers digitais" em seus mercados, trazendo um grande número de consumidores às lojas virtuais para crianças que usam suas plataformas.

Como recompensa, as pequenas empresas ainda podem usar a infraestrutura logística da gigante.

Os *marketplaces* já representam 78% do total do *e-commerce* brasileiro, segundo a *Ebit/Nielsen*. Nos primeiros seis meses de 2020, eles foram responsáveis por 30 bilhões de reais de faturamento do *e-commerce*, um crescimento de 56% em relação ao mesmo período de 2019 (INGIZZA, 2020). Milhares de lojistas que, até então, estavam trabalhando somente com a loja física, decidiram dar uma chance ao online para sobreviver. De acordo com a pesquisa da *Ebit/Nielsen*, as lojas que trabalham tanto no online quanto no e representam 73,1% das vendas digitais no Brasil. No primeiro semestre, elas registraram 57 milhões de pedidos, 54% mais que no mesmo período de 2019. Já o faturamento dos lojistas cem por cento digitais cresceu 26%, totalizando 9 bilhões de reais (INGIZZA, 2020).

O comércio eletrônico se tornou um lema que os comerciantes não podem ser excluídos. Infelizmente, o número de clientes diminuiu significativamente, o que levou a uma diminuição nas vendas (FERREIRA, 2020). Deve ser uma das definições estratégicas de varejistas e fabricantes E investidores de todas as esferas da vida. Caso contrário, a empresa estará destinada a reduzir a competitividade. De comida pronta para transporte, incluindo serviço, Pacotes de viagens e passagens aéreas, desembarques no *e-commerce* atuam de forma interligada aos demais canais de venda. Olhando para o futuro, algumas inovações já são esperadas. Deve ser colocado em prática nos próximos anos, como *drones*, carros autônomos, entrega antecipada com base em algoritmos de inteligência artificial, etc. O comércio móvel deve ser entendido como uma oportunidade para os comerciantes. Empresas de todos os portes já estão investindo em redes sociais.

O *Facebook* e o *Instagram* são usados como ferramentas de comunicação e publicidade, mas esses aplicativos também podem direcionar os consumidores a lojas virtuais ou outros canais de atendimento para promoção de compras. As vendas pelo aplicativo *Whatsapp* (*Whatsapp Business*) também estão crescendo e atendem a lojistas de todos os portes, sendo possível entrar em contato com os clientes de forma rápida e direta (FERREIRA, 2020). Os entraves logísticos são um dos principais empecilhos do comércio eletrônico brasileiro, pois, devido à sua dimensão continental, acarreta grande expressividade no frete e no tempo de entrega dos produtos. Deve-se estimular a cadeia de suprimentos, a localização estratégica do centro de

distribuição e a busca de alternativas para redução dos custos de frete (OLIVEIRA, 2017).

A presente época conhecida como a era da sociedade da informação -, na qual nos tornamos cada vez mais dependentes da tecnologia, a segurança cibernética é um assunto que precisa estar em pauta nas esferas pública e privada, bem como nos âmbitos pessoal e profissional (FERREIRA, 2020).

É possível identificar através das informações explicitadas neste artigo que a maioria dos crimes virtuais ocorre por meio do *phishing* e, de mesmo modo, a partir da utilização da engenharia social (INGIZZA, 2020). Através dessas técnicas, os cibercriminosos exploram as vulnerabilidades tecnológicas e humanas.

A próxima sessão aborda sobre os principais delitos cometidos na internet para melhor explanar os dados expostos nesse estudo.

3. DELITOS COMETIDOS ATRAVÉS DA *INTERNET*

Sobre o início do crime virtual, o relato ocorreu na década de 1970, quando o objetivo dos especialistas em informática era contornar os sistemas e a segurança das instituições financeiras. Na contemporaneidade, os pensamentos e pensamentos dos criminosos são logicamente diferentes daqueles da época, mas a mudança essencial é que todo tipo de pessoa que pode acessar a *Internet* pode cometer delitos cibernéticos usando computadores como principal meio (CASTRO, 2003). Portanto, os usuários domésticos podem ser passivos ou ativos em qualquer tipo de litígio que envolva o crime cibernético.

Os primeiros delitos cibernéticos de informática iniciaram-se na década de 70, sendo executados, em sua grande maioria por pessoas especializadas no ramo informático com o objetivo principal de adentrar ao sistema de segurança das grandes empresas tendo como maior foco as denominadas como instituições financeiras. O perfil atual dos criminosos que atuam nessa área foi alterado, já que nos dias atuais qualquer pessoa que tenha um conhecimento, porém não tão aprofundado basta ter acesso a rede mundial de computadores para que consiga lograr êxito na execução de um crime virtual. (CARVALHO, 2020, p.9).

Nesse meio, direitos básicos do cidadão garantidos pela Constituição Federal, como a igualdade, a privacidade e a dignidade, foram sobrepujados e violados, uma vez que a depender do fato, não era sequer considerado típico, não alcançando certos infratores. Estes criminosos se aproveitam dessas lacunas contidas nas leis para continuar a prática de condutas que estão prejudicando, de várias maneiras, desde pessoas físicas até as pequenas e grandes empresas e também o Governo Federal, que vêm sendo lesados por causa de invasões nos seus sistemas de informações¹(CARVALHO, 2020).

Tais delitos são chamados de delitos cibernéticos virtuais, digitais, informáticos, fraude informática, delitos cibernéticos, delitos cibernéticos transacionais, dentre outros. São várias as denominações dadas à prática de delitos em ambiente virtual.

¹ Segundo matéria do jornal CNN e G1, O site do Ministério da Saúde (www.saude.gov.br/) sofreu um ataque hacker na madrugada sexta-feira (10/01) e saiu do ar. Segundo a mensagem publicada no endereço, “dados internos dos sistemas foram copiados e excluídos”. Todos os portais da pasta, como o “ConecteSUS” e o “Portal Covid” também foram afetados e se encontram sem possibilidade de acesso.

Existem muitos nomes de delitos cibernéticos no ambiente virtual. Não há consenso sobre os melhores nomes para delitos cibernéticos relacionados à tecnologia, delitos cibernéticos de computador, delitos cibernéticos de computador, abuso de computador e fraude de computador. Em suma, esses conceitos ainda não abrangeram todas as tecnologias- delitos cibernéticos relacionados. (POPPER,2018, p.48).

A análise se o comportamento do agente constitui crime deve ser realizada em uma determinada ordem, ou seja, analisa-se primeiro a tipicidade do comportamento, depois a antilegalidade e, por fim, a culpabilidade. O crime é o mesmo para o crime comum e o digital, ou seja, o comportamento humano pode causar danos ou perigo aos ativos mais importantes da sociedade, em ambos os casos o comportamento humano está sujeito a sanções legais (GROSSI, 2005).

O cibercrime pode ocorrer em qualquer lugar, não existindo barreiras para sua prática, este tipo de criminalidade em nada diverge da realizada na realidade, o criminoso emprega diversos artifícios para a prática do crime virtual, esta espécie de delito não se diferencia também na questão dos efeitos e danos gerados a vítima (BORRI,2021). O cidadão que executa ação típica, antijurídica e culpável enquadra nos fundamentos de crime, e será processado, sentenciado por seus atos. O equivalente acontece com o indivíduo que realiza o ato virtualmente (CRESPO,2011).

O cibercriminoso, como sujeito ativo, tem sido identificado, em sua maioria, como jovens desta geração. Mas fato é que, qualquer indivíduo que possui conhecimento informático, com a capacidade de conectar-se a um computador ou dispositivo eletrônico à *internet*, pode ser um malfeitor de grande periculosidade (GROSSI,2005).

Os transgressores responsáveis por delitos virtuais podem ser tanto sujeitos possuidores de um discernimento hábil mais elevado relacionado à *internet*, como hackers ou crackers, quanto utilizadores comuns que, através de suas ações virtuais, realizam delitos em desfavor de outros usuários. Assim sendo, não se deve delinear um retrato tachado sobre o criminoso (CARVALHO,2020).

Borri (2021) comenta que para chegar até o sujeito de transgressão, ou ator do crime, o Direito Penal não pode alcançar pessoas abstratas, virtuais.

Delito cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos delitos cibernéticos cibernéticos são cometidos por cibercriminosos ou hackers que visam ganhar dinheiro ilícito (PINHEIRO,2020).

Os principais tipos de delitos cibernéticos eletrônicos são: Interceptação de informações pessoais de terceiros ou dados sigilosos de organizações e empresas; Roubo de dados financeiros ou credenciais bancárias de terceiros — sejam indivíduos ou organizações; Invasão de computadores pessoais, de empresas ou redes de computadores (POPPER,2018).

Os delitos cibernéticos virtuais são condutas típicas, ilícitas, antijurídicas e culpáveis pelo uso indevido da *internet*, resultando em lesão ou quebra de sigilo, até mesmo estelionato, e as punições para delitos cibernéticos desta natureza ainda são “inexistentes” até a atualidade; fato pelo qual deixa hackers e crackers (POPPER,2018).

Os delitos cibernéticos virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime. São também chamados de delitos de risco informático (PINHEIRO,2020). São exemplos de delitos cibernéticos digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas (POPPER,2018).

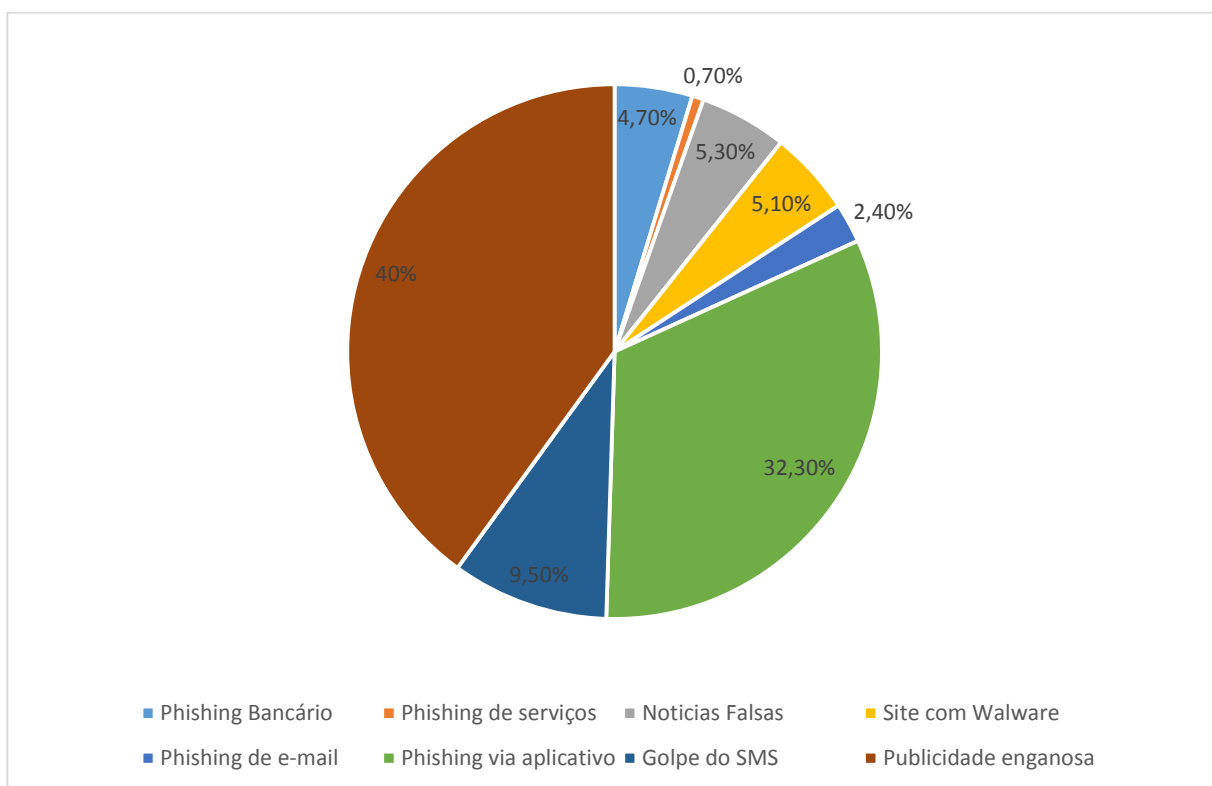
Portanto, os delitos cibernéticos virtuais próprios são aqueles em que o computador, como sistema tecnológico é usado como objeto e meio para execução do crime, já os delitos cibernéticos virtuais denominados impróprios são aqueles realizados com a utilização do computador, onde este é utilizado como instrumento para realização de condutas (POPPER,2018).

Os delitos cibernéticos virtuais denominados impróprios são aqueles realizados com a utilização do computador, ou seja, por meio da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico (POPPER,2018).

O Brasil conta com uma norma criada exclusivamente para regular crimes digitais. A Lei 12.737/2012 especifica punições para infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou "derrubar" sites. Projetos em discussão no Senado caracterizam crimes cometidos na internet e preveem penas mais severas nesses casos (RIBEIRO,2019).

O gráfico 1 mostra os crimes mais cometidos pela internet no Brasil durante o ano de 2018, segundo dados divulgados pela Revista Núcleo do conhecimento (2020), vide:

Gráfico 1 – Crimes cibernéticos



Fonte: Silva,2020, p.12

A análise, que foi realizada entre os dias 01 de Julho e 30 de Setembro de 2018, identificou que houve um crescimento de 44% dos ciberataques.

A segurança cibernética deve referir-se à segurança do ciberespaço, em que ciberespaço se refere ao conjunto de conexões e relacionamentos entre objetos que são passíveis de acesso através de uma rede de telecomunicações generalizada; e, ao conjunto de objetos por si só onde os mesmos apresentem interfaces permitindo seu controle remoto, acesso remoto a dados ou suas participações em ações de controle dentro deste ciberespaço (SILVA,2020).

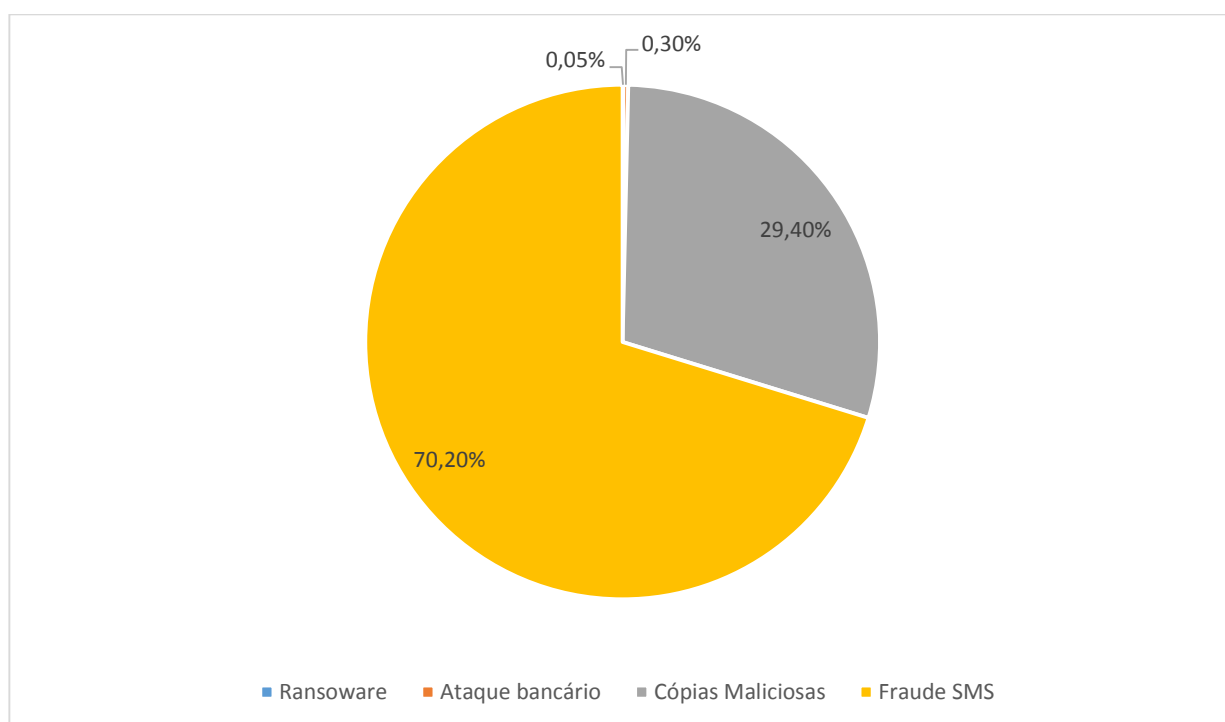
Silva (2020) comenta que é importante destacar o Art. 154-A do Código Penal, que trouxe para o ordenamento jurídico o crime de “Invasão de Dispositivo Informático”, consistente na conduta de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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”. A pena prevista para o crime simples é de detenção de

três meses a um ano e multa, havendo, entretanto, a previsão das formas qualificada e causas de aumento de pena (SOUZA,2020).

A legislação supracitada demonstrou uma evolução da mesma, na medida em que notamos uma preocupação da sociedade com a segurança e com a proteção do direito ao sigilo de seus dados no âmbito digital (SOUZA,2020). A edição da Lei nº 12.737/2012 constituiu um importante avanço ao tipificar expressamente o crime de “invadir dispositivo informático”, criando um tipo penal que visou eminentemente proteger o sigilo dos dados e das informações pessoais e profissionais (SILVA,2020).

Os Principais tipos de ataques por *malwares* são demonstrados no gráfico 2:

Gráfico 2- Principais tipos de ataques por *malwares*



Fonte: Silva,2020, p.15

Com base nas informações acima, o relatório publicado pelo DFNDR Lab expõe que os links maliciosos são 12 vezes mais utilizados em ataques do que os *malwares*.

4. PROTEÇÃO DOS USUÁRIOS NA INTERNET

Sydow (2021), no que tange à regulamentação da Internet no Brasil, está regulada pela Lei que ficou conhecida como Marco Civil da Internet brasileira (Lei nº 12.965/2014) e que possui como objetivo regulamentar o acesso à rede no País, buscando garantir que a internet continue livre e culturalmente diversificada. O legislador, para definir o conceito de internet, se utilizou do art. 5º. inciso I da referida Lei, dispondo que é “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

De acordo com Sydow (2021):

A internet é um grande círculo social, universal e inevitável, quer (sic) permeia todos os demais círculos sociais em que vivemos, que melhora a comunicação entre as partes e representa a evolução cultural da humanidade. Dentro da própria rede há também sub-círculos de interesse, por vezes até mesmo organizados nas denominadas redes sociais. (SYDOW, 2021, p. 46)

Importante ressaltar que a Lei, além de regular o uso da internet, prevê princípios e garantias, o que a faz ser considerada por muitos estudiosos como a “Constituição da Internet”, pois garante direitos e deveres para quem usa a rede, bem como determina diretrizes para atuação do Estado em relação à matéria, sobretudo sem deixar de lado a dinamicidade e a imprevisibilidade que surgem com o descobrimento de novas tecnologias informáticas (ROHRMANN, 2005).

A Lei representa uma positivação de regras e princípios que são necessários à adequação social, comportamental e cultural no que se refere a normas jurídicas. Tal Marco é responsável por demonstrar grande preocupação com os Direitos, sejam eles constitucionais ou não, os protegendo até mesmo em ambiente virtual. Apontando claramente como deve ser o tratamento da comunicação como um direito fundamental e não um mero negócio comercial (CRESPO, 2011).

No artigo 2º, o legislador tratou de disciplinar sobre os fundamentos, um rol que dispõe sobre diversos assuntos, ganhando a liberdade de expressão grande destaque, vez que o referido artigo a contempla em seu caput, que segue acompanhado de outros seis fundamentos. A escolha do legislador se deu de

maneira estratégica, pois busca entender que na prestação de serviços de Internet e na sua utilização os usuários deverão sempre observar os pilares e/ou fundamentos previstos na Lei, dando especial atenção à liberdade de expressão (JESUS; MILAGRE, 2014).

Na análise da Lei, percebe-se ainda que o artigo 3º, inciso I, trata da liberdade de expressão na Internet, que não é absoluta no sentido de não ter consequências, mas o que não pode acontecer é deixá-la de lado, ignorando-a, vez que seu pelo exercício mostra-se fundamental que a internet atinja seus objetivos de comunicação e integração. O que faz com que a liberdade de expressão ganhe lugar de destaque, possuindo razões técnicas e políticas para o oferecimento de tratamento especial que é concedido (SOUZA, 2015).

No artigo 7º o legislador define o acesso à internet como essencial ao exercício da cidadania, e assegura aos usuários direitos, seguindo um pensamento Europeu, surgido na França, no ano de 2009, e declarou que o acesso à internet é “serviço essencial”. Outro ponto que merece destaque no que se refere à Lei, é o fato de abranger hipóteses de responsabilização, onde os provedores de internet podem se isentar da responsabilidade decorrente da má utilização da internet por seus usuários. Para tanto, devem guardar registros de acessos de seus usuários, o que faz com que não haja anonimato ou pelo menos seja reduzido (CARVALHO, 2001).

Por fim, cumpre ressaltar que o destaque oferecido à liberdade de expressão na Lei nº 12.965/2014 foi além de um mero realce como fundamento, já que buscou justificar o posicionamento que é oferecido pelo legislador aos demais dispositivos da Lei, o que ainda se mostra longe de solucionar todos os problemas relativos aos crimes na internet (GRECO, 2005).

Recentemente, inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) europeu, foi sancionada no Brasil a Lei Geral de Proteção de Dados Pessoais, (Lei nº 13.709/2018), que possui como principal objetivo garantir a transparência no uso de dados de pessoas físicas em quaisquer meios, instituindo um novo marco legal de proteção de dados pessoais dos indivíduos nas relações que envolvam o tratamento de informações, alterando inclusive a Lei nº 12.965/2014, tornando mais rígidos os controles sobre dados pessoais e

prevenindo eventuais abusos. Contudo acabou deixando de fora implicações penais, restando apenas as administrativas (PINHEIRO,2010).

Com o advento da LGPD, o indivíduo deverá dar o seu consentimento sobre a cessão de seus dados e informações a terceiros e a outras empresas. Ela “é uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas” (PINHEIRO, 2020, p. 9), visa a proteger a privacidade, resguardar direitos, assegurar que sejam cumpridas garantias relativas à proteção dos direitos humanos.

Sendo importante mencionar:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

O seu artigo 2º dispõe sobre a proteção de dados pessoais e traz como fundamentos, dentre outros: a liberdade de expressão, de informação, de comunicação e de opinião, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. No artigo 17 a Lei assegura que toda pessoa natural é titular de seus dados pessoais, sendo estes garantidos por Direitos fundamentais de liberdade, de intimidade e de privacidade.

Encontra-se no artigo 22 a defesa dos interesses e dos direitos dos titulares de dados, que poderá ser exercida em juízo, de forma individual ou coletiva, conforme disposto na legislação pertinente acerca dos instrumentos de tutela individual e coletiva. Pode-se verificar que a intenção do legislador é de proteger direitos fundamentais, liberdade e privacidade, sem deixar de lado o desenvolvimento da personalidade da pessoa natural, fazendo que haja um controle mais rigoroso no tratamento de dados pessoais.

4.1 ESPIONAGEM ELETRÔNICA

Trabalhar, vender, comprar, jogar, se relacionar, na atual internet o indivíduo tem a possibilidade de se conectar em tempo real com todos seus dados. Geralmente essas informações são salvas em e-mails e chats de forma prática, dessa forma essa praticidade proporciona ao usuário agilidade e também, pode ser usada para lazer e educação (POPPER,2018).

Em delitos definidos como Fraude Virtual, o procedimento utilizado é a de invasão, modificação ou alteração, adulteração em programas de computação de informações ou supressão de dados eletrônicos ou projetos (RAELE,2010).

Existem dois tipos de Fraudes virtuais: As fraudes externas, na qual quem comete a fraude não tem elo direto com a localidade a ser fraudada e a fraude interna que é realizada por aquele indivíduo que está dentro da localidade a ser fraudada seja ele um residente ou funcionário ou mesmo um terceiro que esteja executando um trabalho ou de passagem pelo local (SILVA,2011).

Na execução dos delitos abrangendo fraudes virtuais, o usuário é sujeito a fornecer seus dados financeiros ou pessoais. Parte dos atos na atualidade que são praticados, os fraudadores tentam por meio de redes sociais formas de estimular usuários a fornecer dados pessoais (SILVA,2011).

Atualmente, o uso de tecnologias da informática pelo homem é crescente, dessa forma também aumenta a dependência das empresas por softwares variados, o que amplia a duração de conexão de ambos os acontecimentos a rede mundial de computadores, proporcionando o lançamento de maiores informações planejadas e pessoais nos servidores empresariais. Esse ato aumenta a obrigação de precaução e fiscalização de segurança de dados (SILVA,2011).

Em recinto laboral, deve-se existir mais segurança por meio da aplicação por parte das empresas, tendo em vista que ameaças internas têm a possibilidade serem dificilmente identificadas, pois o sujeito que pratica tal conduta é um usuário considerado legítimo atrapalhando sua identificação (SILVA,2011).

4.2 FRAUDES VIRTUAIS

Características físicas, morais e intelectuais de uma pessoa são a sua honra. A honra deve ser zelada, pois é um patrimônio que o cidadão possui. A honra do indivíduo é subjetiva, composta por sentimentos próprios de respeito, de moral, de propriedades intelectuais e por alguns outros fundamentos (BLUM,2006).

Delitos em desfavor da dignidade da pessoa presumidos no código penal brasileiro e estes são os crimes mais comuns cometidos por meio da internet. O crime de difamação é um dos crimes contra a honra, este está definido no artigo 139 do código penal:

Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa. Parágrafo único. A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções (BRASIL. Código Penal. Art.139.p.69).

Segundo Bolos (2007), a difamação consiste na imputação, a alguém, de fato ofensivo à sua reputação, a pena prevista no Código Penal é de detenção de três meses a um ano, além do pagamento de multa. Trata-se de infração que macula a honra objetiva da vítima. A difamação é muito comum na internet, principalmente nas redes sociais.

Não há monitoramento efetivo na internet, também não existe territorialidade, sendo assim as transações de informações são rápidas, facilitando que materiais sejam copiados e compartilhados de maneira desorganizada ou gerando desrespeito a quem o produziu não dando respaldo ao autor da obra. Crimes contra a propriedade intelectual (BLUM,2006). A violação de direito autoral é crime contra a propriedade intelectual que encontra-se tipificado no Capítulo I do Título III, no artigo 184 do Código Penal, cuja objetividade jurídica é a propriedade imaterial.

Art. 184. Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa (BRASIL. Código Penal. Art.184.p.42).

Quem produz cópias, distribui ou se apropria de uma propriedade intelectual sem autorização prévia do dono ou autor comete uma infração ou crime perante a lei (BLUM,2006).A propriedade Intelectual é o conceito relacionado com a proteção legal e reconhecimento de autoria de obra de produção intelectual tais como

invenções, patentes, marcas, desenhos industriais, indicações geográficas e criações artísticas e garante ao autor o direito, por um determinado período, de explorar economicamente (DWORKIN,2012).

Segundo Castells (2013), infringir aplicativos e programas de computador não é mencionado no código penal brasileiro, que se restringe a cópias de obras intelectuais e a obras fonográficas. A pirataria de softwares é atualmente a maneira mais comum de violação de direito autoral e constitui-se na cópia não autorizada de softwares que são feitas por entidades ou usuários finais (BLUM,2006). A rede mundial de computadores tem diariamente sites em volta do mundo que proporcionam download gratuito de software, é oferecido ao usuário que percorre na rede, cópias desviadas ou falsas, facilitando dessa forma a pirataria pela internet.

Os operadores do direito têm um grande obstáculo, pois o padrão econômico de exploração de propriedade intelectual deve ser analisado, pois nos dias atuais a ideia que se tem é que se está divulgando na internet é público (BLUM,2006).

4.3 O DIREITO À PRIVACIDADE AMEAÇADO PELA VIRTUALIZAÇÃO DA VIDA

A sociedade da informação é aquela que mais satisfatoriamente sabe fazer o melhor uso das novas tecnologias da informação, ou seja, onde as pessoas aproveitam essas vantagens em todos os aspectos de suas vidas: seja no trabalho ou em casa, para seu lazer (FERREIRA; SERRA, 2012).

Essa sociedade foi ainda responsável pelo surgimento de novos produtos financeiros, sendo derivados dos tradicionais títulos e ações, além da exploração de novas atividades, comerciais e financeiras, que foram capazes de elevar a proporção de ativos financeiros mundiais em números nunca vistos antes, fazendo com que fossem reinventadas novas formas de geração de capital, conectando empresas, Estados e investidores internacionais (FARIA, 2010), o que transforma a sociedade e apresenta um conceito novo de normalidade, jamais foi experimentado na história da humanidade, sendo impossível imaginar atualmente um mundo sem a presença da informática e da virtualidade.

O Direito sendo, uma ciência social deve aliar o progresso do ser humano e da sociedade na qual ele está incluso, zelando pelas necessidades de leis que regulam os fatos das relações humanas. Com a chegada da internet e o alastramento da

cultura da globalização, a sociedade andou a “passos largos” em sentido a uma geração submissa da informática, sucedendo muitos atos da vida comum pelos sistemas informatizados (PINHEIRO,2010).Dado a praticidade e a velocidade com que a internet cumpre determinada função, o homem cada vez opta pelas ferramentas virtuais, o que se propaga hoje no meio social é que, se o indivíduo não possui conta de e-mail ou algum tipo de rede social é considerada de alguma forma “afastada” da sociedade.

Para compreender esse progresso, é proveitoso analisar de onde despontou a internet. A palavra significa “rede internacional” - advindo da junção dos termos em inglês Inter (Internacional) e net (rede) – nasceu ao fim do século XX. A princípio, surgiu como dispositivo para internalizar os diálogos em casos de guerra e para entender as relações entre o ser humano e as máquinas. No entanto o uso dos computadores era restrito a poucos usuários, pois especialmente era usado para fins militares e científicos (CARVALHO,2020).

O enorme desafio que a Internet tem de superar é o aumento de crimes cometidos por usuários anônimos que se envolvem em pornografia, ameaças, pedofilia e outros métodos usados por cibercriminosos. Com relação à regulamentação da Internet brasileira, ela é regulamentada pela lei conhecida como Marco Civil da Internet no Brasil (CRESPO,2011).

Como vimos, a internet é um importante meio de comunicação que cresce a cada dia devido ao grande número de pessoas que utilizam desta ferramenta para compartilhar informações com a finalidade pessoal ou comercial. Assim, evidentemente que a internet nos proporciona inúmeros benefícios, contudo, da mesma forma, possibilita a prática de atos ilícitos os quais prejudicam de diversas formas os usuários conectados à rede.

A grande maioria dos crimes cibernéticos são praticados com a utilização de softwares criminosos, tais como os cookies; spyware; spamming; hoaxes; sniffer; cavalo de troia; backdoors; vírus e Worm. Destaca-se, que os referidos crimes podem ser praticados por qualquer pessoa, contudo, evidentemente, existem indivíduos específicos tais como os hackers; craker; pherakers; cardes e cyberterrorists. Ocorre que, a grande dificuldade é indicar com precisão o tempo e o local do crime cibernético. Isto porque, primeiro, no âmbito virtual não existem espaços físicos predeterminados, segundo, é possível programar a execução do crime no tempo.

Desta forma, é essencial a identificação da localização da informação, pois será a partir desta constatação que proporcionará a ideia de território, para que, conseqüentemente, seja aplicada a sanção penal competente. Todavia, atualmente ainda existem poucas legislações que tipificam as condutas criminosas no âmbito virtual, o que, de fato, dificulta a punição dos infratores.

No Brasil, recentemente foi aprovado a Lei n.º 12.695/2014, popularmente conhecida como Marco Civil da Internet, que trouxe inúmeros avanços quanto aos direitos e deveres dos usuários e provedores da internet, porém, infelizmente, por si só ainda não é suficiente ao combate aos crimes cibernéticos que crescem de forma extraordinária. Portanto, é necessário regulamentar leis específicas para o combate ao crime cibernético, bem como que haja investimentos de proteção na segurança das informações dos dados dos usuários.

5. CONSIDERAÇÕES FINAIS

Como vimos, a internet é um importante meio de comunicação que cresce a cada dia devido ao grande número de pessoas que utilizam desta ferramenta para compartilhar informações com a finalidade pessoal ou comercial. Assim, evidentemente que a internet nos proporciona inúmeros benefícios, contudo, da mesma forma, possibilita a prática de atos ilícitos os quais prejudicam de diversas formas os usuários conectados à rede.

A grande maioria dos crimes cibernéticos são praticados com a utilização de softwares criminosos, tais como os cookies; *spyware*; *spammings*; *hoaxes*; *sniffer*; cavalo de troia; *backdoors*; vírus e *Worm*. Destaca-se, que os referidos crimes podem ser praticados por qualquer pessoa, contudo, evidentemente, existem indivíduos específicos tais como os *hackers*; *craker*; *pherakers*; *cardes* e *cyberterrorists*. Ocorre que, a grande dificuldade é indicar com precisão o tempo e o local do crime cibernético. Isto porque, primeiro, no âmbito virtual não existem espaços físicos predeterminados, segundo, é possível programar a execução do crime no tempo.

Desta forma, é essencial a identificação da localização da informação, pois será a partir desta constatação que proporcionará a ideia de território, para que, conseqüentemente, seja aplicada a sanção penal competente. Todavia, atualmente ainda existem poucas legislações que tipificam as condutas criminosas no âmbito virtual, o que, de fato, dificulta a punição dos infratores.

No Brasil, recentemente foi aprovado a Lei n.º 12.695/2014, popularmente conhecida como Marco Civil da Internet, que trouxe inúmeros avanços quanto aos direitos e deveres dos usuários e provedores da internet, porém, infelizmente, por si só ainda não é suficiente ao combate aos crimes cibernéticos que crescem de forma extraordinária. Portanto, é necessário regulamentar leis específicas para o combate ao crime cibernético, bem como que haja investimentos de proteção na segurança das informações dos dados dos usuários.

REFERÊNCIAS

ANDERSON, Ross, BARTON, Chris, BOHME, Rainer, etc all. **Measuring the black web; cybercrime. (How big is criminality on the web?)**The Economist [0013-0613] ano: 2011 vol: 401 fasc: 8755 pág: 69. 2021.

ARAS, Vladimir. **Delitos cibernéticos de informática**. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, p. 51, out. 2001.

BLUM, R M. S. O; BRUNO, M.G.S; ABRUSIO, J.C. **Manual de Direito Eletrônico e Internet**. São Paulo: Lex Editora, 2006.

BRASIL. Supremo Tribunal Federal. (Tribunal Pleno) AÇÃO DIRETA DE INCONSTITUCIONALIDADE POR OMISSÃO N.º 26/DF (Proc.9996923-64.2013.1.00.0000). Requerente: **Partido Popular Socialista**. Intimados: **Congresso Nacional**. Rel.: Min. Celso de Mello. Brasília, DF, Dj 13 de jun. 2019. Dje 28 de jun. 2019 Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4515053>. Acesso em: 01 de ago. de 2021

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: **Presidência da República**, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 25 de abr. de 2021

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Habeas Corpus 82.424/RS. Habeas Corpus. **Antissemitismo. Crime imprescritível**. Conceituação. [...]. Relator: Min. Moreira Alves, 17 set. 2003. Diário de Justiça, Brasília, DF, 19 mar. 2004. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79052>. Acesso em: 23 Outubro. 2021.

BRASIL. Supremo Tribunal Federal. Inquérito 4.781 – **Inquérito das Fake News** RELATOR: MIN. ALEXANDRE DE MORAES. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/mandado27maio.pdf>. Acesso em: 01 outubro 2021.

CARVALHO.A. **Varejo no Brasil: gestão estratégica e ferramentas de proteção na internet**. São Paulo: Atlas, 2020.

DRUCKER, P. Além da Revolução da Informação. **HSM Management**, 2000.

FERREIRA, A. A. **Descrição e avaliação dos modelos de comportamento do comprador**: abordagens parciais e integrativas. Dissertação (Mestrado em Administração). Universidade de São Paulo. São Paulo, São Paulo, 2020.

INGIZZA, Carolina. Vendas on-line no Brasil **Exame**. 2020. Disponível em: <https://exame.com/pme/e-commerce-brasil-cresce-47-primeiro-semester-alta-20-anos/>. Acesso em: 21 março. 2022.

MARTUCI, V.. **E-commerce brasileiro tem alta de 26% no primeiro trimestre**. In: **Economia e Política/Portal Panrotas**. 2020 Disponível em: https://www.panrotas.com.br/mercado/economia-e-politica/2020/04/e-commerce-brasileiro-tem-alta-de-26-no-primeiro-trimestre_172823.html. Acessado em: 28 março 2022.

MENDES, Marcos. Comércio eletrônico no Brasil. 2018 Disponível em: http://www.cultura.ufpa.br/rcientifica/artigos_cientificos/ed_08/pdf/marcos_mendes3.pdf. Acessado em: 28 março 2022.

MORAES, Leonardo. Uma rápida visão sobre o crescimento do e-commerce. 02 abr. 2018. Disponível em: <http://www.ecommercebrasil.com.br/artigos/uma-rapida-visao-sobre-o-crescimento-do-e-commerce/>. Acessado em: 28 março 2022.

OLIVEIRA, P. F. **Comportamento do Consumidor: Vendas on-line**. São Paulo: Pioneira, 2017.

POPPER, Marcos Antônio. **Internet Das Coisas: Potencialidades E Perigos**. Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação. Disponível em https://repositorio.animaeducacao.com.br/bitstream/ANIMA/3703/1/Marcos_Popper%5B48190-49065%5DAD6-versao_final_publicacao.pdf acesso em 23 de maio de 2022.

RIBEIRO, Paula Fernanda. **O crescimento do e-commerce na internet** – período de 2018 a 2019, v. São Paulo – SP. 2019.

SANTOS, Edinalva. **Histórico do Comércio eletrônico**. 2020 Disponível em: <http://www.ebah.com.br/content/ABAAAA9iEAK/comercio-eletronico>. Acessado em: 01 março 2022.

SILVA, Ricardo Leopoldo da. VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 07, pp. 134-149. Abril de 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>, DOI: 10.32749/nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais

SOUZA, Taynah Lopes de; CANONGIA, Claudia. **Technical infrastructure and its importance to national systems of innovation in BRICS**. Projeto “Estudo Comparativo dos Sistemas de Inovação no Brasil, Rússia, Índia, China e África do Sul” – BRICS – Nota Técnica Final em Inglês. Brasília: CGEE. 2020