PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

A EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA NA PREVENÇÃO E PUNIÇÃO DE CRIMES CIBERNÉTICOS:

REFLEXÕES INSPIRADAS NO UNIVERSO CYBERPUNK

ORIENTANDO (A): GUILHERME PAULINO ABRÃO
ORIENTADORA: PROFª: MA. TATIANA DE OLIVEIRA TAKEDA

GOIÂNIA-GO
2024

GUILHERME PAULINO ABRÃO

A EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA NA PREVENÇÃO E PUNIÇÃO DE CRIMES CIBERNÉTICOS:

REFLEXÕES INSPIRADAS NO UNIVERSO CYBERPUNK

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Profª. Orientadora: MA. Tatiana de Oliveira Takeda.

GOIÂNIA-GO

2024

GUILHERME PAULINO ABRÃO

A EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA NA PREVENÇÃO E PUNIÇÃO DE CRIMES CIBERNÉTICOS:

REFLEXÕES INSPIRADAS NO UNIVERSO CYBERPUNK

Data da Defesa: 15 de maio de 2023.

BANCA EXAMINADORA

_____

Orientadora: Profª: MA. Tatiana de Oliveira Takeda Nota

_____

Examinador (a) Convidado (a): Prof. (a) : Pós-doutora Claudia Luiz Lourenço

Nota

Agradecimentos

RESUMO

Este trabalho aborda a efetividade da legislação brasileira na prevenção e punição de crimes cibernéticos, usando o universo cyberpunk como uma perspectiva analítica. O objetivo é identificar deficiências na legislação atual e futura relacionada à cibercriminalidade, bem como desenvolver métodos preventivos. Por meio da análise de obras com temática cyberpunk, o estudo busca revelar possíveis lacunas na legislação cibernética e encontrar soluções para essas questões. O propósito desta pesquisa é aprimorar a atual legislação e identificar áreas onde brechas podem surgir, a fim de abordá-las de maneira eficaz e proativa, utilizando os problemas de uma ficção próxima da realidade como comparativo de problemas atuais e iminentes. O estudo visa fortalecer o arcabouço jurídico relacionado a crimes cibernéticos, tornando-o mais eficiente e ágil em um ambiente em constante evolução. Com o fim de chegar-se aos resultados foram empreendidos estudos baseados no método indutivo e com o auxílio de pesquisa eminentemente bibliográfica.

Palavras-chave: cibercrime; cyberpunk, crime digital; *internet*

ABSTRACT

This work raises the effectiveness of Brazilian legislation to prevent and punish cybercrimes, using the Cyberpunk universe as a method of analysis and perspective of the near future. The objective is to identify the actual and future law shortcomings about cyber criminality, as to develop preventive methods for the problem. Through the analysis of cyberpunk works, the study tries to show possible gaps in cyber law and find solutions for these problems. The purpose of this research is to improve the existing law and identify where possible gaps could be found, in order to be dealt with efficiently and with proactivity, using problems of a fiction close to our reality as a comparison of actual and imminent problems in our society. The study also seeks to reinforce the legal framework of cybercrimes, making it efficient and nimble in a place of constant evolution. In order to reach the results, studies were undertaken based on the inductive method and with the aid of eminently bibliographical research.

Keywords: *cybercrime; cyberpunk; digital crime; internet*

SUMÁRIO

INTRODUÇÃO

Com o avanço da tecnologia, os vírus de computador se tornaram algo cada vez mais notório, e apesar de ser um problema recorrente. O vírus, assim como na própria virologia, um vírus é uma entidade microscópica parasita, o que significa que eles precisam invadir células hospedeiras para se reproduzirem e se replicarem, e com os vírus de computador não se trata de algo tão diferente, pois os vírus de computador são programas de *software* maliciosos projetados para se infiltrar em sistemas de computador e causar danos ou realizar ações indesejadas sem o consentimento do usuário.

Assim como os vírus na biologia, os vírus de computador são considerados parasitas, pois se anexam a programas ou arquivos legítimos para se propagarem. Eles podem se espalhar de uma máquina para outra, muitas vezes por meio de redes ou dispositivos de armazenamento, como unidades USB (*pendrives* por exemplo). Estes vírus de computador podem causar uma série de problemas, incluindo a corrupção de dados, o roubo de informações pessoais e a interrupção das operações normais de um sistema de computador.

O problema é que, desde o surgimento do primeiro vírus, conhecido mundialmente como *Creeper*, em 1971, ainda não era tão malicioso como os atuais, onde o mesmo só espalhava uma mensagem que dizia: "*I'm the creeper, catch me if you can!*" (Sou o *Creeper*, me pegue se puder!). Esse vírus não causava danos aos sistemas, mas marcou o início do que eventualmente evoluiria para as ameaças de segurança cibernética que vemos hoje, onde, além de cada vez mais elaboradas, têm se tornado ainda mais malicioso e mais difíceis de lidar, e justamente devido à esse avanço, as ameaças vêm se modificando e se tornando cada vez mais maleáveis e de difícil punibilidade dos agentes criminosos, como por exemplo, o caso dos vírus denominados de *Worms*, eles causaram estragos significativos no passado, explorando vulnerabilidade em sistemas sendo um dos mais conhecidos o *Blaster*, mas hoje, a maioria dos sistemas operacionais possui uma segurança muito maior, e as atualizações automática ajudam a corrigir rapidamente as vulnerabilidades encontradas.

No entanto, atualmente o *Ransomware*, vem sendo um dos *malwares* (ameaças cibernéticas) mais preocupantes na atualidade. Ele criptografa os arquivos de um sistema e exige um resgate em troca da chave de descriptografia.

Embora não seja uma evolução direta dos vírus antigos, o *ransomware* moderno é sofisticado e pode se espalhar rapidamente, explorando vulnerabilidades semelhantes às utilizadas por *worms*.

O *Ransomware* é uma ameaça cibernética preocupante na atualidade por várias razões, a primeira delas é o fato de que ele criptografa os arquivos de uma vítima e exige um resgate em troca da chave de descriptografia. Isso pode causar sérios danos, interrompendo operações comerciais e bloqueando o acesso a dados críticos.

Além disso, os ataques de *ransomware* podem atingir empresas, organizações governamentais e indivíduos, tornando-se uma ameaça generalizada, assim como mostra a figura 1.

Figura 1: Exemplo de ataque de *ransomware*: *Ransom Crypto888*

Fonte: https://www.softsystem.com

Os ataques de *ransomware* também evoluíram em termos de sofisticação e táticas, com alguns grupos criminosos formando "empresas" de *ransomware* que oferecem serviços de ataque a outros criminosos, tornando mais difícil a identificação dos responsáveis.

Outro aspecto particularmente preocupante é a questão da impunibilidade. A impunibilidade dos criminosos de *ransomware* é uma preocupação significativa, pois muitos deles operam em jurisdições onde é difícil para as autoridades aplicar a lei ou usam criptomoedas que dificultam o rastreamento de transações.

Isso torna desafiador processar e responsabilizar os autores e no Brasil a situação não é muito diferente, vários crimes de *Ransomware* tem se tornado recorrentes e preocupantes devido às brechas existentes.

Isso torna desafiador processar e responsabilizar os autores e no Brasil a situação não é muito diferente, vários crimes de *Ransomware* tem se tornado recorrentes e preocupantes devido às brechas existentes.

A Seção 1 abordará as várias ameaças cibernéticas, a maneira como elas evoluíram e a importância da regulamentação urgente para a redução de ataques e torná-los passíveis de punição criminal.

Por sua vez, a Seção 2 analisará como a legislação brasileira tem lidado com os crimes cibernéticos, examinando sua evolução, possíveis alterações necessárias, além de identificar como os cibercriminosos contornam as lacunas legais

Por fim, a Seção 3 fará a análise da temática *cyberpunk* com o objetivo de explorar as medidas cabíveis na ficção para prevenir os cibercrimes, incluindo as possíveis formas potenciais de cibercrime dentro do universo e como as obras abordam esses problemas. Destaca-se também como essas narrativas podem contribuir para a criação de novas leis mais eficazes no cenário atual.

1 - EMERGÊNCIA DOS CRIMES CIBERNÉTICOS E A NECESSIDADE DE REGULAMENTAÇÃO

1.1 – CONTEXTUALIZAÇÃO DA CRESCENTE AMEAÇA DOS CRIMES CIBERNÉTICOS

Os vírus de computador, popularmente conhecidos como *malware*, já não são uma novidade, pois já são conhecidos desde o surgimento do primeiro *malware* em 1971. A quantidade de *malware* que se espalha e surge na *internet* desde então é simplesmente enorme e apesar do trabalho das pessoas especializadas na área da informática, o problema dos *malwares* vai além do controle desses especialistas.

De acordo com o último relatório de ameaças globais do FortiGuard Labs de 2021, o *ransomware* vem crescendo 1070% a cada ano.

Segundo Maddison, EVP de produtos e CMO da *Fortinet*, seu relatório de 2023 revela que ao menos 75% das empresas sofreram uma invasão em 2022. Esse grande número de ataques mostra a urgência das organizações em garantirem que estão lidando com as técnicas mais recentes de ataques de *ransomware* em redes, *endpoint* e nuvens. O surgimento dos novos *malware* denominados de *ransomware*, têm se tornado um problema massivo, mas além deles ainda é importante falar da preocupação da existência dos *malwares* de vigilância ou intrusão de dados. Diferenciando dos antigos *malwares* um problema de ameaça que apenas causava incômodo ao usuário, mas não causava tanta preocupação, como eram os casos de *malware* de *Macro* onde causavam apenas corrupção de arquivos, como o *Microsoft Word* ou *Excel*, tornando o documento ilegível por exemplo, ou até mesmo os vírus de *Boot* que infectavam discos rígidos e disquetes, para quando fossem inicializado, carregassem a memória do computador e causando falhas na inicialização do sistema e tornando-o inoperável. Há também ainda o mais popular caso antes dos *Ransomware* que durou aproximadamente entre os anos 2000 e 2010, que, segundo a *Kaspersky Lab,* os *Worms* massivos, que se espalhavam de maneira autônoma pela rede, geralmente explorando vulnerabilidades em sistemas e que embora não causasse danos diretos a arquivos, eles sobrecarregavam redes de computadores, propagavam-se rapidamente para outros sistemas e, em alguns casos, exibiam mensagens nas telas dos sistemas infectados tornando-se uma verdadeira dor de

cabeça. Um grande exemplo disso seria o Vírus do Macaco Roxo, como ficou popularmente conhecido o chamado Vírus *BonziBuddy*, que se tratava de um vírus completamente inofensivo, mas que causava completa irritação dos usuários, por justamente, ficar com um macaco roxo sobressaltado em suas telas.

Na atualidade, temos lidado com problemas muito piores, como o caso dos já mencionados *Ransomware*, que têm sido motivo de tirar o sono dos líderes de TI, por basicamente se tratar de um *malware* que se torna um cibercrime de “sequestro de dados” onde os responsáveis realmente pedem um resgate em troca da chave de descriptografia dos dados.

O que torna mais difícil o rastreamento dos criminosos é justamente o método do resgate exigido, onde o pagamento é geralmente feito através de criptomoedas, tornando assim extremamente difícil de localizar o responsável pelo dano causado, pois essas criptomoedas são, por natureza, pseudônimas. As carteiras de criptomoedas justamente por serem identificadas através de chaves públicas e não por nomes reais torna difícil vincular uma transação a uma pessoa física. E além disso muitos criminosos utilizam ferramentas de privacidade *online*, como redes privadas virtuais (VPNs) e serviços de navegação anônima, para ocultar sua identidade e localização.

1.2 DECLARAÇÃO DO PROBLEMA E IMPORTÂNCIA DA REGULAMENTAÇÃO EFICAZ

Segundo a pesquisa da *FortiGuard Labs* (2023), é fato que o mundo inteiro encontra-se preocupado com o problema de *ransomware* apesar de algumas regiões estarem mais preocupadas que outras. Além disso, Maddison (2023) ainda diz que:

> Há uma desconexão significativa entre o quão preparados os entrevistados dizem estar e a sua capacidade de impedir um ataque de *ransomware*. Embora 84% das organizações da América Latina tenham dito que estão muito ou extremamente preparadas para mitigar um ataque, a pesquisa revelou que 53% foram vítimas de *ransomware* no último ano e 45% foram atacadas uma ou mais vezes.

Apesar dessas diferenças, todas as regiões percebem a perda de dados como o principal risco associado a um ataque de *ransomware*, junto à preocupação

de não serem capazes de acompanhar um cenário de ameaças cada vez mais sofisticado.

Ainda se tratando da mesma pesquisa de 2023 da *Fortinet*, a região Ásia-Pacífico e Japão, exclusivamente, lista a falta de conscientização e treinamento do usuário como sua principal preocupação. De acordo com os entrevistados, os da América Latina estavam mais propensos a terem sido vítimas de um ataque de *ransomware* no ano de 2020 (78%) em comparação com 59% na América do Norte e 58% na região da Europa Oriente Médio e África. As técnicas de ataque também variam entre as regiões, embora as iscas de *phishing* sejam comuns.

O *phishing* é uma forma de fraude *online* em que criminosos tentam enganar as pessoas para que revelem informações pessoais, como senhas, números de cartão de crédito e informações bancárias. Os golpistas usam o *phishing* como forma de engenharia social, e fazem isso fingindo ser entidades confiáveis, como bancos, empresas ou órgãos governamentais. O termo *phishing* origina-se através de golpes via *emails* que, mais tarde dá espaço para novos meios para o mesmo método de golpe, como por exemplo, mensagens de texto (SMS) que deu origem à subtipologia de *phishing* denominada *smishing*, *sites* falsos (*pharming*) e até mesmo ligações telefônicas (*vishing*). É também por meio do conjunto de técnicas ardilosas que a grande maioria das pessoas acabam entrando em contato com os *malware*, por acharem que se trata de alguma pessoa, órgão ou empresa legítima, mas se tratam de uma fraude, e dessa forma abrem algum arquivo infectado em seu computador pessoal ou até mesmo de trabalho, podendo assim, corromper arquivos, roubar senhas, sequestrar fotos e outros dados. A partir do momento em que a máquina é infectada, o limite do dano causado vai até onde a criatividade do *hacker* criminoso o levar.

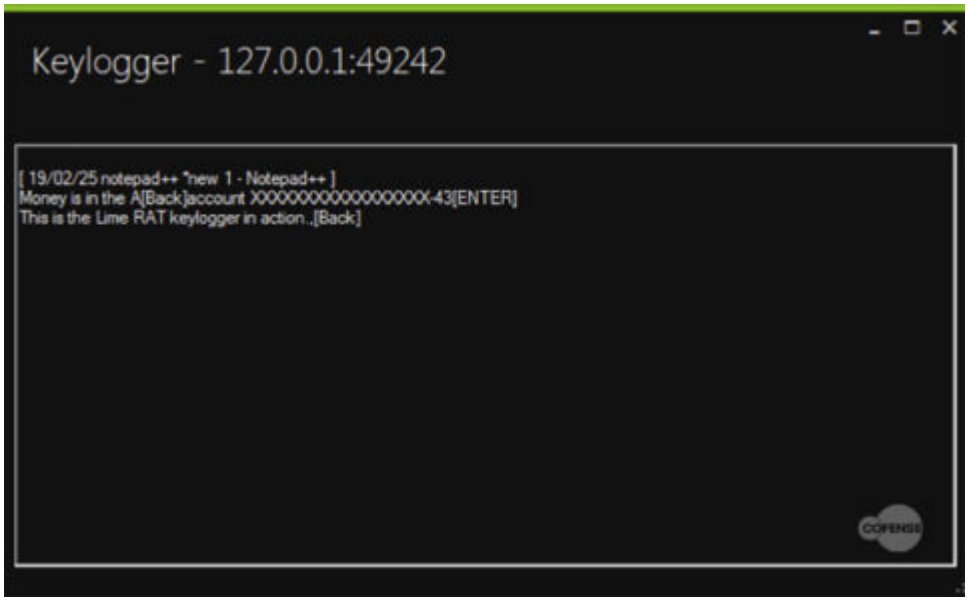
Além do problema do *ransomware*, também é necessário considerar os *spywares*. Embora não sejam mais tão ameaçadores atualmente como o *ransomware,* eles ainda representam uma preocupação significativa. O *spyware* trata de um termo generalista para *softwares* maliciosos que infiltram dispositivos, coletam informações pessoais como registros de digitação, histórico de navegação e informações de *login*, que podem posteriormente ser usados para atividades maliciosas, como roubo de identidade e fraude financeira, ou até mesmo vendidos para terceiros.

Além disso, os *spywares* também invadem a privacidade das pessoas, monitorando suas atividades *online* e *offline* sem o conhecimento ou consentimento

da vítima. Ainda vale a pena lembrar que ele também é uma ferramenta que já foi e continua sendo usada por governos e entidades corporativas para espionagem.

Em resumo, existem três tipos de *spyware* mais comuns e usados atualmente, sendo eles o *Adware*, um tipo de *software* que exibe anúncios publicitários em computadores ou dispositivos móveis, geralmente de forma intrusiva, como *pop-ups* ou *banners*, enquanto o usuário está navegando na *internet* ou usando aplicativos. O *trojan* trata-se de um tipo de *malware* que parece legítimo, como por exemplo um arquivo ou aplicativo, mas executa funções maliciosas, como roubo de informações ou danos ao sistema. Ele não se replica por conta própria e pode se disfarçar como *software* útil, normalmente como um documento ou aplicativo. O termo "*trojan*" vem da mitologia grega do cavalo de tróia. O *keylogger* é um dos mais comuns atualmente para roubo de senhas ou até mesmo mensagens, usado para monitorar e registrar as teclas digitadas em um dispositivo, o maior perigo de um *keylogger* está no fato de que podem ser usados de maneira furtiva, sem o conhecimento do usuário, podendo ter os dados capturados e enviados para um local remoto para análise ou exploração por parte do invasor, apesar de também ser bastante usado de forma legítima como para monitoramento parental ou de funcionários. O LimeRAT é um exemplo de um *trojan* que atua como encriptador e *keylogger* bastante conhecido, conforme mostrado na Figura 2:

Figura 2: Exemplo de coleta de dados realizada pelo módulo *keylog* do LimeRAT



Fonte: https://cofense.com

Um notório exemplo de uma proliferação de *spyware* comercial foi o Caso *Pegasus*, em 2021, quando foi revelado que várias autoridades foram espionadas com o *software Pegasus* da *NSO Group*, como por exemplo a diretora do serviço secreto da Espanha, Paz Estebán, que foi demitida na esteira do escândalo de espionagem dos telefones celulares, do primeiro-ministro Pedro Sánchez e de vários outros integrantes do movimento separatista da Catalunha. Isso levou a pedidos de moratória internacional até que a ONU constituísse um marco regulatório para operações comerciais envolvendo *spywares*, conforme apresentado pela *Fortinet* e veiculado por *sites* de notícias como El País, Sofis, Istoé e BBC News e que será citado posteriormente em comparação com o caso fictício, previsto em 2014 pelo *videogame Watch Dogs 2* da desenvolvedora *Ubisoft*.

Em resumo, essas transações de *softwares* espiões podem ser tão danosas quanto atividades como o narcotráfico, o tráfico de armas e de órgãos, e é importante enquadrá-las nas cadeias de valor do crime internacional.

É fato, no entanto, que os países que produzem ou autorizam esse comércio de *softwares* e programas espiões são cúmplices semelhantes àqueles que controlam atividades ilícitas como o narcotráfico, visto que, apesar de não existir previsão legal para acontecimentos como o Caso *Pegasus*, é de extrema imoralidade a espionagem, coletando dados pessoais e profissionais sigilosos de terceiros sem o seu consentimento. Não há diferença substantiva no campo moral, com a exceção de que empresas como a *NSO Group* produzem algo sofisticado enquanto o narcotráfico opera com uma cadeia de valor simples e com emprego de mão de obra empobrecida e desesperada.

É em casos como esses que torna-se difícil classificar em listas quais seriam as ameaças mais perigosas da atualidade, e tornando impossível o mencionamento apenas de um tipo de ameaça cibernética, sendo que, em cada área há um tipo diferente de ameaça cibernética, que atuam de maneiras diversas, mas que atualmente se resumem a um único objetivo, roubar dados, ameaçar ou obter dinheiro das vítimas, independentemente do método empregado.

1.3 FUNDAMENTAÇÃO TEÓRICA: CRIMES CIBERNÉTICOS E LIMITAÇÕES LEGAIS

O problema do crime cibernético e a maneira como a legislação falha em criar leis e punir os devidos criminosos é simplesmente vasta e que poderia ser dividida em tópicos de assuntos para cada um dos possíveis problemas.

Tratando primeiramente sobre uma jurisdição transnacional, a natureza global da *internet* torna difícil determinar qual jurisdição tem autoridade ou não sobre um crime cibernético específico. Muitas vezes os criminosos operam em um país, enquanto as vítimas estão em outro, o que pode complicar a aplicação da lei.

Para piorar ainda mais a questão problematizada acima, o anonimato proporcionado pela *internet* pode dificultar a identificação e rastreamento de criminosos, além de mascarar o local de origem do crime cometido. O uso de serviços de rede privada virtual (VPN) e técnicas de anonimato torna desafiador rastrear os infratores, simulando por exemplo, sua localização na Rússia, quando, na realidade, estão localizados no Brasil. Justamente pelo fato do anonimato nas redes, muitas agências de aplicação da lei enfrentam limitações em termos de recursos técnicos e capacidade para investigar crimes cibernéticos, sofrendo com a falta de especialistas na área para investigar crimes cibernéticos mais complexos.

A falta de cooperação internacional em crimes cibernéticos também é um problema, pois frequentemente esses crimes envolvem múltiplos países, exigindo cooperação internacional para a investigação e aplicação da lei. Nem sempre é fácil garantir a colaboração entre as jurisdições, uma prova disso é o problema que temos por exemplo, quando se trata de crimes cometidos por brasileiro no exterior e toda a burocracia que envolve a extradição do criminoso.

1.3.1 Definição e exemplos de crimes cibernéticos relevantes

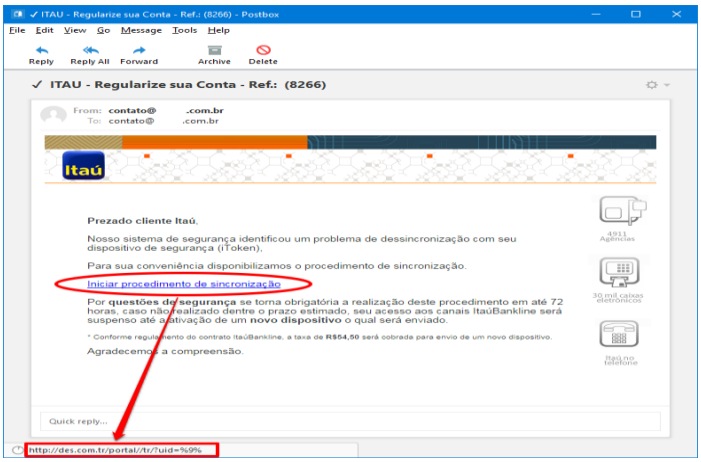
Segundo o Centro de Recursos da *Kaspersky Lab* (2023):

> O crime 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 crimes cibernéticos é cometida por cibercriminosos ou *hackers* que querem ganhar dinheiro. No entanto, ocasionalmente, o crime cibernético visa danificar computadores ou redes por outros motivos que não o lucro. Nesses casos, os motivos podem ser pessoais ou políticos.

Essas atividades muitas vezes exploram a tecnologia e a infraestrutura da *internet* ou até mesmo do despreparo dos indivíduos para cometer atos ilegais.

Além do *Ransomware* e *Spyware* já citados, outro exemplo relevante de crime cibernético é o *Phishing*, e tem sido um dos métodos mais comuns de fraude na *internet* por um longo tempo. O *phishing* geralmente ocorre por *email*, mas também têm se tornado popular em aplicativos de mensagens e outras redes sociais, como *WhatsApp* e *Instagram*. Os criminosos enviam *emails* ou *directs*, fingindo se passar por empresas legítimas ou com uso de *links* falsos enganando assim pessoas desavisadas a fornecer informações pessoais, como senhas e informações de cartão de crédito, ou com uso de *softwares* maliciosos, como citado anteriormente, os *keyloggers*, onde costumam ser usados de forma conjunta. Na figura 3 há um exemplo de *phishing* comum, mas que diminuiu muito as tentativas após medidas das caixas de *email* (*Gmail*, *Outlook*, etc.) detectarem automaticamente uma tentativa de fraude, onde os golpistas personalizam os *emails* para se adequar a uma vítima específica, usando informações pessoais previamente coletadas para aumentar a credibilidade do ataque. Veja-se:

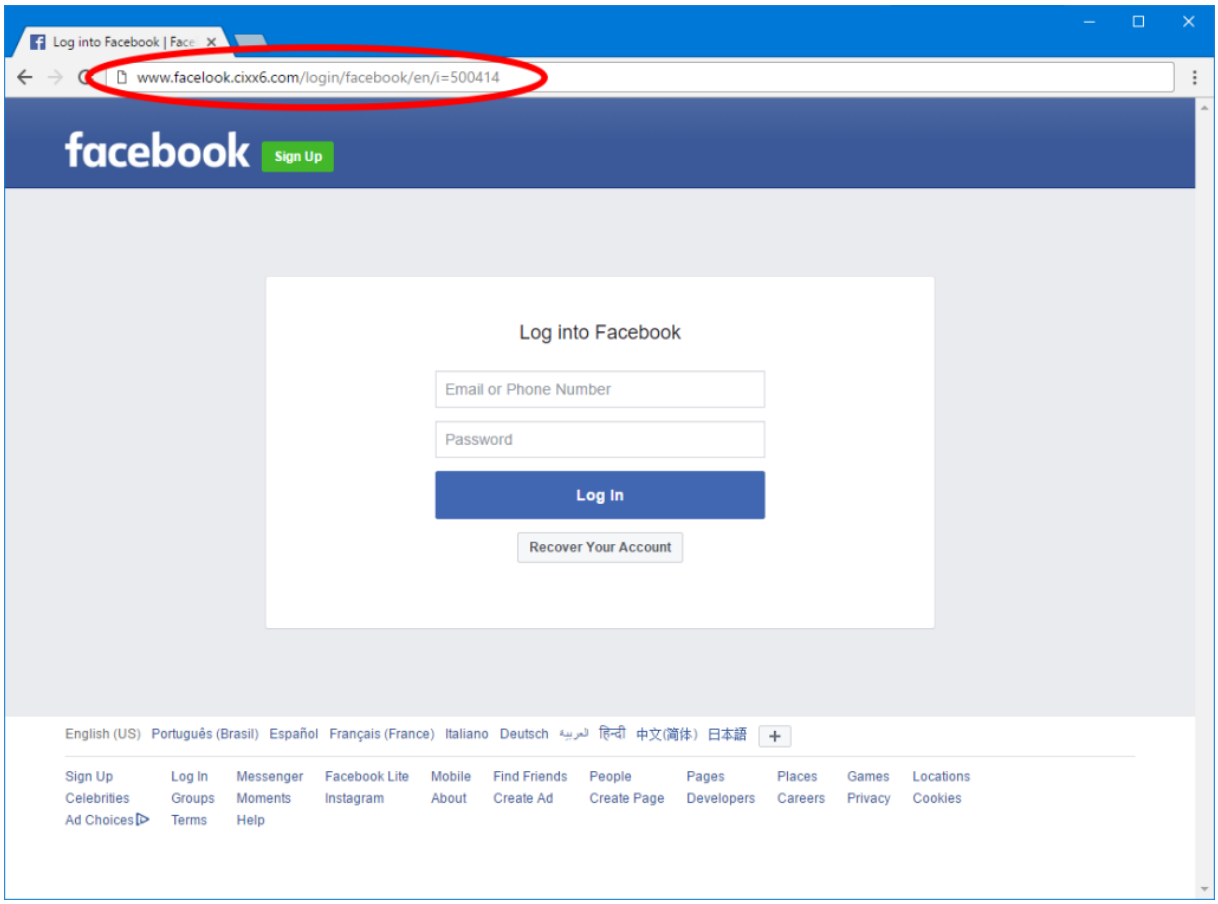
Figura 3: *Email* falso, se passando por entidade bancária, contendo *link* malicioso (*spear phishing*)



Fonte: https://www.lumiun.com/blog

Hoje em dia, o uso de *links* falsos é mais comum, pois é uma maneira mais fácil de realizar o golpe e a vítima muitas vezes nem sequer percebe, apenas possuindo um pouco mais de cuidado ou malícia, têm-se a noção de se tratar de um golpe. No entanto, atualmente as tentativas por *email* têm diminuído, enquanto outras formas de *phishing* foram criadas e dando origem a novos subtipos, como através de SMS (*smishing*), métodos já conhecidos popularmente como “Bença Tia” (*vishing*), golpistas se passando por pessoas ou empresas legítimas (*social phishing*) e até mesmo clonagem de *sites* (*pharming*), assim como é mostrado nas figuras 3. A vítima é direcionada primeiramente para um *site* falso e, em seguida, redirecionado para o *site* verdadeiro após inserir suas credenciais. À primeira vista, parece muito que a primeira tentativa de *login* tratou-se apenas de um erro de conexão, mas nesse ponto as informações da vítima já foram comprometidas. Veja-se:

Figura 4: Exemplo de *site* de *phishing* com endereço incorreto

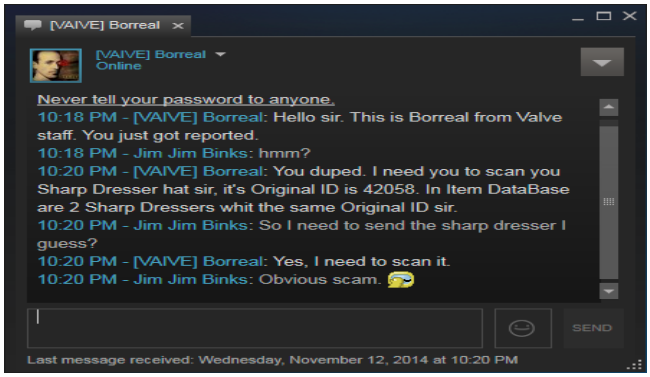


Fonte: https://www.lumiun.com/blog/

Ainda se tratando dos tipos de engenharia social e *phishing,* há outros métodos de engenharia social, como o conhecido como *Scam*, onde é comum acontecer em vários âmbitos, um *scam* pode acontecer na forma de fornecedor falso, se tratando na verdade de criminosos fingindo ser fornecedores de uma empresa e enviando faturas falsas para pagamento, por exemplo, e dessa forma as empresas podem pagar por serviços ou produtos que nunca receberam, causando perdas financeiras e assim é concluído um golpe de *scam*.

Outro exemplo de *scam* que acontece no mundo dos jogos também, é o de troca de itens em jogos *online*, por normalmente a maior parte do público ser de adolescentes, onde estes desavisados podem trocar itens como *skins* (visuais cosméticos personalizados) que normalmente são adquiridas com dinheiro real, ou até mesmo em trocas e vendas de contas *online*, que chegam a obter valores exorbitantes, onde por exemplo uma conta com o nome de usuário Zeuzo do jogo *World of Warcraft* foi vendida pela quantia de 9,5 mil dólares. Os criminosos podem se passar por alguém que trabalhe na empresa, por exemplo, e pedir para verificar algum item na conta conta do jogo, pois aparenta ter algum problema, e que para isso seria necessário realizar uma troca, e após a “verificação” o item será devolvido caso não haja nenhum problema, e nisso o golpista realiza o roubo do produto em forma de troca, um exemplo prático disso é mostrado na figura 5, onde o golpista se passa por um funcionário da empresa *Valve* (desenvolvedora da plataforma de distribuição de *software Steam*). Outra forma disso são jogadores que dizem prometer trocar um item raro por outro valioso e, em seguida, não cumprir com a negociação, e dessa forma, roubar um item valioso, ou até mesmo a conta do jogo. E para piorar esses casos, as medidas de prevenção de *scam* pela indústria são péssimas, tornando sempre um problema maior para a vítima do golpe. Veja-se:

Figura 5: tentativa de *scam* realizada via *chat*, na plataforma *Steam*



Fonte: https://steamcommunity.com

Outro problema que, apesar de não ser muito comum ao público geral, é bem comum entre aqueles que fazem uso constante da *internet* ou que a utilizam de maneira profissional, são os Ataques de Negação de Serviço (DDoS), os criminosos sobrecarregam os servidores com tráfego malicioso para tornar *sites*, serviços inacessíveis, ou até mesmo tornar um computador incapaz de operar na *internet*. A *Gcore* (2022) informou que o volume de ataques DDoS praticamente dobraram em relação a 2021, Slastenov, *Product Manager Security* da *Gcore* também diz na mesma pesquisa:

> *Fintech* (*startups* ou empresas que desenvolvem produtos financeiros totalmente digitais), jogos e comércio eletrônico são os que mais sofrem. Recentemente, abordamos isso em nosso estudo sobre tendências de ataque DDoS no primeiro e segundo trimestre de 2022. Por exemplo, em março deste ano, resistimos a um poderoso ataque de inundação de UDP em uma empresa de jogos e, em abril, combatemos uma inundação de TCP de mais de 24 horas de ataque a um serviço de *fintech*. Novos casos estão surgindo a cada mês, e o volume e o número de ataques mais que dobraram no ano passado.

Um exemplo prático de como funciona Ataques DDoS, apesar de não se tratar de um ataque criminoso, é o *site* do SISU onde, em época de inscrição sofre de sobrecarga todos os anos, devido ao grande número de acessos simultâneos à plataforma.

1.3.2 Discussão das lacunas atuais na legislação brasileira

O principal problema na atualidade ao tratar de crimes cibernéticos no Brasil, é sem dúvida a falta de preparo das pessoas como um todo. A falta da criação de setores públicos especializados em crimes cibernéticos, como por exemplo a existência da Polícia Técnico-Científica ou de Infância e Juventude, destaca a crescente importância de uma polícia especializada e a necessidade de pessoas capazes que atuem na área de proteção de dados e investigação cibernética a cada dia que passa.

No entanto, por certa perspectiva, é certamente óbvio a falta de um setor especializado na área, visto que o Brasil também sofre de um sério problema de falta de especialistas competentes na área e os poucos que existem, ou acabam sendo

contratados por empresas no exterior ou se limitam a ganhar um salário medíocre e da mesma forma, acabam por empenhar um serviço medíocre.

O começo de toda a crise legislativa na área de cibercrime certamente começa na falta de profissionais qualificados para lidar com crimes cibernéticos complexos e de grande porte, no entanto, isso se dá também justamente pela falta de conhecedores na área, a baixa taxa de ataques complexos em setores públicos da mesma forma em que empresas privadas ou pessoas são atacadas.

Fato esse que por sua vez acarreta na impunibilidade dos criminosos, seja pela falta numérica ou de habilidade dos profissionais que impeçam esse tipo de atividade, pela falta de legislação ou de interesse público, que não abrange a questão de algum possível crime cibernético, visto que é recorrente e de notoriedade da grande parte dos brasileiros golpes por celular, e na sua grande maioria, esquemas de engenharia social, que por sua maior parte poderia ser limitada e evitada por grande parte da população apenas com a conscientização pública sobre o básico de segurança cibernética.

Juntamente com a falta de conscientização, a capacidade técnica limitada onde muitas agências de aplicação da lei acabam enfrentando limitações em termos de recursos técnicos, burocracias e a capacidade para investigar crimes cibernéticos, agravam ainda mais a situação de golpes em pessoas despreparadas, sendo muitas vezes necessário recorrer à uma investigação privada ou atividade semelhante para se obter qualquer resultado para identificar e localizar criminosos, e assim, ter possibilidades de reverter uma situação grave.

O anonimato *online* também deve ser trazido à luz mais uma vez, e que por sua vez pode dificultar muito a localização e identificação dos criminosos por conta do uso de máscaras de IP (*Internet Protocol*), que é uma identificação numérica atribuída a cada dispositivo conectado a uma rede de computadores para permitir a comunicação e a identificação exclusiva na *Internet*, como por exemplo, através do uso de VPNs, *Proxy Servers* ou até mesmo, quando se trata de casos mais complexos, através de redes de computadores zumbis (popularmente conhecidos como *botnets*).

Não sendo todos fatos acima o suficiente, é ainda mais difícil a coleta de provas em casos cibernéticos, ainda mais quando os criminosos utilizam técnicas de ocultação avançadas e criptografias de ponta para proteger suas atividades.

Além disso, também deve-se recordar novamente dos casos de cibercriminosos mais simplórios, que usam do *phishing* para extorquir vítimas despreparadas, sendo esse o caso, também há o problema de muitas empresas e pessoas que ainda carecem de conscientização e educação em relação à segurança cibernética, principalmente pela parte das pessoas com maior idade, o que facilita assim, a ocorrência de crimes por *phishing*.

1.3.2.1 Análise da velocidade da evolução tecnológica versus a adaptação legal

Muitas tecnologias são altamente complexas e desafiadoras de entender, ainda mais para especialistas em direito, o que torna a criação de leis eficazes e aplicáveis um desafio quando não elaborada por pessoas que compreendem amplamente ambos os assuntos e a falta destes profissionais é visível, pois não é de todo conhecimento dos operadores do direito ou da tecnologia da informação conhecer tanto da legislação e da complexidade tecnológica, tornando tão difícil e desafiador criar leis efetivas, assim como é desafiador explicar termos de comum uso no meio cibernético, como *software*, *scam*, *bots* ou VPN, para pessoas comuns que não possuem o amplo acesso à esse tipo de informação. Toda essa questão de desafios ao integrar direito, legislação no geral, com a tecnologia e a segurança cibernética, só nos mostra a cada vez mais que é decorrido o assunto, a necessidade de especialistas nesta específica área.

Além disso, é um fato de que a *internet* transcende as fronteiras nacionais, o que torna a coordenação internacional e a aplicação de leis mais uma vez, ainda mais difícil. Crimes cibernéticos podem ser cometidos em um país, enquanto as vítimas se encontram em outro. O que torna um imenso problema, pois é difícil lidar com questões complexas, como no caso do ataque ao sistema *Kaseya VSA*, da empresa *Kaseya*, realizado pelo grupo *hacker REvil*, em julho de 2021, onde a maior parte do problema afetou a América Latina, e apesar da empresa possuir sede nos Estados Unidos e não se saber a exata origem de onde a ameaça começou, justamente devido ao anterior problema mencionado de anonimato, mas especula-se de que o ataque teria origem na Rússia, conforme pesquisa da *CISO Advisor* e *TecnoBlog* ambas do ano de 2022.

Tradicionalmente, as leis demoram a ser criadas e aprovadas, visto que as tecnologias evoluem muito rapidamente, criando-se novos modelos de celular e peças

de computador a cada ano, além de mudarem de sistema operacional frequentemente. Dessa forma, quando uma lei é promulgada, pode ser que a tecnologia já tenha avançado para além do escopo da legislação, existindo assim, essa dificuldade de punibilidade e equiparação entre a tecnologia e a legislação.

Além disso, as questões relacionadas a conflitos de interesses em empresas de tecnologia são um fator adicional de complexidade. Empresas de tecnologia muitas vezes enfrentam desafios ao equilibrar inovação e segurança, uma vez que a expansão de seus serviços e produtos pode estar em conflito com as preocupações de privacidade e segurança dos cidadãos. Por exemplo, empresas de mídias sociais podem coletar uma grande quantidade de dados dos usuários para personalizar experiências, mas isso levanta preocupações sobre a privacidade e o uso indevido de informações pessoais.

Ao mesmo tempo, governos podem buscar acesso a esses dados para fins de segurança nacional e aplicação da lei. Esses conflitos de interesses podem tornar ainda mais desafiador o desenvolvimento de leis que encontrem o equilíbrio adequado entre a inovação tecnológica e a proteção dos direitos e segurança dos cidadãos.

À medida que a coleta de dados, por meio de aplicativos, redes sociais, sistema operacionais se tornam mais difundida e sofisticada, questões urgentes de privacidade emergem no meio digital. Cada clique, cada busca, cada interação *online* alimenta um vasto ecossistema de dados que é tanto a espinha dorsal da economia digital quanto o principal alvo para cibercriminosos.

A crescente preocupação com a privacidade dos dados é justificada pelos constantes relatos de violações de segurança e explorações de vulnerabilidades. Empresas, governos e indivíduos se veem cada vez mais vulneráveis a ataques cibernéticos, que variam de violações de dados massivas a ataques direcionados e até mesmo espionagem cibernética, mas este é um assunto que convém a ser tratado mais detalhadamente em tópicos posteriores.

Os cibercriminosos operam em um ambiente altamente sofisticado, com aparelhos de última geração e muita das vezes se tratam de aparelhos importados e até mesmo proibidos no nosso território, tornando as fronteiras físicas irrelevantes e o anonimato é facilmente alcançado. Eles exploram falhas em sistemas de segurança, utilizam técnicas de engenharia social e lançam ataques de *phishing* para obter acesso não autorizado a informações sensíveis, além de poderem causar outros tipos de danos

Em resposta a essa crescente ameaça, a cibersegurança evolui constantemente, empregando tecnologias avançadas como inteligência artificial e aprendizado de máquina para detectar e prevenir atividades maliciosas. Além disso, regulamentações de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e leis de privacidade de dados em várias jurisdições, como posteriormente levaria a inspirar na criação da Lei Geral de Proteção de Dados (LGPD), que foram promulgadas para proteger os direitos individuais e impor medidas mais rígidas para o tratamento de dados pessoais.

No entanto, a batalha pela cibersegurança está longe de ser vencida. Os cibercriminosos continuam a adaptar suas táticas, explorando novas vulnerabilidades e aproveitando as lacunas na segurança e na legislação. É um jogo de gato e rato que exige vigilância constante, colaboração global e investimento contínuo em medidas de proteção cibernética robustas.

À medida que avançamos em um mundo cada vez mais digitalizado, a proteção da privacidade e a defesa contra cibercrimes se tornam imperativos fundamentais para garantir a segurança e a integridade de nossas informações pessoais e institucionais.

Além disso, vale a pena ressaltar que também existe um certo abuso da privacidade em alguns casos, sendo um caso mais comum aos nossos olhos, como o caso do *WhatsApp*, onde desde 2016 existe um debate acerca da superproteção de dados. Um exemplo disso, foi casos noticiados no Brasil, noticiado até mesmo pelo portal de notícias do G1, onde aconteciam de quadrilhas criminosas de vários tipos que, compartilhavam informações ilegais através do aplicativo e que, por conta da criptografia de mensagens que o *WhatsApp* fornecia, as mensagens enviadas por meio do aplicativo são visíveis apenas para o remetente e o destinatário, impedindo que terceiros, incluindo o próprio *WhatsApp*, acessem o conteúdo das mensagens. Essa medida de segurança é projetada para proteger a privacidade dos usuários. No entanto, essa forte proteção de dados também gerou preocupações de segurança pública e de aplicação da lei. Isso ocorre porque, embora a criptografia de ponta a ponta seja uma camada essencial de segurança para proteger a privacidade das pessoas, também pode ser explorada por criminosos para realizar comunicações secretas e ilegais. Prova disso, é o alerta da *Cisco* no mês de outubro de 2023, sobre uma vulnerabilidade de alta gravidade que afeta alguns modelos de *switch* de central de dados, permitindo que invasores adulterem o tráfego criptografado, permitindo que

invasores não autenticados leiam ou modifiquem tráfego criptografado entre *sites* de maneira remota, sendo assim, uma brecha para vazamento ou sequestro de dados.

Além disso, é um fato inegável que o público em geral e muitos legisladores frequentemente enfrentam dificuldades em compreender totalmente as implicações das novas tecnologias e o alcance de seu impacto na sociedade. As inovações tecnológicas muitas vezes avançam em um ritmo tão acelerado que é desafiador para a maioria das pessoas acompanhar e compreender plenamente as complexidades envolvidas. Isso, por sua vez, pode resultar em leis mal concebidas ou na falta de regulamentação adequada em áreas onde a intervenção é crucial.

É importante destacar que a tecnologia muitas vezes ultrapassa as fronteiras dos conhecimentos tradicionais, e os legisladores podem não estar equipados para lidar com questões altamente técnicas e multifacetadas, como acontece na maioria dos casos quando se trata da área cibernética. Como resultado, o processo de formulação de políticas e leis relacionadas à tecnologia pode ser moroso e, em alguns casos, pode não acompanhar as necessidades da sociedade em constante evolução.

Portanto, existe uma necessidade contínua de educação e conscientização sobre as implicações das novas tecnologias, bem como de esforços colaborativos entre especialistas em tecnologia, legisladores e os cidadãos para garantir a criação de leis eficazes e regulamentações equilibradas que sirvam ao melhor interesse da sociedade como um todo, assim como uma maior prevenção contra crimes e problemas cibernéticos.

2 – LEGISLAÇÃO BRASILEIRA E CRIMES CIBERNÉTICOS: AVALIANDO O CENÁRIO ATUAL

2.1 – ANÁLISE DAS LEIS BRASILEIRAS RELACIONADAS A CRIMES CIBERNÉTICOS

Durante todos os anos após a popularização da *internet*, foram criadas algumas leis relativas à mesma. No entanto, a grande maioria das leis criadas possuem apenas a finalidade de regulamentação, explicando e estabelecendo sobre registros de conexões, dados pessoais , uso e coleta de dados, assim como outros. Um grande exemplo disso é o Marco Civil da *Internet* (Lei nº 12.965/2014) que surgiu com a principal finalidade de estabelecer limites na *internet* e impor normas de segurança para dados e registros. Quatro anos após isso, é criado a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que altera a Lei do Marco Civil da *Internet* para criar um reforço ainda maior na proteção de dados e conteúdo virtual, assegurando ainda mais a proteção de dados, além de deixar mais claro quem serão os responsáveis pelo tratamento de dados, além de assegurar ao usuário uma maior clareza de quem são os responsáveis. Além disso, a Lei traz também uma maior defesa e proteção à dados pessoais sensíveis, sendo passíveis de multas e indenizações, o que traz um reforço ainda maior à Lei nº 12.737/2012.

No entanto, no Brasil a lei mais incisiva sobre a questão de crimes cibernéticos propriamente dita, como invasão de dados e manipulação indevida é tratada no Código Penal Brasileiro apenas com a Lei 12.737/2012, deixando uma grande lacuna entre a responsabilidade das empresas e aplicações (aplicativos e programas) e o criminoso propriamente dito, visto que, devido à Política de Privacidade as empresas se recusavam a colaborar em muitos casos jurídicos pois estariam infringindo as Normas de Privacidade de seus aplicativos e de sua empresa, causando assim uma lacuna na lei, impossibilitando muitas vezes, dessa forma, o rastreio ou identificação de algum criminoso na *internet*.

É notável que nossos legisladores trabalham para melhorar esta questão, uma vez que o Marco Civil da *Internet* já foi modificada após 4 anos de sua vigoração para a nova Lei Geral de Proteção de Dados, mas uma vez que a LGPD foi promulgada em 2018 vigorou apenas 2 anos após a promulgação e isso após vários

adiamentos anteriores à sua implementação. A nova Lei nº 13.709/2018 é sem dúvidas um grande marco para os estudiosos no âmbito da legislação cibernética, no entanto é inegável a sua má implementação e a dificuldade de interpretação que causa na grande maioria das pessoas, sejam elas operadores do direito ou não. Justamente por ser uma lei inspirada em uma outra lei internacional, torna-se difícil sua aplicação no nosso país, uma vez que os problemas enfrentados por crimes cibernéticos em outros países nem sempre são os mesmos, já que se encontram em contextos diferentes e tipos diferentes de crimes mesmo apesar de ser completamente necessária a cooperação internacional na resolução de crimes cibernéticos de grande escala.

2.1.1 – Efetividade da legislação: analisando sucessos e fracassos na prevenção e punição

A efetividade da legislação brasileira na prevenção de crimes cibernéticos é indiscutível: continua persistindo em falhas e inefetividade. Um exemplo notório disso foi o vazamento de dados em 2021 que ocorreu através dos *sites* do Ministério da Saúde e do ConecteSUS, que ficou fora do ar após um ataque de *ransomware* realizado pelo grupo *Lapsus$*, isso nos mostra que o Brasil é um país que certamente não está preparado para lidar com ataques de grande escala, já que, nem mesmo seus órgãos governamentais estão prontos para lidar com os ataques, já que mesmo após implementação da LGPD não encontraram os criminosos, pois um ano após o crime, foram presos dois suspeitos de serem os líderes da organização *hacker*, mas que no ano de 2023 realizaram ataques à *Uber* e *Revolut*.

Para tornar toda a situação de prevenção destes casos, em Janeiro do atual ano (2024) foi publicada em diversos *sites* que tratam sobre o assunto de Cibersegurança o maior vazamento de dados do mundo inteiro, que foi encontrado por diversos pesquisadores da área de segurança, o vazamento apelidado de MOAB (*Mother Of All Breaches*) trata-se não de um vazamento de dados específico, mas de uma compilação de vários vazamentos. O mais preocupante disso tudo é não apenas a dimensão do problema, por se tratar da quantidade de 26 bilhões de arquivos, de aproximadamente 3,800 pastas, onde cada pasta corresponde a um vazamento de dados. Para fins de estimativa, o maior vazamento até a MOAB era de 15 bilhões de arquivos. E o mais preocupante disso, é que os três países mais afetados pelo

vazamento da MOAB são Brasil, Estados Unidos e Alemanha, e no Brasil os *sites* que estão nessa base de dados incluem dados governamentais como USP, SPTrans e Petrobras, além de empresas privadas, como CCA, Descomplica (vazamento em 2021) e Vakinha (vazamento em 2020).

2.1.2 Discussão sobre a adaptação da legislação à natureza mutável dos crimes digitais

Ao se tratar de cibercrime em nosso sistema atual, é inegável o avanço para prevenção do mesmo, no entanto, o problema acaba sendo mais profundo e mais desafiador do que uma simples Lei de Crimes Eletrônicos, visto que a evolução da tecnologia acaba por superar a capacidade da atual legislação de abordar de maneira eficaz novas formas de crimes cibernéticos, como ataques *ransomware*, formas de *phishing*, e outros métodos de crimes cibernéticos mais atuais em que a legislação não estava nem um pouco preparada, como o atual caso do uso indevido de inteligência artificial para crimes e vulnerabilidades de segurança emergentes.

No caso de ataques como o *ransomware*, apesar da previsão legal como crime, o processo criminal envolta é completamente difícil, podendo na maioria dos casos ultrapassar barreiras internacionais, como nos inúmeros casos citados anteriormente, onde é necessária a cooperação de diversos países tanto para o rastreio quanto para a prisão do cibercriminoso, o que por sua vez, pode levar anos para ser realizada, quando encontrados.

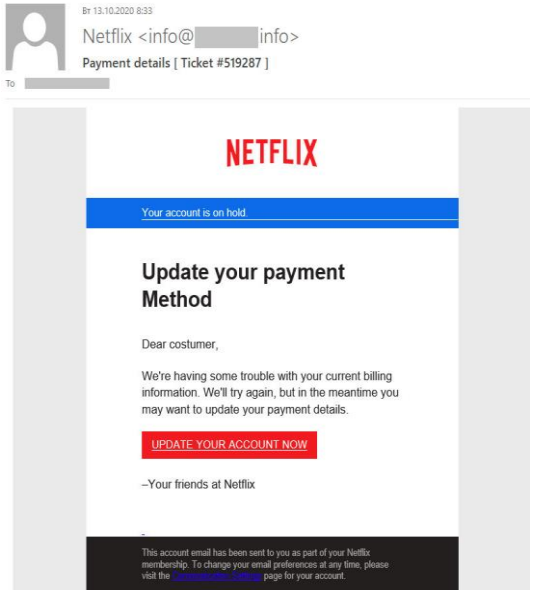
Além disso, a necessidade de leis específicas mostram-se cada vez mais necessárias neste mundo que vem se tornando cada vez mais moderno e globalizado, através de constantes exposições em redes sociais, virtualização de contas, documentos e dados, a popularização da realidade virtual e a nova crescente de inteligências artificiais. O problema da falta de leis específicas, por exemplo, pode ser encontrado em ambiguidades como na questão de fraude eletrônica ou abuso de dados.

2.2 DEFINIÇÃO E EXEMPLOS DE CRIMES CIBERNÉTICOS RELEVANTES E SUA MUTABILIDADE

Os crimes cibernéticos podem ser definidos não apenas como crimes cometidos apenas na *internet*, mas como atividades ilegais que envolvam o uso da tecnologia da informação e comunicação, como por exemplo, fraudes, invasão de sistemas, roubos de informações pessoais ou corporativas, disseminação de *malware* e até mesmo realização de outras atividades ilícitas.

Um exemplo da mutabilidade de cibercrime é o *phishing*, já citado anteriormente, em que os criminosos enviam *emails* conforme mostrado na figura 6, links não seguros ou mensagens falsas que se passam por entidades legítimas para enganar as pessoas a fornecerem informações pessoais, como senhas e números de cartão de crédito, onde este tipo de atividade têm evoluído para contornar medidas de segurança visto que os endereços de *email* agora possuem um sistema de detecção de *spam*, diminuindo os riscos de golpe, buscam atualmente meios de *phishing* por SMS (*smishing*) como por exemplo na figura 7, onde os golpistas usam na maior parte das vezes nomes de bancos ou de operadoras telefônicas, e o *phishing* em redes sociais (*pharming*) que é mostrado nas figuras 8 e 9, e que estão se tornando mais comuns, se passando por *sites* conhecidos, porém com uma leve diferença do original, seja no endereço do *site* ou no conteúdo. Veja-se:

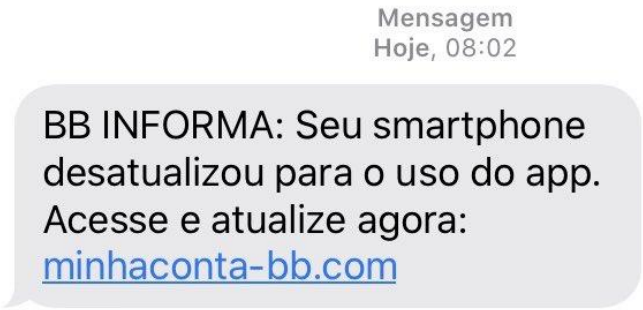
Figura 6: Exemplo de tentativa de *phishing* de serviço de *streaming* via *email*



Fonte: https://www.kaspersky.com.br/blog

Na figura abaixo, podemos ver um exemplo de *smishing*, o tipo de *phishing* via SMS citado anteriormente:

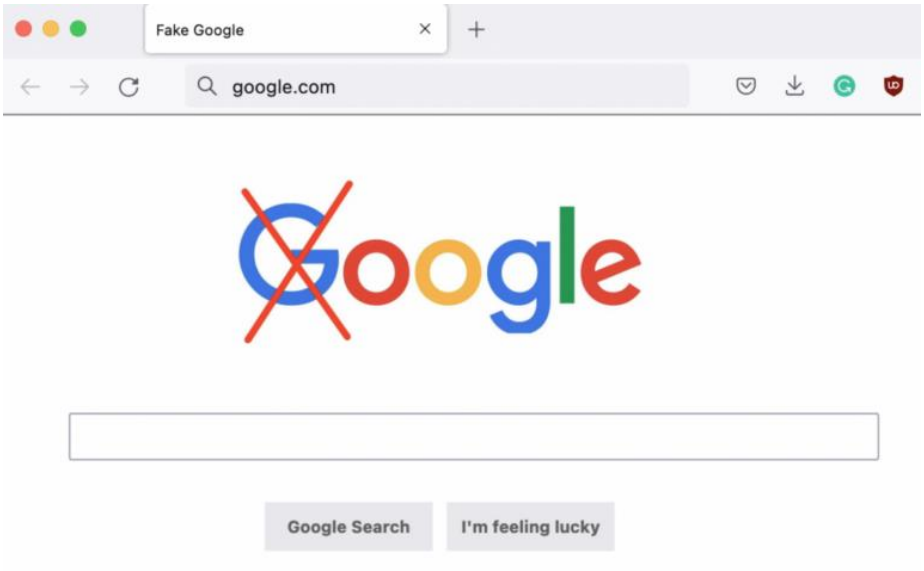
Figura 7: Exemplo de *smishing* usando agência bancária



Fonte: https://www.studio.fm.br

A figura a seguir mostra de forma mais clara como o *pharming* funciona na prática, onde temos um *site* semelhante ao buscador Google, com a única exceção de que possui um X vermelho na letra inicial:

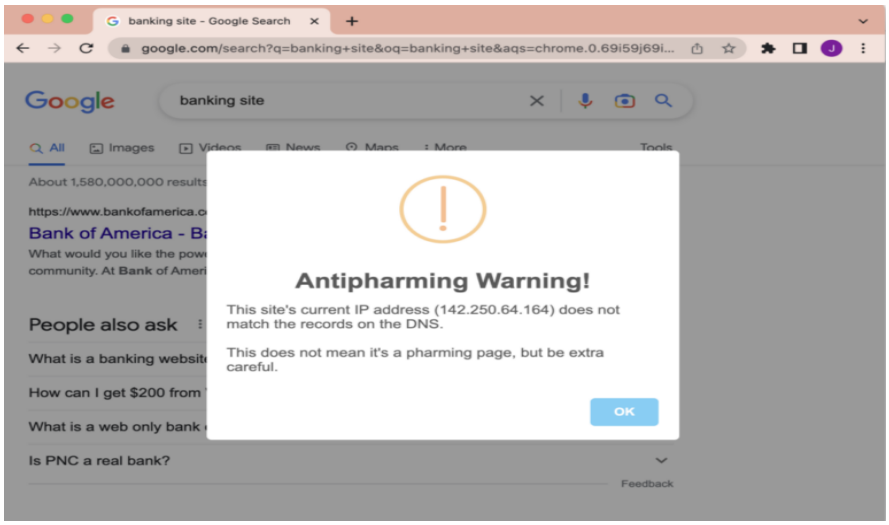
Figura 8: Exemplo de *site* falso de *pharming*, onde simula o *site* da Google, porém com um X cortando a letra “G”



Fonte: https://www.valimail.com

Ainda se tratando do *pharming*, a maioria dos navegadores possuem um sistema de detecção de *pharming* quando o *site* é suspeito, assim como podemos ver na imagem abaixo:

Figura 9: Aviso de detecção de *pharming* da ferramenta DNSSEC



Fonte: https://www.valimail.com

2.3 DISCUSSÃO DAS LACUNAS ATUAIS NA LEGISLAÇÃO BRASILEIRA

Muitas das leis existentes, assim como o Código Penal Brasileiro, foram criadas antes da disseminação da tecnologia digital e podem não ser específicas o suficiente para abordar de maneira adequada alguns tipos de crimes que, mesmo já conhecidos, têm se transferido e popularizado para o meio cibernético. Isso por muitas vezes pode levar à ambiguidade e dificuldade na aplicação da lei. A natureza virtual dos crimes cibernéticos pode apresentar por si só significativos desafios na coleta de evidências digitais, e isso se agrava ainda mais quando o(s) criminoso(s) operam anonimamente ou fora das fronteiras do Brasil, podendo assim, dificultar muito a investigação e a responsabilização dos culpados.

Os crimes cibernéticos representam uma ameaça cada vez mais complexa e globalizada, desafiando as estruturas tradicionais de aplicação da lei. Esses delitos, que variam desde roubo de dados pessoais até ataques cibernéticos, sejam direcionados ou em larga escala contra instituições governamentais e empresas, muitas vezes transcendem fronteiras nacionais com facilidade. E nesse cenário, a cooperação internacional emerge como um elemento crucial para enfrentar essa realidade. A troca de informações entre agências policiais de diferentes países é essencial para rastrear e prender os responsáveis por esses crimes. No entanto, a eficácia dessa cooperação é frequentemente minada pela falta de harmonização das

leis entre as jurisdições. Cada nação possui seu próprio conjunto de regulamentações e procedimentos legais, o que acaba por criar obstáculos significativos durante as investigações que ocorrem entre as fronteiras.

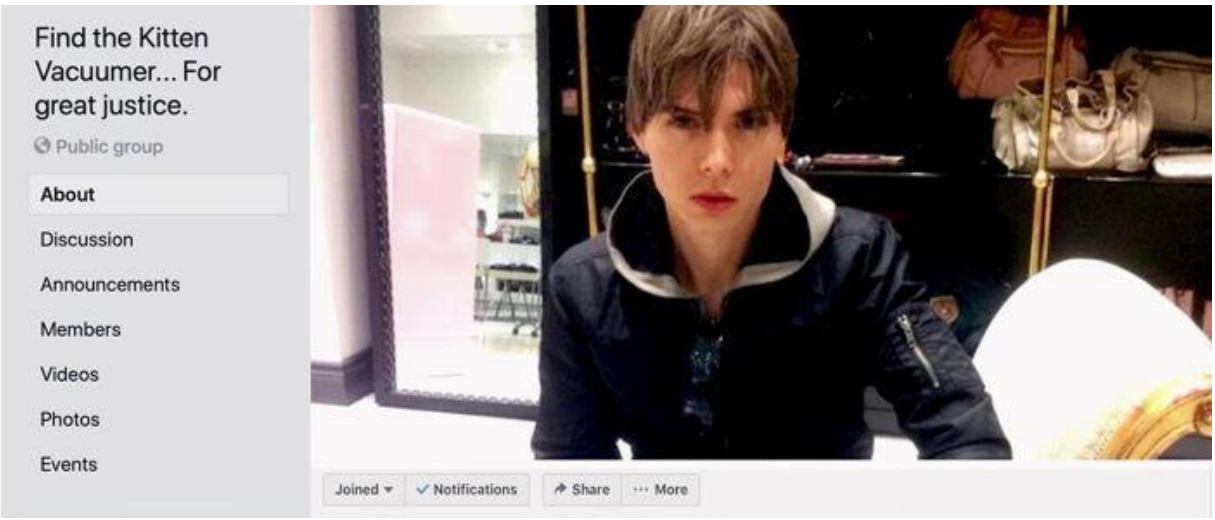
Essa falta de harmonização legal se manifesta de várias maneiras. Primeiramente, a diferença nos sistemas legais, como os princípios de jurisdição e padrões de evidências, podem complicar a coleta e a apresentação de provas em casos que envolvem múltiplos países onde, por exemplo, existem vários cibercriminosos de um mesmo grupo que fazem parte de diferentes países. Além disso, as disparidades nas definições e penalidades para crimes cibernéticos podem resultar em lacunas na aplicação da lei, permitindo que os criminosos escapem de responsabilidades legais devido a diferenças de interpretação legal entre nações envolvidas. Isso acaba criando uma situação na qual os cibercriminosos podem explorar as brechas entre os sistemas legais para evitar a detecção e a punição.

Diante deste cenário, torna-se imperativo promover a cooperação internacional e a harmonização legal para combater eficazmente o cibercrime. Isso requer o estabelecimento de mecanismos formais de cooperação entre as agências policiais de diferentes países, bem como o desenvolvimento de acordos e tratados internacionais que abordem as lacunas legais e promovam uma abordagem unificada para a investigação e o processamento dos cibercrimes. Somente através dos esforços conjuntos e coordenados será possível enfrentar efetivamente essa ameaça transnacional, protegendo indivíduos, empresas e instituições governamentais contra os crescentes riscos associados à atividade criminosa na era digital. O documentário *Don't Fuck With Cats*: Uma Caçada *Online* é uma prova disso, onde em dezembro de 2010, num *post* do *YouTube*, um desconhecido brinca com dois gatinhos em cima de uma cama para, em seguida, coloca-os em um saco plástico e acopla num aspirador de pó numa abertura, fazendo a sucção de todo o ar do saco e que os gatinhos morram sufocados.

Esse *post* sádico acaba viralizando nas redes e desperta a indignação das pessoas que o assistiram e que reagiram, prometendo a punição do culpado. Apesar de tudo, os esforços policiais foram inicialmente inertes, o que mobilizou a criação do grupo do *Facebook "Find the Vacuum Kitten Killer for Great Justice"*, conforme na figura 10, em que devido aos esforços da comunidade para resolver o crime, um grupo de proteção animal também ofereceu um prêmio de 5000 dólares para quem identificasse o responsável pelo delito, e que após vários esforços conjuntos de

pessoas, e após outros acontecimentos e *post* relacionados ao "*Vacuum Kitten Killer*", as autoridades policiais conseguiram, quatro anos após, localizar e prender o criminoso. Mas vale a pena ressaltar que as autoridades policiais internacionais se mobilizaram apenas após a morte do estudante Jun Lin, e que foi correlacionado ao crime e rastreado com ajuda dos diversos justiceiros virtuais que sanaram o crime. O grupo de *Facebook* ainda existe até os dias atuais, conforme mostra a figura 10. Veja-se:

Figura 10: Grupo de Facebook "*Find the Kitten Vacuumer… For great justice"*



Fonte: https://www.facebook.com

A rápida evolução da tecnologia na era digital tem proporcionado uma série de benefícios e oportunidades, mas também tem apresentado desafios significativos para a aplicação da lei e a legislação no meio cibernético. À medida que novas tecnologias emergem e se desenvolvem, surgem também novas formas de cibercrimes, que muitas vezes superam a capacidade das leis existentes de acompanhá-las e regulá-las de forma adequada. Questões como proteção de dados, inteligência artificial, *blockchains* e *Internet* das Coisas (IoT) são apenas alguns exemplos de áreas em que a legislação pode não estar totalmente preparada para lidar de maneira eficaz.

A proteção de dados, por exemplo, tornou-se uma preocupação central com a proliferação de informações pessoais armazenadas digitalmente e as crescentes ameaças de violações de dados e roubo de identidade. A legislação de privacidade de dados existente pode ser confusa, defasada ou até mesmo pode não ser suficiente para abordar desafios complexos apresentados por novas tecnologias

em vista da rápida evolução e mutabilidade da tecnologia, especialmente considerando as crescentes preocupações com a privacidade e segurança dos dados dos usuários.

Da mesma forma, o uso crescente da inteligência artificial em uma variedade de contextos levanta questões éticas e legais sobre responsabilidade, discriminação algorítimica e trransparência. A legislação atual pode não oferecer diretrizes claras sobre a maneira como essas tecnologias devem ser regulamentadas e responsabilizadas por seu impacto potencial na sociedade.

Além disso, as *blockchains*, que é uma tecnologia de banco de dados digital que funciona como um livro-razão distribuído e descentralizado que registra transações de forma segura e transparente, usando uma rede de computadores interconectados. Cada transação é registrada em um bloco de informações, que é criptograficamente vinculado aos blocos anteriores, formando uma cadeia contínua de registros (origem do nome *blockchain*). Sua descentralização garante segurança e transparência, pois as transações são verificadas e validadas pelos participantes da rede. A *blockchain* é amplamente utilizada em diversas áreas, desde criptomoedas até contratos inteligentes, devido à sua confiabilidade e resistência a fraudes. No entanto, apesar de sua promessa de segurança e transparência, também apresentam desafios regulatórios, especialmente no que diz respeito a questões de conformidade, identificação e rastreabilidade de transações. A legislação existente pode não estar equipada para lidar adequadamente com a complexidade desses sistemas descentralizados e suas implicações legais.

Ainda tratando do mesmo tópico, a *Internet* das Coisas (IoT) introduz uma série de preocupações em relação à segurança cibernética, privacidade e responsabilidade legal. A interconexão de dispositivos inteligentes em redes amplas podem criar vulnerabilidades significativas que podem ser exploradas por criminosos cibernéticos. No entanto, a legislação atual pode não ser suficientemente abrangente para lidar com essas questões emergentes de forma eficaz.

Em face desses inúmeros desafios, é fundamental que os legisladores estejam atentos às evoluções tecnológicas e trabalhem para atualizar e adaptar a legislação existente para garantir que ela permaneça relevante e eficaz na proteção dos direitos individuais, da segurança cibernética e da integridade dos sistemas tecnológicos em rápida evolução. O que por sua vez acaba exigindo uma abordagem proativa e colaborativa entre governos, empresas, sociedade civil e especialistas em

tecnologia para desenvolver políticas que promovam a inovação responsável e a proteção dos interesses públicos.

Algumas críticas à legislação existente argumentam que as penalidades para crimes cibernéticos podem ser inadequadas, não refletindo a gravidade dos danos causados ou falhando em dissuadir eficazmente os criminosos de se envolverem em atividades ilícitas. A complexidade das infrações cibernéticas que muitas vezes transcende as fronteiras geográficas e jurisdicionais dificultam a aplicação consistente e eficaz da lei.

Em muitos casos, as sanções impostas por infrações cibernéticas podem parecer desproporcionais em relação aos danos causados, especialmente quando comparadas a crimes tradicionais. Isso pode ser atribuído, em parte, à dificuldade de quantificar os prejuízos associados aos crimes cibernéticos, que muitas vezes envolvem perdas financeiras, violações de privacidade e danos à reputação que podem ser difíceis de mensurar.

Além disso, a natureza transnacional dos crimes cibernéticos apresenta desafios adicionais no que diz respeito à aplicação da lei e à imposição das penalidades efetivas. A cooperação internacional entre agências de aplicação da lei e governos é essencial para essa questão, mas nem sempre é fácil de alcançar devido a diferenças em sistemas legais, procedimentos de investigação e políticas de extradição.

A proteção dos direitos individuais também surge como uma preocupação central no contexto da aplicação da lei em casos de crimes cibernéticos. O uso de técnicas de vigilância digital e monitoramento *online* para combater atividades criminosas levanta questões sobre privacidade e liberdades civis, no entanto essas técnicas ainda apresentam sua dualidade, podendo ser usadas tanto para fazer justiça, assim como no caso anterior do *Vacuum Kitten Killer*, como no caso de inúmeros cibercrimes já citados. É fundamental garantir que os métodos utilizados para investigar e processar infratores cibernéticos respeitem os direitos fundamentais dos cidadãos, evitando abusos e garantindo o devido processo legal.

Para abordar essas questões complexas, é necessário um enfoque multidisciplinar que envolva não apenas a aplicação rigorosa da lei, mas também o desenvolvimento de políticas públicas que promovam a educação em cibersegurança, o fortalecimento das capacidades de investigação digital e a cooperação internacional

entre as partes interessadas. Somente assim será possível avançar na proteção dos direitos individuais e na promoção de um ambiente digital seguro e confiável.

3 – A TEMÁTICA CYBERPUNK COMO ESPELHO DA REALIDADE ATUAL E POSSÍVEIS EVOLUÇÕES

3.1 – EXPLORANDO OS PRINCIPAIS ELEMENTOS DO UNIVERSO CYBERPUNK

A temática *cyberpunk* já não é algo recente na nossa cultura, através de filmes, da literatura, jogos, arte, entre outros. No entanto, após o jogo *Cyberpunk 2077* se tornar viral nas redes, catapultando o subgênero do retrofuturismo para o *mainstream*, o tema em si ganhou uma relevância ainda maior na cultura. Muitas obras com a temática têm se tornado cada vez mais populares, pela temática relevante e atual, pela estética inovadora e futurista, ou pelas inúmeras possibilidades dentro deste subgênero da ficção científica.

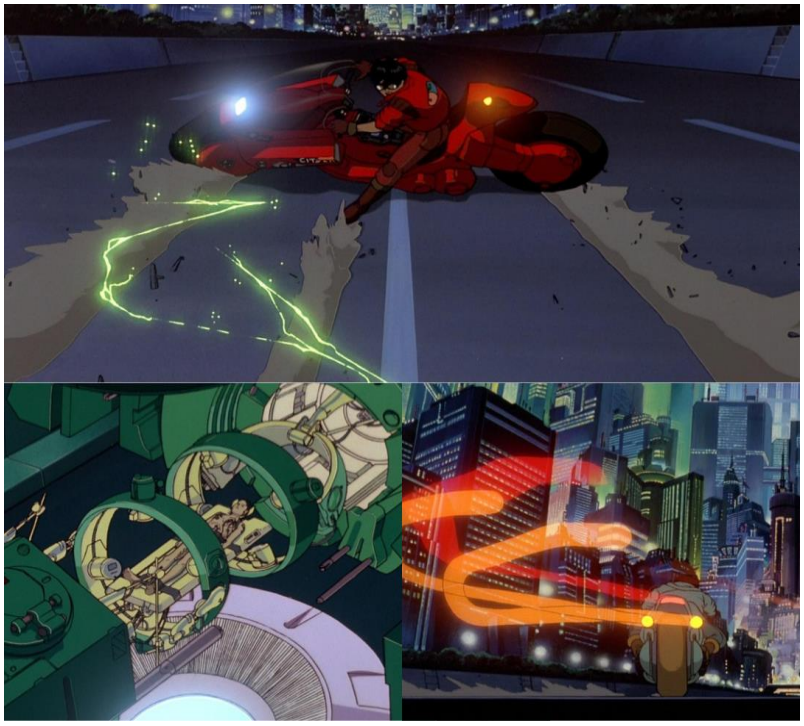
Conforme a matéria "*Cyberpunk* além de 2077: Entenda o que significa o gênero" (2021) em 1951 com a obra "A Fundação", de Isaac Asimov, a temática começa a ter uma certa relevância, mas somente em 1968 com "Androides Sonham com Ovelhas Elétricas?", mais conhecido como "*Blade Runner*" de Phillip K. Dick é que o subgênero começa a ser moldado e tomar uma maior força. Ainda assim, apenas em 1980 o nome *Cyberpunk* surge, com Bruce Bethke, que utilizou o nome para batizar seu conto em 1983 e abraçado por fãs do gênero, como William Gibson, com sua obra na figura 11, o romance Neuromancer em 1984, obra essa que previu exatamente o surgimento da *internet* e a maneira como ela se tornaria algo popular e de amplo acesso, dando assim, a verdadeira visibilidade para a temática e tornando-se a obra precursora do movimento, que sem muito tardar, se tornou muito popular no Japão após o colapso da bolha financeira e imobiliária na década de 1990 (失われた10年 *Ushinawareta Jūnen*) dando origem a grandes obras como *Akira* e *Ghost in the Shell*, que são os dois pilares da animação japonesa da época, sendo títulos que carregam muitas similaridades incluindo a temática *cyberpunk*, conforme a figura 12. Veja-se:

Figura 11: Livro Neuromancer de William Gibson

Fonte: https://www.amazon.com.br

A imagem do filme *Akira*, lançado em 1991, ilustra a atmosfera característica do universo *cyberpunk*, destacando a profusão de tecnologia, *LEDs* e cores vibrantes, contrastando vividamente com o cinza urbano da cidade. Veja-se:

Figura 12: Imagens do filme Akira (1991)



Fonte: https://imgur.com

O Japão foi sem dúvidas um dos maiores pilares para a definição atual da estética e temática *cyberpunk* que conhecemos atualmente: o gênero que *sci-fi* que se passa sempre em um futuro muito próximo e possui o lema *"High tech, Low life*" (alta tecnologia, baixa qualidade de vida), e onde uma das marcas mais importantes do gênero se encontra no fato dos autores da temática sempre tentam prever um futuro da maneira mais pessimista, niilista possível, pegando os problemas da sociedade atual e extrapolando para um limite distópico, ou seja, onde tudo dá errado, onde as questões sociais e tecnológicas, questionando o avanço da tecnologia e como ela se tornaria invasiva, normalmente saindo do controle dos seres humanos, levantando questões sociais e filosóficas. E é possível ver nessas obras, mesmo em obras originárias como o *Blade Runner* ou *Ghost in the Shell* temáticas e enfoques ainda relevantes para a nossa sociedade atual.

Essas narrativas costumam se passar em grandes metrópoles futuristas, com cores brilhantes e luzes neon por todas as partes, mas que sofrem com a pobreza e a criminalidade ao serem analisadas de maneira mais detalhada. Normalmente tratam suas histórias com megacorporações como vilãs, onde o protagonista normalmente busca infligir-lhes prejuízos normalmente sem qualquer ganho pessoal com tais atos, daí o motivo do "*punk*" em *cyberpunk*. além disso, as obras sempre tentam mostrar um ambiente que mescla o virtual e o real, onde a fronteira entre eles se perde, com um enfoque no lado sombrio e sinistro onde computadores dominam todos os aspectos da vida cotidiana, as megacorporações substituíram o centro de poder do Estado

3.1.1 Visão geral da abordagem do universo cyberpunk como lente analítica

A temática *cyberpunk* por se tratar de um mundo distópico em um futuro próximo, abre portas para várias possibilidades e alternativas que tratem de ameaças digitais, assim como veremos mais detalhadamente em breve alguns títulos que não se encontram longe da nossa realidade, assim como o caso do já citado *Neuromancer*, que de certa forma, conseguiu prever como seria a popularização da *internet* nos dias atuais.

Desde 1980 a preocupação da crescente modernização digital tem sido relevante e motivo desencadeador de várias obras distópicas famosas, não bastando

as obras já citadas, temos por exemplo obras também como “De Volta para o Futuro”, “Exterminador do Futuro”, “Eu, Robô”, “A.I. - Inteligência Artificial”, por exemplo. No entanto, essas obras tratam de outro subgênero da ficção científica, denominada de *Cassete Futurism* onde possui um foco mais voltado para a década de 80, com a estética de VHS, lasers, computadores e sintetizadores, sem necessariamente se tratar de distopias, enquanto o subgênero *cyberpunk* concentra seu foco nas megacorporações, hackers, futuro próximo, cibernética e distopias conforme explica o *site UpdateorDie!*.

Uma forma de diferenciá-los seria comparar duas grandes obras de cada gênero: “De Volta para o Futuro” e “*Neuromancer*”. Onde na primeira obra focou na popularização de tecnologias de uso pessoal, como ligações por vídeo, a biometria, carros voadores, tela plana, casas inteligentes, entre outros. Enquanto isso a obra *Neuromancer* nos traz a ideia de computador pessoal, onde os denominados *decks* são computadores pessoais usados para acessar a *matrix* (termo também emprestado para o filme de 1999), um ciberespaço, uma realidade virtual onde as pessoas vivem em rede, assim como a atual *web* que conhecemos hoje, juntando recursos visuais e textuais. Ainda se tratando do mesmo livro, o personagem principal é um *cowboy*, contratado para roubar dados, quebrar *firewall* ou realizar complicadas invasões nos sistemas da *matrix*, esse *cowboy*, que hoje podem ser chamados de *hacker* por realizarem tarefas similares.

Além disso há mais duas curiosidades no livro de Gibson, que se trataria das carteiras digitais, assim como o *Apple Pay* ou *Google Pay* que conhecemos hoje, que fazem a mesma função. Durante a estadia numa colônia espacial, os personagens recebem chips que armazenam a identidade e todo seu dinheiro, de modo que apenas de aproximar o chip em leitores espaciais, eles conseguiriam realizar as transações. Além disso, mesmo após 34 anos do lançamento da, os personagens são contratados por uma inteligência artificial para aumentar suas capacidades, porque a empresa que a programou não deu total poder para o programa de computador, com medo de que ela se rebelasse, assunto este que se encontra presente até os dias atuais e ainda um medo de muitas pessoas.

3.2 ANÁLISE DE OBRAS-CHAVE: EXAMINANDO AS LIÇÕES DO UNIVERSO CYBERPUNK

A simples existência do gênero *cyberpunk* acaba por gerar várias reflexões e dúvidas sobre as possibilidades futuras. Mesmo que se trate de uma distopia, as motivações para a criação da mesma é baseada em nossa realidade, mesmo que ainda se trate de um certo exagero da realidade, não deixa de ser uma possibilidade e às vezes até mesmo um alerta.

Um exemplo claro de como o universo *cyberpunk* nos traz lições e reflexões para a nossa realidade é o já citado *Neuromancer*, que aborda a inter-relação entre máquinas e humanos, a realidade virtual, a dependência da tecnologia e questões de segurança. A obra por si só levantou questões sobre bancos de dados, o citado ciberespaço, na obra - *"*Ciberespaço… uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando..." trouxe a importância da segurança da informação que passou a ser analisada apenas dos dias atuais, tratando também sobre o problema dos ciberataques, da vigilância em massa e a importância do direito à privacidade, como por exemplo, podemos ver no trecho a seguir retirado da própria obra - “Toda IA já construída possui um rifle eletromagnético apontado e amarrado à sua testa".

Os debates sobre esses temas têm implicações legais significativas em áreas como leis de proteção de dados, que poderiam servir para complementação, por exemplo, na criação da nossa LGPD. Além disso, há também discussões sobre a necessidade de uma legislação *anti-hacking* mais abrangente, ao invés de apenas mudar um único artigo do Código Penal Brasileiro, como é o caso do Artigo 154-A. No entanto, surge nos últimos dois anos um problema crucial: a falta de regulamentação sobre o uso das Inteligências Artificiais (IAs) após sua popularização, bem como sobre a utilização e armazenamento dos dados gerados por elas para sua adaptação.

A maioria das obras desse gênero acabam tratando de problemas que poderiam facilmente acontecer na vida real, sendo assim, as obras já tratadas ou que ainda serão tratadas serviriam como reflexões para uma prevenção de possíveis catástrofes ou prejuízos. Um exemplo disso seria *Snow Crash* de Neal Stephenson que examina economia digital e anarquia na *internet*, por exemplo, e que nos oferece

um escopo sobre a regulamentação da *internet*, além da responsabilidade por conteúdo online, que se já houvesse uma manutenção preventiva na legislação, poderia ter evitado o Caso Choquei em que aconteceu em dezembro de 2023 que apenas trouxe a necessidade de leis após a morte de Jessica Canedo.

3.2.1. Discussão detalhada de obras como *Mr. Robot*, *Watch Dogs 2* e *Lain Serial Experiments*

Na série de televisão *Mr. Robot*, o protagonista Elliot Alderson, um jovem que é programador e trabalha como engenheiro de segurança virtual na empresa *Allsafe* e que também atua como um *hacker* vigilante na noite, onde com suas espionagem às pessoas, acaba por realizar denúncias e desmascarar criminosos na sociedade, a verdadeira trama da série acontece após uma tentativa *hacker* de invasão à *Allsafe*, onde um grupo *hacker* extremista denominado de *fsociety* tenta por meio dessa invasão recrutá-lo para destruir a firma em que trabalha.

Com a premissa de uma sociedade onde a megacorporação *E-Corp* toma conta do Estado no lugar do governo, *Allsafe* é uma empresa particular, que toma conta de grande parte da segurança de dados que envolve a *E-Corp*, com o recrutamento de Elliot para a *fsociety*, o grupo extremista tem o fundado objetivo de destruir todos os dados da megacorporação, onde ao apagar esses dados, todas as pessoas estariam “livres” da empresa corrupta, pois neste mundo virtual, suas dívidas deixariam de existir, seus registros seriam excluídos, e as ações e verbas da empresa entrariam em colapso, tornando o governo do país uma verdadeira anarquia. Essa série que aborda os temas de identidade digital, segurança cibernética, conflitos éticos, além de corporações corruptas e instituições financeiras, destaca questões de segurança da informação, nos mostrando mais uma vez que a maior possibilidade de falha de segurança é sem dúvida o ser humano, também levanta questionamentos sobre o *hacking* ético frente ao cibercrime e as implicações legais do ativismo digital. Também levanta preocupações sobre a privacidade dos dados dos usuários e o papel do governo na proteção contra ameaças cibernéticas.

Em *Mr. Robot* é destacado mais uma vez uma necessidade iminente de uma legislação *anti-hacking* para podermos lidar de forma rápida e eficaz com os ataques cibernéticos e problemas de invasão, não apenas cometidos contra pessoas, mas contra empresas, países, órgãos, etc.

Já na obra *Serial Experiments Lain*, apesar de se tratar de uma animação pouco conhecida, bastante antiga e bem exagerada em alguns aspectos, acaba levantando questões sobre o anonimato na *internet*, liberdade de expressão *online*, crimes virtuais e a responsabilidade legal dos provedores de serviços de *internet*, além de abordar a preocupação dos desafios legais associados à proteção da identidade digital. A animação gira em torno de uma adolescente introvertida, que se conecta a uma rede global de computadores e mergulha em um mundo virtual complexo com o nome de *wired*. Em vários episódios da animação são mostrados casos de *hacking* e invasões de sistemas na *wired*, causando danos aos usuários. Por exemplo, em uma cena, um personagem é alvo de um ataque cibernético que compromete sua identidade digital e afeta sua vida real. Esses incidentes levantam questões sobre a responsabilidade dos provedores de serviços de *internet* em proteger seus usuários contra ameaças cibernéticas e garantir a segurança de suas plataformas *online*.

Já no jogo *Watch Dogs 2*, é retratado um grupo de *hackers* que se unem para expor atividades corruptas de megacorporações e agências governamentais, destacando questões como vigilância em massa, que é realizado por essas agências, invasão de privacidade e os limites do poder das grandes empresas. Esta obra nos dá *insights* sobre cibercrimes, *hacking* ético, legislação e proteção de dados e os desafios que são enfrentados pelas autoridades ao regular o uso de tecnologias em atividades criminosas e ativismo digital. A história do jogo segue o grupo *hacker* denominado de *DedSec*, liderado pelo protagonista Marcus, em uma luta contra o sistema corrupto e as megacorporações que controlam a cidade de São Francisco. A história do protagonista começa quando Marcus é acusado injustamente pelo sistema de vigilância centralizado, com nome de *ctOS 2.0*, de um crime que não cometeu, a partir de então, para provar sua inocência e lutar contra a opressão do sistema, ele se une ao grupo *DedSec* para desmascarar a verdade por trás das operações corruptas dessas megacorporações e expor os segredos sujos dos poderosos por trás delas.

Durante todo o progresso do jogo, realiza-se uma série de missões que envolve *hackear* dispositivos eletrônicos e sistemas de seguranças para coletar informações que sejam comprometedoras para expor a corrupção. O grupo enfrentam várias ameaças ao longo da história, incluindo empresas de tecnologia gananciosas, grupos de criminosos e agências governamentais que buscam manter o controle da população. *Watch Dogs 2*, assim como no Caso *Pegasus* visto anteriormente, nos traz preocupações sobre a invasão de privacidade e a vigilância em massa por meio de

tecnologias de monitoramento, como o citado sistema *ctOS 2.0*, que por sua vez levanta questões éticas sobre os limites do monitoramento governamental e corporativo e os direitos individuais à privacidade. Além disso, Marcus e o grupo *DedSec* se envolvem em atividade de *hacking* para alcançar seus objetivos, o que levanta questões sobre a legalidade e a ética *hacking*, dessa forma, o jogo nos mostra uma diferença entre o *hacking* ético, usado para expor a verdade e lutar contra a injustiça, e cibercrimes, realizados por interesses egoístas ou maliciosos. E por fim, a história também destaca consequências negativas do desenvolvimento não regulamentado da tecnologia, especialmente quando nas mãos de megacorporações gananciosas. Isso destaca a necessidade de regulamentações mais rígidas para proteger os consumidores e garantir a segurança e privacidade de dados dos indivíduos, que por sua vez traz em fóruns *onlines* como *Reddit* a forma em que o jogo e a GDPR europeia se entrelaçam, de forma que a lei proíbe as companhias de obter e compartilhar dados sem o conhecimento e consentimento dos usuários, tornando de certa forma a distopia do universo *Watch Dogs* impossível de acontecer na União Europeia devido à sua lei preventiva sobre a coleta de dados.

Aqui, em similaridade com *Mr. Robot* vemos mais uma vez a necessidade de uma lei *anti-hacking*, porém através de uma diferente perspectiva, podendo assim ver de diferentes maneiras como a legislação poderia afetar o cotidiano. Não sendo o bastante, o jogo também nos mostra a maneira como a supervigilância também pode se tornar um grande problema civil.

3.2.1.1 Identificação de momentos em que as obras apresentam desafios similares à falta de regulamentação em crimes cibernéticos

As obras deste gênero frequentemente exploram os desafios resultantes da ausência da regulamentação de cibercrimes. Um exemplo notável, que não é possível deixar de fora e que merece várias citações, é novamente, *Neuromancer*, onde os *hackers* possuem habilidades avançadas para invadir sistemas corporativos e governamentais sem serem detectados. A falta de regulamentação eficaz permite que esses *hackers* operem livremente, comprometendo a segurança dos dados e causando danos significativos, assim como acontece na maioria dos casos de ataques *ransomware* no mundo todo. Por exemplo, o protagonista, Case, é recrutado para realizar um grande golpe de *hacking*, explorando as falhas de segurança existentes

de uma megacorporação. Isso destaca como a ausência de regulamentação em cibercrimes permite que indivíduos explorem vulnerabilidade em sistemas digitais para benefício próprio.

Outra obra que aborda o tema cibercrime é *Blade Runner*, dirigido Ridley Scott e inspirado no livro “Androides Sonham Com Ovelhas Elétricas?” de Philip K. Dick, onde questões sobre a humanidade dos androides e a identidade digital são exploradas. A falta de uma regulamentação eficaz leva a conflitos sobre os direitos e responsabilidades das inteligências artificiais, tema que é extremamente atual e necessário, assim como a segurança cibernética. Por exemplo, no filme, os replicantes, androides criados para servir aos humanos, buscam liberdade e reconhecimento como seres conscientes, levantando questões sobre sua proteção legal e liberdade. Também vale a pena citar o jogo *Detroit: Become Human* que também desperta a mesma exata temática sobre os androides e seus direitos.

A já citada animação *Serial Experiments Lain* também aborda esses temas quando a protagonista Lain se conecta à *Wired* e explora questões de identidade *online* e anonimato na *internet*. A falta de regulamentação adequada resulta em desafios relacionados à privacidade *online* e crimes virtuais. Por exemplo, Lain se depara com gangues virtuais que operam sem restrições dentro do ciberespaço, aproveitando-se da falta de regulamentação para realizar atividades criminosas, vale citar também que os mesmos criminosos se reuniam anonimamente em *chats* para poderem discutir sobre diversos assuntos, onde pode-se fazer um paralelo à atual *Dark Web* que conhecemos atualmente.

Por fim, a série *Mr. Robot*, aborda também a temática através do protagonista Elliot Alderson, um *hacker* ético altamente habilidoso que se envolve em atividade de *hacking* para expor corporações corruptas e instituições financeiras, um pouco similar ao caso que se passa no universo do jogo *Watch Dogs*. A falta de regulamentação eficaz permite que essas corporações operem de forma opressiva, enquanto Elliot e sua equipe buscam expor a verdade e promover a justiça, mesmo que através de invasões de dados, trazendo mais uma vez a questão sobre o *hacking* ético. A série também destaca questões como vigilância em massa, invasão de privacidade e a ética do *hacking*, tal qual a franquia de jogos *Watch Dogs*.

Os exemplos citados ilustram apenas uma parcela de como as obras *cyberpunk* destacam os desafios causados pela falta de regulamentação em crimes cibernéticos e ressaltam a importância de desenvolver leis e políticas eficazes para

lidar com os avanços tecnológicos e proteger a sociedade digital, antes que desastres possam acontecer.

3.2.1.2 Relacionando as dificuldades de regulamentação das obras com possíveis problemas atuais e futuros para a regulamentação

O principal problema para regulamentar algo com base na análise de uma ficção é que nem sempre se trata de algo acurado com a realidade. A possibilidade de uma previsão ser precisa e correta é baixa, além do grande problema principal tratar da questão da demora na criação, positivação e efetividade da lei.

Ainda nessa questão, é importante ressaltar novamente a forma como o universo *cyberpunk* geralmente apresenta cenários distópicos, que podem distorcer a percepção da realidade e dificultar a aplicação prática das regulamentações propostas. No caso do *cyberpunk*, acaba podendo retratar uma tecnologia ou situação social de forma exagerada ou simplificada na grande maioria das vezes, o que torna desafiador extrapolar essas representações para o contexto real.

Outra dificuldade está na própria natureza dinâmica da sociedade e da tecnologia. As obras de ficção são frequentemente escritas em um momento específico e acabam refletindo em preocupações e perspectivas desse certo período. No entanto, a realidade pode evoluir de maneiras imprevisíveis, tornando as regulamentações baseadas nessas obras rapidamente obsoletas ou inadequadas para lidar com novos desafios, mostrando assim necessário a ajuda de especialistas em ambas as áreas, do direito e da tecnologia, para a regulamentação de forma adequada.

Além disso, a implementação de regulamentações muitas das vezes envolve uma complexa interação entre diferentes partes interessadas, como legisladores, reguladores, empresas e grupos da sociedade civil. Diferentes interpretações das obras *cyberpunk* e suas implicações podem levar a debates acalorados e atrasos no processo de uma regulamentação ou outra.

Diante dessas dificuldades, é crucial adotar abordagens mais holísticas e baseadas em evidências para a regulamentação, que considerem não apenas as representações das obras de ficção, mas também em dados empíricos, análises de impactos e consultas públicas. Isso pode ajudar a garantir que as regulamentações

sejam eficazes, proporcionais e adaptáveis à medida que a sociedade e a tecnologia continuam a evoluir.

Para avançar de maneira mais profunda na compreensão das dificuldades de regulamentação dessas obras, é importante considerar também as nuances das narrativas ficcionais e como elas podem influenciar a percepção pública e a tomada de decisão política. As obras *cyberpunk* muitas vezes exploram questões éticas, morais e filosóficas de maneiras que desafiam as convenções sociais e políticas, levando o público a questionar suas próprias crenças e valores.

Essas narrativas complexas podem apresentar dilemas éticos e situações hipotéticas extremas que não tem equivalência direta na realidade. Tornando dessa forma, problemático extrair políticas ou regulamentações diretamente dessas narrativas, pois ignoram o contexto único e as nuances das obras de ficção.

Para finalizar, enquanto as obras do universo *cyberpunk* podem fornecer *insights* valiosos sobre questões sociais, éticas e tecnológicas, é essencial abordá-las com um olhar crítico, cauteloso e profissional ao considerar sua relevância para a regulamentação. Isso envolve não apenas uma análise cuidadosa das narrativas em si, mas também um entendimento amplo do contexto social, político e cultural no qual essas obras são produzidas e consumidas em relação ao contexto da realidade atual em que se vive.

3.3 REFLEXÃO SOBRE COMO O UNIVERSO CYBERPUNK PODE OFERECER INSIGHTS PARA A ABORDAGEM DAS LACUNAS LEGAIS

Uma vez entendendo os perigos da análise de forma errada pode causar e como uma legislação mal elaborada pode proporcionar diversas brechas e problemas, além do aumento dos casos de cibercrime, cabe também oferecer *insights* sobre como combatê-las de maneira eficaz.

Já que a obra *Neuromancer* vem sendo citada no decorrer deste estudo, vale destacar que é possível observar uma divisão gritante entre os ricos que habitam em espaços de alta tecnologia e os pobres que lutam para sobreviver nas ruas caóticas e sujas, a seguinte citação deixa isso ainda mais claro "Poder, no mundo de Case, significava poder corporativo. As *zaibatsus*, as multinacionais que davam forma ao curso da história humana, haviam transcendido antigas barreiras. Vistas como organismos, haviam adquirido uma espécie de imortalidade." Esta disparidade, por

exemplo, ressalta como as leis muitas vezes beneficiam a elite, deixando os menos privilegiados em desvantagem, demonstrando assim um possível problema de desigualdade socioeconômica amplificada.

Já o mangá *Ghost in the Shell de* Masamune Shirow ilustra um universo com um ambiente completamente envolto de tecnologia, de forma que a tecnologia avançada pode ser usada para explorar as lacunas legais. Um exemplo disso são corporações poderosas que usam tecnologias de vigilância e *hackers* habilidosos que exploram brechas de segurança, destacando a necessidade de leis atualizadas para proteger os direitos individuais e a privacidade em um mundo digitalizado. Apesar disso, a obra aborda na maior parte do tempo a linha entre humanos e máquinas, que acaba por se mesclar, de maneira a deixar confusa, e mesmo que não seja igual é de fato hoje em dia, com a ajuda da inteligência artificial, está cada vez mais difícil notar e diferenciar o que é criado por humanos ou por IAs, o mangá nos traz algumas citações interessantes:

> Se uma proeza tecnológica é possível, o homem a fará. Quase como se estivesse enraizado em nosso âmago.
>
> A linha entre humanos e máquinas está se tornando cada vez mais borrada.
>
> Em um mundo consumido pela tecnologia, é importante lembrar de nossa própria humanidade.
>
> Todos estamos conectados, quer percebamos ou não.

Na obra *Blade Runner* de Philip K. Dick, o ambiente completamente futurista e sombrio retrata uma sociedade onde a corrupção é endêmica e as instituições legais são facilmente corrompidas por interesses poderosos. Isso acaba por enfatizar a importância da transparência e da aplicação imparcial da lei para evitar lacunas na justiça. Esse mesmo tema também é reforçado na animação japonesa *Psycho-Pass*, onde o governo usa de tecnologias de vigilância extrema para detectar e prevenir crimes antes que aconteçam, inclusive prendendo ou executando pessoas como maneira preventiva de combate à criminalidade, com base em exames cerebrais, um exame nacional onde através dela determinaria até mesmo as melhores possibilidades de profissão para cada cidadão. No entanto, apenas o governo tem acesso a todas as informações dos cidadãos, mantendo a sociedade no escuro sobre como as decisões são tomadas, até que uma falha no sistema é descoberta, causando

sérios problemas. Esses dois exemplos, em ambos os casos, destacam a corrupção e a falta de transparência no sistema.

No livro *Snow Crash* de Neal Stephenson é apresentado grupos marginalizados que se rebelam contra o sistema estabelecido, destacando as lacunas legais e sociais que permitem a opressão persistir. A resistência desses grupos destaca a necessidade de reformas legais e sociais para abordar o tema das desigualdades subjacentes e garantir a justiça para todos. Ainda nessa temática, a já citada série de televisão *Mr. Robot*, nos dá um *insight* de uma sociedade distópica onde megacorporações controlam tudo, sendo um novo tipo de Estado, e que através da opressão da megacorporação *E-Corp* que controla tudo, acaba por gerar o grupo rebelde *fsociety* e que acaba ganhando apoio da grande massa da sociedade e gerando uma verdadeira anarquia no universo da série. Além da série também reforçar a questão de reformas legais e sociais, rebelião e resistência, também destaca a possibilidade de controle de massa da grande população, além de uma tomada de poder maior e mais forte que o governo.

Na série de televisão *Altered Carbon* de Richard K. Morgan, assim como no anime *Serial Experiments Lain*, as questões éticas relacionadas à tecnologia são exploradas, como privacidade e violações dos direitos humanos devido a lacunas legais. Enquanto *Altered Carbon* também aborda a manipulação genética e inteligência artificial, *Serial Experiments Lain* foca no problema da privacidade excessiva, rebeliões e os limites entre o mundo físico e o digital, mas ambos destacam a importância de uma abordagem ética e responsável no desenvolvimento e na regulamentação tecnológica. Essas obras constantemente questionam quais os limites entre o mundo físico e o digital, apesar de suas nuances e diferenças, até mesmo entre as épocas, ressaltando a necessidade de considerar cuidadosamente as implicações éticas em um ambiente tecnológico em constante evolução.

CONSIDERAÇÕES FINAIS

É importante sempre destacar não apenas as possibilidades e a amplitude dos crimes cibernéticos, é fato que estes delitos já são comuns e até bem conhecidos nos dias atuais. No entanto, o verdadeiro problema encontra-se não apenas na nossa falta de legislação, pois também há brechas nas legislações internacionais, mas sim, na falta da punição e prevenção contra cibercrimes, visto que, a maioria dos crimes visam pessoas mais vulneráveis e com pouco conhecimento tecnológico, e uma vez que desamparadas, buscam sanar seus problemas na justiça, que no entanto é muita das vezes, morosa e até mesmo falha, sendo incapaz de solucionar ou reparar danos por si só. Assim, a própria temática traz à tona os justiceiros virtuais, que estão sempre em busca de criminosos na *internet*, para poder ajudar e amparar vítimas de golpes *online*, da mesma forma que, também desmascaram corrupções e diversos tipos de crimes cometidos na *internet*. E ainda por cima, tudo conforme é previsto e muito bem representado nas obras *cyberpunk* em sua forma mais explícita e crua tanto da forma como atuam os cibercriminosos como aqueles que os combatem.

No contexto legal, tanto a nível nacional quanto internacional é notável a falta de regulamentações abrangentes relacionadas a crimes cibernéticos, avanços tecnológicos e em outras áreas emergentes da tecnologia. Essa lacuna normativa é notável e levanta preocupações sobre como lidar com questões mais complexas e em constante evolução nesses campos.

Ao examinar as diversas obras apontadas neste estudo, podemos obter uma ampla gama de perspectivas sobre como criar novas leis que abordam diferentes formas de *hacking*, seu impacto geral nos indivíduos e formular estratégias preventivas para esses crimes. Além disso, ao analisar essas obras, podemos antecipar possíveis problemas futuros relacionados à tecnologia e implementar medidas preventivas para evitar potenciais catástrofes.

Também é crucial lembrar que as medidas para combater crimes cibernéticos não se limitam apenas à legislação. A conscientização da população sobre os possíveis golpes e crimes, bem como a forma de evitá-los, denunciá-los e identificá-los rapidamente, desempenha um papel fundamental no combate ao crime virtual. Essa conscientização pode ser promovida de diversas maneiras, incluindo campanhas publicitárias em diferentes meios de comunicação como TV e *internet*, por

meio de propagandas e redes sociais, além de minicursos e palestras que poderiam ser oferecidos por autoridades de defesa ou segurança pública e empresas privadas. Por exemplo, *workshops* sobre segurança *online*, guias práticos de como reconhecer e evitar fraudes *online* e até mesmo simulações de *phishing* para educar as pessoas sobre como identificar e responder a tentativas de golpe online, medidas preventivas contra ataques cibernéticos e tentativas de *hacking*, etc.

REFERÊNCIAS

ALTERED Carbon [Seriado]. Direção: David Ellison. Produção: Netflix. Estados Unidos: Netflix, 2018

ADVISOR, CISCO. **BHI Energy conta como foi o hack por ransomware a seus sistemas**. Cisco Advisor, 25 out. 2023. Disponível em: https://www.cisoadvisor.com.br/bhi-energy-conta-como-ransomware-hackeou-seus-sistemas/. Acesso em: 26 out. 2023

ADVISOR, CISCO. **Ransomware: porque a empresa paga, de uma forma ou de outra?**. Cisco Advisor, 26 out. 2023. Disponível em: https://www.cisoadvisor.com.br/ransomware-por-que-toda-empresa-paga-de-uma-forma-ou-de-outra/. Acesso em: 26 out. 2023

ADVISOR, CISCO. **Violação à rede da Seiko ultrapassa 60 mil itens de dados**. Cisco Advisor, 26 out. 2023. Disponível em: https://www.cisoadvisor.com.br/violacao-a-rede-da-seiko-supera-60-mil-itens-de-dados-pessoais/. Acesso em: 26 out. 2023

AFP. **AI pede congelamento do uso de tecnologias de cibervigilância após caso Pegasus**. Istoé Dinheiro, 24 jul. 2021. Disponível em: https://istoedinheiro.com.br/ai-pede-congelamento-do-uso-de-tecnologias-de-cibervigilancia-apos-caso-pegasus/. Acesso em: 8 nov. 2023

AFP. **Caso Pegasus: entenda o caso de espionagem que ameaça o governo da Espanha**. Exame, 10 mai. 2022. Disponível em: https://exame.com/mundo/caso-pegasus-entenda-o-caso-de-espionagem-que-ameaca-o-governo-da-espanha/. Acesso em: 18 out. 2023

ARNTZ, PIETER. **“The mother of all breaches”: 26 billion records found online [Updated]**. Malwarebytes Lab, 23 jan. 2024. Disponível em: https://www.malwarebytes.com/blog/news/2024/01/the-mother-of-all-breaches-26-billion-records-found-online. Acesso em: 2 fev. 2024

BEAKLINI, BRUNO. **Espionagem: os bastidores sombrios do caso Pegasus**. Outras Palavras, 02 ago. 2021. Disponível em https://outraspalavras.net/geopoliticaeguerra/espionagem-os-bastidores-sombrios-do-caso-pegasus/. Acesso em: 8 nov. 2023

CABRAL, CARLOS. **Embargo dos EUA contra o software espião Pegasus não torna ambiente cibernético mais seguro**. El País, 12 dez. 2021. Disponível em: https://brasil.elpais.com/opiniao/2021-12-12/embargo-dos-eua-contra-o-software-espiao-pegasus-nao-torna-ambiente-cibernetico-mais-seguro.html. Acesso em: 18 out. 2023

CANALFS0CIETY. **Cisco alerta sobre bug que permite que invasores quebrem a criptografia de tráfego**. Samir News. Disponível em: https://www.samirnews.com/2023/07/cisco-alerta-sobre-bug-que-permite-que.html. Acesso em: 16 jan. 2024

CIO. **Ransomware é ataque mais preocupante para 85% dos líderes de TI**. Sofis, 05 out. 2021. Disponível em: https://www.sofis.com.br/noticias/ransomware-e-ataque-mais-preocupante-para-85-dos-lideres-de-ti/. Acesso em: 18 out. 2023

DATACENTERDYNAMICS. **Descoberto o maior vazamento de dados da História**, 24 jan. 2024. Disponível em: https://www.datacenterdynamics.com/br/not%C3%ADcias/descoberto-o-maior-vazamento-de-dados-da-historia/. Acesso em: 2 fev. 2024

DICK, Phillip K. **Blade Runner - Androides Sonham Com Ovelhas Eletricas?**. Tradução: Ronaldo Bressane. 3. ed. São Paulo: Aleph, 2019.

FACEBOOK. **Find the Kitten Vacuumer… For great justice.** Facebook. Disponível em: https://www.facebook.com/groups/ForGreatJustice/. Acesso em: 19 fev. 2024

G1 MA. **Polícia desarticula quadrilha que aplicava golpes pelo WhatsApp no MA**. G1, 25 jul. 2016. Disponível em: https://g1.globo.com/ma/maranhao/noticia/2016/07/policia-desarticula-quadrilha-que-aplicava-golpes-pelo-whatsapp-no-ma.html. Acesso em: 9 jan. 2024

GATLAN, SERGIU. **Cisco warns of but that lets attackers break traffic encryption**. Bleeping Computer, 6 jul. 2023. Disponível em: https://www.bleepingcomputer.com/news/security/cisco-warns-of-bug-that-lets-attackers-break-traffic-encryption/. Acesso em: 16 jan. 2024

GEIB, HEINI THOMAS. **Você sabe o que é Phishing? Entenda agora mesmo**. Lumiun Blog, 29 set. 2017. Disponível em: https://www.lumiun.com/blog/voce-sabe-o-que-e-phishing-entenda-agora-mesmo/. Acesso em 19 fev. 2024

GCORE. **DDoS and bot attacks in 2022: Business sectors at risk and how to defend**. Bleeping Computer, 21 set. 2024. Disponível em: https://www.bleepingcomputer.com/news/security/ddos-and-bot-attacks-in-2022-business-sectors-at-risk-and-how-to-defend/. Acesso em: 16 jan. 2024

GCORE. **Gcore Thwarts 500 Million PPS DDoS Attack on Gaming Company**. Gcore, 6 jul. 2023. Disponível em: https://gcore.com/news/500-million-pps-ddos-attack-in-2023/. Acesso em: 9 jan. 2024

GCORE. **How We Protected a Famous Gaming Company Against a 450+ Gbps DDoS Attack**. Gcore, 10 oct. 2023. Disponível em: https://gcore.com/news/how-we-protected-a-gaming-company-against-ddos-attack/. Acesso em: 9 jan. 2024

GIBSON, William. **Neuromancer**. Tradução: Fábio Fernandes. 5. ed. São Paulo: Aleph, 2016.

GRUSTNIY, LEONID. **Roubo de ouro no World of Warcraft**. Kaspersky Daily, 21 jun. 2021. Disponível em: https://www.kaspersky.com.br/blog/wow-weakauras-auction-scam/17682/. Acesso em: 9 jan. 2024

GRUSTNIY, LEONID. **Phishing até na Netflix**. Kaspersky Daily, 18 nov. 2021. Disponível em: https://www.kaspersky.com.br/blog/netflix-phishing/18512/. Acesso em: 18 fev. 2024

HENRIQUE, MARCOS. **Zphisher - Gerador de Phishing**. 100Security, Disponível em: https://www.100security.com.br/zphisher. Acesso em: 13 mar. 2024

HUREL, LOUISE MARIE. FRANCISCO, PEDRO AUGUSTO P. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência e uso de tecnologias de vigilância**. El País, 03 ago. 2021. Disponível em: https://brasil.elpais.com/opiniao/2021-08-02/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-atividades-de-inteligencia-e-uso-de-tecnologias-de-vigilancia.html.
Acesso em: 18 out. 2023

IT, INTERNATIONAL. **Lapsus$ Group: Sites do ConecteSUS e do Ministério da Saúde sofrem ataque hacker durante a madrugada**, International IT, 10 dez. 2021. Disponível em:
https://www.internationalit.com/post/lapsus-group-sites-do-conectesus-e-do-minist%C3%A9rio-da-sa%C3%BAde-sofrem-ataque-hacker-durante-madrugada.
Acesso em: 12 out. 2023

JIMO. **Avoiding Common Scams**. Steam. Disponível em: https://steamcommunity.com/sharedfiles/filedetails/?l=thai&id=177244559. Acesso em: 19 fev. 2024

IMGUR. **Akira**. Imgur, 21 abr. 2013. Disponível em: https://imgur.com/a/gYb2i. Acesso em: 26 jan. 2024.

MASAMUNE, Shirow. **The Ghost in the Shell**. 1. ed. São Paulo: JBC, 2016.

MR. Robot - Sociedade Hacker [Seriado]. Direção: Sam Esmail. Produção: Steve Golin, Chad Hamilton, Igor Srubshchik. Estados Unidos: Universal Cable Productions, 2015.

PAIVA, IURI. **Espionagem virtual e Direitos Humanos: caso Pegasus e outras ameaças**. Observatório de Crises Internacionais UFPE, 31 ago. 20222. Disponível em: https://sites.ufpe.br/oci/2022/08/31/espionagem-virtual-e-direitos-humanos-caso-pegasus-e-outras-ameacas/. Acesso em: 8 nov. 2023

PETKAUKAS, VILIUS. **Mother of all breaches reveals 26 billion records: what we know so far**, Cybernews, 29 jan. 2024. Disponível em: https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/. Acesso em: 2 fev. 2024

SPADONI, PEDRO. **26 bilhões de dados: veja se você está no maior vazamento da história**. Olhar Digital, 23 jan. 2024. Disponível em: https://sincomerciariossc.org.br/2024/01/26/26-bilhoes-de-dados-maior-vazamento-da-historia/. Acesso em: 2 fev. 2024

SERIAL Experiments Lain [Seriado Animado]. Direção: Ryūtarō Nakamura. Produção: Triangle Staff. Japão: TV Tokyo, 1998.

SOFTSYSTEM. **Vírus ransomware busca vítimas no Brasil**. Softsystem, 19 jun. 2023. Disponível em: https://www.softsystem.com/softsystem/exibeNoticias.jsp?publicacao.codPublicacao=1036&codListaTipoPublicacao=2. Acesso em: 12 fev. 2024

STEPHENSON, Neal. **Snow Crash**. Tradução: Fábio Fernandes. 2. ed. São Paulo: Aleph, 2015

STUDIO, REDAÇÃO. **Smishing: o golpe do falso SMS está ganhando espaço nos meios digitais**. Studio FM, 6 out. 2020. Disponível em: https://www.studio.fm.br/2020/10/smishing-o-golpe-do-falso-sms-esta-ganhando-espaco-nos-meios-digitais/. Acesso em 18 fev. 2024

THINKSTOCK. **How to respond to a ransomware attack**. CIO, 05 mar. 2016. Disponível em: https://www.cio.com/article/221850/how-to-respond-to-a-ransomware-attack.html. Acesso em: 18 out. 2023

WATCH Dogs 2. Montreal: Ubisoft Montreal, 2014. Jogo eletrônico.

VALIMAIL. **Phishing vs. Pharming**. Valimail. Disponível em: https://www.valimail.com/guide-to-phishing/phishing-vs-pharming/. Acesso em: 18 fev. 2024