CENTRO PAULA SOUZA
ETEC DARCY PEREIRA DE MORAES
CURSO TÉCNICO COM HABILITAÇÃO PROFISSIONAL EM SERVIÇOS JURÍDICOS

Bruna Leandro de Souza
Danilo Eduardo do Nascimento Santos
Kauã Vinícius de Lima Proença
Letícia Kirilov Braga de Oliveira

INDAGAÇÕES SOBRE O CRIME CIBERNÉTICO NO BRASIL: UMA PESQUISA BIBLIOGRÁFICA DESSA OCORRÊNCIA.

ITAPETININGA
2023

Bruna Leandro de Souza

Danilo Eduardo do Nascimento Santos

Kauã Vinícius de Lima Proença

Letícia Kirilov Braga de Oliveira

INDAGAÇÕES SOBRE O CRIME CIBERNÉTICO NO BRASIL: UMA PESQUISA BIBLIOGRÁFICA DESSA OCORRÊNCIA.

Trabalho de Conclusão de Curso apresentado como exigência parcial para a obtenção da Habilitação Profissional de Técnico em Serviços Jurídicos, a Escola Técnica Estadual de Itapetininga, sob orientação do Professor MBA Esp. André Luiz Oliveira Santos.

ITAPETININGA

2023

“Dedico este trabalho primeiramente a Deus por sempre estar conosco nos guardando, e a todas as pessoas que estiveram ao meu lado durante essa jornada acadêmica. Aos meus pais, pela constante inspiração e apoio incondicional. Aos meus amigos, por compartilharem comigo as alegrias e desafios deste percurso. Aos meus professores, pela orientação e conhecimento transmitido. E, acima de tudo, dedico este TCC a todos que cooperaram conosco para que esse sonho se torne realidade, como prova de que a perseverança e a dedicação podem tornar os sonhos realidade”

“Primeiramente agradecemos a Deus por nos dar sabedoria e paciência durante o processo de aprendizado para enfim concluirmos este curso. Agradecemos também ao nosso orientador/professor pelo suporte, orientação e paciência durante essa longa jornada acadêmica e a todos os professores e profissionais que nos auxiliaram compartilhando seus conhecimentos e experiências para enriquecer essa pesquisa. Somos gratos também a todos os familiares por todo apoio incondicional, pelas palavras e pela compreensão durante todos os momentos em que precisamos, principalmente nos momentos dedicados a este Trabalho de Conclusão de Curso”

“Creio no riso e nas lágrimas como antídotos contra o ódio e o terror.”

Charles Chaplin

RESUMO

Este trabalho de conclusão de curso (TCC) realiza uma análise aprofundada do cenário de crimes cibernéticos no Brasil por meio de uma pesquisa bibliográfica abrangente. Explora as tendências, desafios e implicações dos crimes cibernéticos, destacando a crescente importância desse fenômeno na era digital. O estudo também investiga as estratégias de prevenção e combate adotadas no contexto brasileiro. Ao reunir informações de fontes confiáveis, este trabalho oferece uma visão abrangente do crime cibernético no Brasil, contribuindo para uma compreensão mais sólida desse problema contemporâneo.

Palavras-chave: Crimes Cibernéticos, Brasil, Tendências, Desafios, Implicações, Prevenção, Combate, Era Digital

ABSTRACT

This course completion work (TCC) carries out an in-depth analysis of the cybercrime scenario in Brazil through a comprehensive bibliographical research. Explores the trends, challenges and implications of cybercrime, highlighting the growing importance of this phenomenon in the digital age. The study also investigates prevention and combat strategies adopted in the Brazilian context. By bringing together information from reliable sources, this work offers a comprehensive view of cybercrime in Brazil, contributing to a more solid understanding of this contemporary problem.

Keywords: Cybercrimes. Brazil, Tendencies, Challenges, Implications, Prevention, Combat, Digital Age.

SUMÁRIO

1. INTRODUÇÃO

Com a globalização e consequentemente com o avanço tecnológico crescente e a interconexão digital, a sociedade moderna enfrenta um complexo desafio: o crime cibernético, por meio de diversas formas de ataques virtuais, também conhecido como Phishing na linguagem técnica surgiu como umas das maiores ameaças aos bancos de dados e da segurança das informações que atinge não só pessoas físicas, mas de uma forma mais contundente pessoas jurídicas que mais se propaga na sociedade atual.

Sobretudo é uma técnica que contém a manipulação psicológica (o engano de suas vítimas) com o objetivo de obter informações confidenciais de usuários, como senhas, números de cartões de crédito e dados pessoais, invasão de contas bancárias, arquivos pessoais por meio de mecanismo enganosos se passando por entidades confiáveis. Essa prática criminosa tem gerado grandes prejuízos financeiros e violações ao direito à privacidade de indivíduos, instituições governamentais e empresas em todo o mundo.

Nesse cenário, é primordial compreender a importância e estudar a prática do crime cibernético, afim de que se possa desenvolver estratégias eficazes de prevenção da confidencialidade dos dados através do desenvolvimento de ferramentas que combatam de forma continua as bases de dados que hoje são armazenadas em nuvens, por intermédio de uma análise profunda desta prática delituosa, é possível identificar seus mecanismos, metas e consequências, como as técnicas exploradas pelos criminosos virtuais para enganar suas vítimas.

Este trabalho tem como principal objetivo investigar, analisar e contextualizar algumas ilações sobre os fenômenos dos crimes cibernéticos e mostrar a sua relevância na sociedade contemporânea, desse modo fornecer um uma perspectiva mais ampla sobre a prática dos crimes cibernéticos e suas consequências na sociedade moderna.

É necessário se entender melhor o funcionamento do crime cibernético e suas nuances, espera-se contribuir para a formação de uma sociedade mais resiliente e consciente, capaz de enfrentar essa ameaça crescente e proteger-se de maneira eficaz no ambiente digital.

2. JUSTIFICATIVA

Estamos vivenciando nas últimas décadas uma grande evolução tecnológica, onde em pouco tempo várias mudanças consideráveis vêm adentrando em nosso modo de vida e consequentemente fazendo com que a vulnerabilidade dos usuários aumente pela falta de informações. Essas mudanças têm sido muito benéficas para os criminosos com intenções de cometerem crimes cibernéticos.

Por conta desse aumento considerável, nesse trabalho de Conclusão De Curso estaremos abordando esse tema para que haja conscientização necessária para a população, evitando ao máximo que pessoas caiam nesses golpes pela ausência de conhecimento.

3. OBJETIVOS:

3.1. Objetivos Gerais:

No cenário atual, vemos que a sociedade está frequentemente em contato com a internet. Também é notório que com o avanço da tecnologia, muitas pessoas são vítimas de Crimes Cibernéticos, e nosso objetivo é realizar um estudo sobre a prática criminosa e conscientizar sobre ela.

3.2. Objetivos Específicos:

Informar e alertar a população sobre essa prática criminosa cibernética que aumenta cada vez mais conforme o avanço tecnológico.

4. SOCIOLOGIA E A ORIGEM HUMANA: EXPLORANDO AS TEORIAS SOBRE O SURGIMENTO DAS SOCIEDADES

4.1. Pirâmide de Maslow

A “Pirâmide de Maslow” refere-se à teoria da hierarquia das necessidades proposta pelo psicólogo Abraham Maslow. Essa teoria sugere que as necessidades humanas estão organizadas em diferentes níveis, dispostos em uma forma de pirâmide.

A teoria da pirâmide de Maslow também pode ser aplicada na área jurídica. Embora as necessidades humanas básicas permaneçam as mesmas, as formas como elas são satisfeitas pode variar no contexto jurídico. Aqui está uma possível adaptação da pirâmide de Maslow para a área jurídica:

> O modelo da pirâmide de Maslow, com suas cinco necessidades hierárquicas, continua a ser uma ferramenta valiosa para compreender a motivação humana e as aspirações individuais. (MYERS 2004, p. 428)

Como dito por Abraham Maslow, são essas as cinco necessidades hierárquica:

1. Necessidades fisiológicas: Isso inclui acesso a recursos básicos, como alimentação adequada, moradia segura e saúde física. Na área jurídica, é importante garantir o acesso à justiça e aos direitos fundamentais de cada indivíduo;

2. Necessidades de segurança: Isso envolve a proteção contra ameaças físicas e emocionais, bem como a segurança jurídica. No contexto jurídico, é essencial garantir que as leis sejam aplicadas de forma justa e que os direitos individuais sejam protegidos;

3. Necessidades sociais: Isso inclui a necessidade de pertencimento, interação social e conexão com a comunidade. Na área jurídica, é importante promover a justiça social, os direitos humanos e a igualdade perante a lei;

4. Necessidades de estima: Isso envolve o reconhecimento, a autoestima e o respeito. Na área jurídica, é fundamental garantir o respeito pelos direitos dos indivíduos, bem como promover a dignidade humana e a igualdade;

5. Necessidades de auto realização: Isso se refere ao desejo de alcançar o potencial máximo e realizar-se pessoal e profissionalmente. Na área jurídica, isso

pode ser alcançado por meio do desenvolvimento profissional, da busca pela justiça e da contribuição para a sociedade.

4.2. Teoria do Contrato Social

Uma das teorias mais influentes sobre a origem da sociedade é a teoria do contrato social, associada a filósofos como Thomas Hobbes, John Locke e Jean-Jacques Rousseau. Essa perspectiva sugere que as sociedades surgiram a partir de um acordo tácito ou explícito entre os indivíduos. Hobbes argumentou que as pessoas, em um estado de natureza, eram egoístas e agressivas, o que as levou a buscar a segurança em uma sociedade organizada por meio de um contrato social. Locke defendia a ideia de que as pessoas se uniam para proteger seus direitos naturais à vida, à liberdade e à propriedade. Rousseau, por sua vez, enfatizava a busca pela igualdade e a formação de um contrato social que refletisse a vontade geral.

> Suponhamos que homem chegando a aquele ponto em que os obstáculos prejudiciais à sua conservação no estado de natureza sobrepujam pela sua resistência as forças de que cada indivíduo dispõe para manter-se nesse estado. Então, nesse estado primitivo já não pode subsistir, e o gênero humano parecia se não mudasse de modo de vida (Rousseau, p. 69-70).

4.3. Teoria da evolução social

Outra perspectiva importante é a teoria da evolução social, que se baseia na ideia de que as sociedades humanas evoluíram ao longo do tempo, passando por estágios de desenvolvimento. Herbert Spencer e Auguste Comte foram dois pensadores notáveis que contribuíram para essa abordagem. Spencer argumentou que a sociedade era como um organismo em evolução, com diferentes partes desempenhando funções específicas. Comte, por sua vez, propôs que a sociedade progredia de um estágio teológico para um estágio metafísico e, finalmente, para um estágio positivo, caracterizado pela compreensão científica.

4.4. Revolução industrial e urbanização

A Revolução Industrial no século XVIII trouxe uma transformação fundamental na vida das sociedades. A urbanização acelerou à medida que as pessoas migraram das áreas rurais para as cidades em busca de emprego nas fábricas. Isso resultou em mudanças na estrutura familiar, nas condições de trabalho e nas relações sociais, assim implementando uma nova forma de vida humana que gira em torno do capitalismo resultando e um novo tipo de sociedade.

4.5. Era digital e a sociedade da informação

A virada do século XXI trouxe consigo a Era Digital e a Sociedade da Informação. O advento da internet, das redes sociais e da tecnologia da informação transformou radicalmente a forma como as pessoas se comunicam, trabalham, aprendem e interagem socialmente. A globalização digital encurtou as distâncias e conectou pessoas de todo o mundo em uma escala nunca vista.

> No fim do segundo milénio da Era Cristã, vários acontecimentos de importância histórica têm transformado o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias da informação está remodelando a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre a economia, o Estado e a sociedade em um sistema de geometria variável (Manuel Castells, p. 21).

4.6. Desafios e oportunidades na era digital

A Era Digital trouxe desafios e oportunidades únicos para a sociedade, as questões como privacidade, segurança cibernética, desigualdade digital e o impacto da automação no mercado de trabalho são temas críticos que os sociólogos exploram. Ao mesmo tempo, a tecnologia oferece oportunidades para a participação cívica, a mobilização social e a disseminação de informações.
A jornada da origem humana até a Era Digital é uma história de mudanças sociais profundas e constantes, a sociologia desempenha um papel essencial na análise e compreensão dessas transformações, identificando tendências, desafios e oportunidades, à medida que avançamos na Era Digital, é fundamental continuar a explorar e questionar as implicações sociais da tecnologia, bem como as formas pelas

quais a sociedade molda e é moldada por essas inovações. A sociologia continuará a desempenhar um papel crucial à medida que enfrentamos os desafios e aproveitamos as oportunidades da era digital em constante evolução.

4.7. Conceito de sociedade

A sociedade pode ser definida como um grupo de pessoas que compartilham uma série de elementos comuns, como valores, normas, cultura, território geográfico e interações sociais; ela é caracterizada pela organização e interdependência de seus membros, que cooperam para alcançar objetivos individuais e coletivos. A sociedade é, portanto, um sistema complexo de relações sociais que se desenvolve ao longo do tempo e que influencia o comportamento e as experiências dos indivíduos que a compõem.

4.8. Origem da sociedade

A origem da sociedade é um tema complexo e controverso que tem sido debatido ao longo da história da filosofia e da sociologia, diferentes teorias e perspectivas oferecem interpretações diversas sobre como as sociedades humanas surgiram, nas ciências sociais e humanas, o termo "sociedade" refere-se a um conjunto complexo e organizado de pessoas que compartilham normas, valores, locais, culturas e interações sociais. Ele é uma parte essencial da existência humana e desempenha funções importantes na estruturação da vida em comunidade, no desenvolvimento das relações interpessoais e no desenvolvimento da identidade, desde tribos indígenas isoladas até sociedades altamente urbanizadas e tecnologicamente avançadas, existem muitas variedades de sociedades em todo o mundo.

> Mas a ordem social é um direito sagrado que serve de alicerce a todos os outros é um direito sagrado que serve de alicerce a todos os outros. Esse direito, todavia, não vem da natureza; está, pois, fundamentado sobre convenções (Rousseau, p. 10).

4.9. A era digital e a sociedade conectada

A era digital tem sido marcada pela proliferação da internet, dispositivos móveis, redes sociais e inúmeras outras tecnologias que interconectam as pessoas em todo o mundo. A sociologia moderna reconhece que essas conexões digitais têm um impacto profundo na forma como construímos relacionamentos, compartilhamos informações e interagimos socialmente.

Os criminosos cibernéticos são indivíduos ou grupos que utilizam a tecnologia digital para cometer crimes, tais como hacking, fraude online, roubo de identidade, disseminação de malware e outros, eles podem ser motivados por diversos fatores, como ganho financeiro, notoriedade, espionagem, ativismo ou simplesmente por desafio, é importante reconhecer que os criminosos cibernéticos não formam um grupo homogêneo; suas motivações e backgrounds são variados. A sociologia desempenha um papel crucial na análise dos fatores sociais que contribuem para a criminalidade cibernética

4.10. Consequências e respostas sociais

A criminalidade cibernética tem consequências significativas para a sociedade, incluindo perda financeira, violação de privacidade e ameaças à segurança nacional. A sociologia desempenha um papel fundamental na compreensão dessas consequências e no desenvolvimento de estratégias de prevenção e combate.

Entretanto a sociologia ajuda a avaliar a eficácia das leis e regulamentos relacionados à criminalidade cibernética, bem como a compreender os desafios enfrentados pelas autoridades na aplicação da lei. Portanto, se mostra fundamental a conscientização e Educação Pública, sociologia pode contribuir para campanhas de conscientização e programas educacionais que visam informar o público sobre os riscos da criminalidade cibernética e como se proteger.

A criminalidade cibernética é um fenômeno complexo e multifacetado que está intrinsecamente ligado à sociedade digital, a sociologia desempenha um papel fundamental na análise das causas sociais subjacentes à criminalidade cibernética, bem como na busca por soluções eficazes para enfrentar esse desafio. À

medida que a era digital continua a evoluir, a sociologia continuará a desempenhar um papel crucial na compreensão das complexas interações entre tecnologia, indivíduos e sociedade

5. CONCEITO DE CRIME CIBERNÉTICO

O crime é um reflexo de uma complexa sociedade dinâmica entre normas sociais, valores, princípios, culturas e um sistema governamental; entretanto, a definição de crime traz como base em normas e leis estabelecidas por uma sociedade que tem o foco em diminuir a criminalidade e punir quem infringe as normas da nação. Portanto, o ato criminal se caracteriza pela ação de um indivíduo que vai contra as normas legais, e estará sujeito as sanções legais e punitivas.

Atualmente, estamos vivendo em uma era tecnológica, onde os crimes cibernéticos vêm se protagonizando cada vez mais. Os crimes cibernéticos passaram a ser praticados em 1960, nos Estados Unidos quando os primeiros computadores começaram a ser utilizados em grandes empresas e organizações governamentais. Como na época a tecnologia não era acessível a todos, sua utilização era limitada a profissionais que trabalhavam na área, tais como cientistas, engenheiros e matemáticos.

> Em uma noção geral, os primeiros sinais de crimes informáticos seriam os primeiros atos de sabotagens, a novas tecnologias ampliadas neste período histórico, como explicam Damásio de Jesus e José Milagres (BRASIL, 2016, p. 22)

A prática criminosa se deu início a partir da curiosidade de alguns estudantes universitários que buscavam ampliar seus conhecimentos inicialmente através da intranet que posterior se transformou em internet que promoveu a conexão mundial na troca de dados, e com novos desafios, muitos desses desafios mostraram a eles algumas vulnerabilidades do sistema de computadores e redes. A partir dessas descobertas os criminosos foram obtendo acessos ilícitos a dados privados nas mais diversas atividades.

> Toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material". (ROQUE, 2007, p.25)

Hoje em dia esses crimes cibernéticos se ampliaram junto da tecnologia, fazendo com que qualquer pessoa com pequenas informações consiga praticar tal ato. Com essas informações eles são capazes de praticar diversos outros crimes cibernéticos, como por exemplo:

- Pirataria;
- Cryptojacking;
- Phishing
- Extorsão cibernética
- Falsificação de dados financeiros, documentos particulares ou cartões de crédito;
- Violação de propriedade intelectual (fraudes de identidades)

O crime cibernético Phishing é considerado o crime mais fácil de aplicação, e o mais perigoso para população, por esse motivo estaremos nos aprofundando neste tema.

6. PASSADO HISTÓRICO ANTERIOR AO PHISHING

Em uma Terça-feira, dia 28 de junho de 2022, em Brasília, a Polícia Federal efetivou o projeto da Unidade Especial de investigação de Crimes Cibernéticos (UEICC). A implementação está em conformidade com as orientações das iniciativas estratégicas do Ministério da Justiça e Segurança Pública para combater a criminalidade cibernética, concentrando-se na investigação formal de casos sensíveis e complexos relacionados a crimes de alta tecnologia.

Embora a termologia "Phishing" tenha sido criada apenas na década de 90, essas ações criminosas vêm de muito antes. No Brasil tivemos uma década responsável pelo pico de usuários de Internet, como explica a revista Veja:

A internet no Brasil experimentou um crescimento espantoso, notadamente entre os anos de 1996 e 1997, quando o número de usuários aumentou 1000% (mil por cento), passando de 170 mil em janeiro de 1996 para 1,3 milhão em dezembro de 1997. Em janeiro de 2000, eram estimados 4,5 milhões de "internautas". Atualmente,

cerca de 10 milhões de brasileiros podem acessar a Rede de suas residências. Se consideradas as pessoas que têm acesso apenas nos seus locais de trabalho, esse número sobe para 15 milhões. (REVISTA VEJA, 2000)

Estudos comportamentais comprovam que a tecnologia influenciou para os crescimentos desses crimes, mas a prática desse ato ilícito passa a existir desde a criação da chamada civilização.

7. ORIGEM DO PHISHING

O Termo Phishing é se refere a "pescar", onde os criminosos conseguem pescar os dados da vítima para usar em meios fraudulentos. Isso já ocorria desde a primeira civilização, onde os criminosos tentavam se caracterizar para conseguir benefícios a partir da identidade de outra pessoa. Boa parcela da população culpa o desenvolvimento da tecnologia como responsável por esses crimes, mas independentemente da tecnologia criminosos já existiam e praticavam crimes similares ao Phishing.

O Phishing é definido como extração de informações confidenciais por meio de métodos ilícitos, onde o criminoso consegue capturar senhas, dados pessoais e até mesmo números de cartão de crédito da vítima.

> Em 1995, devido ao grande aumento de usuários no início da década de 90 a internet foi transferida para a administração de instituições não-governamentais, que se encarregam, entre outras coisas, estabelecer padrões de infraestrutura, registrar domínios, etc. Exemplos dessas instituições são a Internet Society, situada nos Estados Unidos, mas atuando no mundo inteiro, e o Comitê Gestor da Internet que atua restritamente no Brasil. (MONTEIRO, 2001)

Embora não exista uma data exata para identificar a origem a essa prática, sabemos que a prática começou a ser relatada desde a década de 1990. Os primeiros casos eram mais simples em comparação aos atuais, pois no início os criminosos enviavam e-mails em massa para tentar enganar as pessoas alegando serem empresas famosas e instituições financeiras, mas com os avanços tecnológicos os golpistas começaram a evoluir suas técnicas para maior obtenção de dados.

A partir do momento que uma pessoa se conecta a internet diversos dados ficam disponíveis para criminosos, o que facilita a execução de diferentes tipos de crimes.

> O phishing é um dos métodos mais antigos e eficazes de engenharia social, que consiste em enviar mensagens eletrônicas fraudulentas que tentam induzir o destinatário a revelar informações confidenciais ou executar alguma ação maliciosa.” (SILVA, 2019, p. 27)

A crescente conectividade à internet ampliou o risco de exposição de dados pessoais e informações sensíveis. A troca de dados através de endereços IP e a enorme quantidade de informações disponíveis online oferecem uma janela de oportunidade para os criminosos explorarem vulnerabilidades e perpetrarem crimes cibernéticos.

8. AUMENTO DOS CRIMES CIBERNÉTICOS NAS ÚLTIMAS DÉCADAS

Vemos atualmente um aumento considerável na adoção de atividades online com a chegada da era tecnológica. Por conta dessas novas ferramentas os criminosos conseguem tirar proveito das pessoas que não possuem conhecimento básico sobre a segurança pessoal e tecnológica. As redes sociais no geral foi um dos contribuintes para essa coleta de dados pessoais, já que se tornou um território livre para circulação de dados de forma excessiva, onde um considerável número de pessoas usa de forma irresponsável, expondo ao público informações confidenciais. Nesse contexto é notório que a sociedade se tornou dependente de mídias sociais para viver, já que a utilização da mesma pode ser a geradora de dopamina e hormônios de prazer.

No mundo, dois em cada três usuários já foram vítimas de crimes virtuais, que atingem 556 milhões de pessoas todos os anos. Só no Brasil, o prejuízo anual é o maior de todos, estimado em R$ 16 bilhões. Os dados são de 2012, da empresa de segurança virtual Symantec.

De acordo com o relatório de 2014 da Kaspersky Lab, outra companhia de segurança na Internet, o Brasil é o segundo país onde mais acontecem fraudes bancárias. (TECMUNDO, 2016)

9. CRIMES CIBERNÉTICOS NAS ORGANIZAÇÕES DE SÃO PAULO

Os crimes cibernéticos representam uma preocupação crescente para organizações em São Paulo e em todo o mundo. Esses crimes envolvem atividades ilegais realizadas através de dispositivos eletrônicos e da internet, como fraudes, ataques de Phishing, roubo de dados, invasões de sistemas e outros tipos de violações de segurança. Em São Paulo, assim como em outras grandes cidades, empresas de todos os setores têm sido alvo de crimes cibernéticos. Isso inclui desde pequenas empresas até grandes corporações. Os criminosos cibernéticos podem visar informações confidenciais, como dados financeiros, informações pessoais dos clientes e propriedade intelectual.

> O aumento dos crimes cibernéticos no estado de São Paulo reflete uma tendência global de crescimento desse tipo de delito, que afeta tanto pessoas físicas quanto jurídicas. Segundo o relatório da empresa de segurança digital Kaspersky, o Brasil foi o segundo país mais atacado por hackers em 2022, ficando atrás apenas da Rússia. Os ataques mais comuns foram os de phishing, que consistem em enviar e-mails falsos para obter dados pessoais ou financeiros das vítimas, e os de ransomware, que bloqueiam o acesso aos arquivos do computador e exigem um resgate para liberá-los.” (SILVA, 2022, p. 23)

Para combater esses crimes, as organizações em São Paulo têm investido em medidas de segurança cibernética, como firewalls, sistemas de detecção de intrusões, criptografia de dados e conscientização dos funcionários sobre boas práticas de segurança. Além disso, a colaboração com as autoridades policiais e especialistas em segurança cibernética é essencial para investigar e combater essas atividades criminosas. É importante que essas organizações estejam constantemente atualizadas sobre as ameaças cibernéticas em evolução e implementem medidas de segurança adequadas para proteger seus sistemas e informações.

10. LEIS DE ROUBOS DE DADOS

10.1. Lei Carolina Dieckmann

De acordo com a Lei Carolina Dieckmann (Lei Brasileira 12.737/2012), elencou as condutas consideradas penalmente típicas, mas não reconheceu várias condutas delitivas que ocorrem na Internet. Como resultado, esses comportamentos foram denominados doutrinariamente como "crimes virtuais impróprios". Além disso, o artigo afirma que o presente estudo examina o conteúdo da Lei mencionada e todas as alterações que ela trouxe ao sistema pátrio brasileiro. O objetivo é descobrir como os Tribunais Superiores pátrios entenderam esse assunto. No entanto, mesmo diante das mudanças significativas no direito brasileiro com o objetivo de sanar o problema, a referida legislação parece não ser capaz de atender à demanda crescente de delitos desse tipo.

Os artigos 154-A e 154-B e os artigos 266 e 298 do Código Penal brasileiro foram alterados, conforme mencionado pela Lei Carolina Dieckmann (Lei Brasileira no 12.737/2012). Os "delitos ou crimes informáticos" são tipificados por essa lei. Por exemplo, o artigo 154-A aborda a invasão de dispositivo informático alheio e o artigo 154-B aborda a interceptação de comunicações eletrônicas. O texto não lista todas as ações que a Lei considera crimes cibernéticos, mas enfatiza que o trabalho atual se concentra na análise das previsões penais contidas na Lei no 12.737/2012, que serão examinadas minuciosamente a seguir, enfatizando seus principais componentes constitutivos. O trabalho também examina as posições dos Tribunais Superiores pátrios sobre o assunto.

10.2. Marco Civil da Internet Lei Nº 12.965/2014

O Marco Civil da internet foi uma lei criado pelo Poder Executivo no início do ano de 2014, mais precisamente em 23 de abril de 2014, onde em uma Conferência Internacional, conhecida como NETMundial10, realizada em São Paulo, que reuniu 90 países do mundo inteiro.

O propósito da Lei 12.965/2014 é garantir à segurança digital e defesa dos consumidores que usam a internet para adquirir produtos ou serviços, pois regula a comercialização das empresas que utilizam do meio digital como meio de comércio, assegurando a livre iniciativa, bem como a livre concorrência. Regendo também os

serviços que são prestados pelas multinacionais provedoras de Internet, criando um fornecimento com garantia de funcionalidade e segurança para os usuários, essa lei para o Brasil estabeleceu princípios, garantias, direitos e deveres para o uso do meio digital.

O Marco Civil da Internet também representa um avanço na participação social e na democracia digital, pois foi construído a partir de um amplo debate público que envolveu diversos setores da sociedade, como governo, academia, empresas, organizações não governamentais e internautas. O processo de elaboração da lei durou cerca de sete anos e contou com mais de 2 mil contribuições online e presenciais. Dessa forma, o Marco Civil da Internet expressa os anseios e as demandas dos cidadãos brasileiros que utilizam a rede mundial de computadores para se comunicar, se informar, se educar, se divertir e exercer seus direitos.

> Art. 1° Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (LEI 12.965, de 2014)

Conforme estabelecido no artigo 5° inciso XII da Constituição Federal.

> Art. 5° XII – “É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (BRASIL, 1988).

Garantir a proteção de dados dos usuários ou pessoais no meio digital é uma preocupação comum entre as empresas. Com uma lei que regulamenta e define limites o Marco Civil da internet passa a ser uma regra essencial para o uso digital de forma saudável segura.

Entretanto algumas organizações terão que se adequar as políticas de segurança dos seus sites e dos bancos de dados da empresa e de seus usuários em função do Marco Civil da interne, uma lei que regulamenta e exige uma série de condições e regras que visam proteger e assegurar ainda mais as informações pessoais dos seus usuários

Visto que esta nova legislação institui novos regulamentos tanto para os provedores de conexão, quanto para os provedores de aplicação de internet a sigam respeitando suas regras e normas entre usuários e empresas buscando diminuir o uso

indevido de informações privadas. Como a lei veta o uso e o fornecimento dos dados para fins que o usuário não permitiu.

10.3. Três Princípios Básicos Do Marco Civil Da Internet

A fiscalização deve se ocorrer por meio de alguns órgãos fiscalizadores que têm o dever de detectar as infrações cometidas no ambiente digital, como a Anatel e da Secretaria Nacional do consumidor. Enquanto isto ocorre o Comitê Gestor da internet deve promover estudos com o objetivo de regulamentar regras e padrões de neutralidade e proteção de dados além de pontuar recomendações referentes ao assunto para melhorar a segurança virtual

É necessário que os provedores de conexão e aplicação a inviolabilidade dos dados dos usuários por meio de criptografia e consentimento dos usuários. Por isto o princípio da neutralidade proíbe que os provedores de conexão façam qualquer distinção de velocidade entre as páginas na internet prejudicando o usuário. Por se tratar de uma lei extensa, que aborda diversos aspectos em torno do ambiente digital, o Marco Civil da Internet ainda traz outras questões relevantes.

10.4. Aspectos De Regulamentação Do Marco Civil Da Internet No Meio Empresarial

Por ser uma lei extensa, que aborda uma diversidade de aspectos do meio digital, o Marco Civil da internet trouxe uma série de medidas que visam a segurança de dados dos usuários O Marco Civil da Internet trouxe uma série de medidas que visam a segurança de dados dos usuários e o acesso igualitário a todos os provedores de aplicação de internet. Com isso, a lei reforça a necessidade de as empresas adotarem medidas que garantem a proteção da informação.

Isso significa que a empresa pode ter que adequar o seu site para assegurar aos usuários uma navegação tranquila. Medidas como implementar uma Política de Privacidade e um Termo de Uso no site são essenciais de acordo com as exigências da lei. A companhia também deve revisar o tratamento que os dados recebem uma vez que o usuário navega pelo site. Caso a página faça uso de cookies, por exemplo, a funcionalidade deve estar explícita na Política de Privacidade do site.

Além disso, a empresa também deve ter cuidado com as informações fornecidas pelo usuário através do preenchimento de formulários e com ações de marketing dirigido. Por fim, as empresas que se adequarem ao Marco Civil.

10.5. Lei Geral De Proteção De Dados (LGPD)

A Lei n. 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor no ano de 2020. Essa é uma lei brasileira que regula o tratamento de dados pessoais e estabelece diretrizes para o uso adequado de informações pessoais, visando evitar abusos, e priorizar a liberdade e privacidade do cidadão. A lei estabelece o que é considerado dados pessoais e informa que para casos específicos é necessário muito cuidado pois são mais frágeis e expostas. Tais como: dados digitais, pessoais, infantil entre outros. Serve como garantia de direitos, assim dito em seu Art. 1°:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (LEI 13.709, de 2018)

A atuação dessa lei auxilia diretamente na proteção de dados de pessoas sensíveis, atuando no tratamento de dados de forma digital, tanto para pessoas jurídicas como natural.

11. COMPETENCIA PARA JULGAMENTO DE CRIMES CIBERNÉTICOS

A competência de julgar os crimes cibernéticos varia de acordo com a natureza do crime. Regularmente, os responsáveis por estar função incluem a Policia Federal, o Ministério Público Federal e a Justiça Federal. Crimes graves como ataques que afetem a segurança Nacional ou Invasões de sistemas governamentais, são julgados pela Justiça Federal.

De acordo com o artigo 70 do Código de Processo Penal:

> Art. 70 competência será, de regra, determinada, pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução. (LEI 3.689, de 1941)

Já o §1º do artigo 70 do Código de Processo Penal (CPP) estabelece uma regra importante para determinar a competência territorial em casos de infrações penais que tenham iniciado no território nacional, mas cuja consumação ocorra fora do Brasil. Nesse contexto, a competência jurisdicional será definida com base no local onde ocorreu o último ato de execução no Brasil.

Isso significa que, se uma infração penal for iniciada no Brasil, por exemplo, com crimes cibernéticos ocorrendo em território nacional, mas sua conclusão ou consumação acontecer fora do país, o tribunal competente para julgar o caso será aquele onde ocorreu o último ato relacionado à execução da infração dentro do Brasil.

Essa regra visa garantir que a jurisdição para julgar o crime permaneça no país onde o delito teve origem, mesmo que parte do cybercrime tenha ocorrido no exterior. Dessa forma, o Código de Processo Penal busca assegurar a aplicação da lei penal brasileira em casos de crimes transnacionais ou que tenham repercussões além das fronteiras nacionais.

É importante destacar a regulamentação do artigo 6°do Código Penal que aborda a definição do local do crime como sendo aquele onde ocorre qualquer uma das etapas que compõem o processo criminoso. Contudo, nos casos de crimes Cibernéticos é importante destacar que tais etapas podem ser realizadas em diversos locais diferentes.

Nesse caso, será utilizado o artigo 70 do CPP, por meio do site em que foi praticado o ato. Se por acaso os sites situados em provedores fora do Brasil, será aplicado algumas regras compostas pelo artigo 88 do Código de Processo Penal (CPP) que diz:

> Art. 88 No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República. (LEI 3.689, de 1941)

Contudo, em casos de crimes cibernéticos, a atribuição de competência torna-se desafiadora devido à natureza da internet. A competência em crimes cibernéticos envolve considerações complexas, como o princípio da territorialidade ou

nacionalidade, muitas vezes requerendo cooperação internacional, inclusive por meio de pedidos de extradição para julgamento no país onde o crime foi cometido.

12. DELEGACIAS ESPECIALIZADAS EM CRIMES CIBERNÉTICOS

No Brasil, as delegações focadas na criminalidade digital desempenham um papel vital na aplicação da lei num ambiente cada vez mais digital e interligado. O contexto jurídico brasileiro exige certas abordagens para lidar com a complexidade dos crimes cibernéticos, e estas delegações servem como pedras-chave nesta violação da lei.

É fundamental compreender que o ordenamento jurídico brasileiro evoluiu para incluir o ambiente digital e reconhecer os crimes cibernéticos como crimes passíveis de punição. Isto é crucial dado o crescimento exponencial das atividades online e a consequente necessidade de regulamentação, as delegacias especializadas são uma manifestação dessa adaptação jurídica em resposta à crescente demanda por investigações e ações judiciais envolvendo crimes cibernéticos.

No ordenamento jurídico brasileiro, essas delegações são responsáveis pela investigação e coleta de provas relativas aos crimes cibernéticos, isto é especialmente desafiador dada a natureza mundial e errática da Internet, que permite que os criminosos operem anonimamente a partir de qualquer local do mundo. O sistema judicial brasileiro exige que as provas sejam obtidas de maneira lícita e persuasiva, portanto, as delegações especializadas devem contratar especialistas em computação de primeira linha para garantir a admissibilidade das provas perante um juiz.

Estas unidades desempenham um papel significativo na educação e prevenção, além da investigação. O sistema jurídico brasileiro incentiva a prevenção do crime, e delegações especializadas colaboram frequentemente com outras instituições para informar o público sobre ameaças cibernéticas e boas práticas de segurança digital, isto não só salvaguarda os cidadãos, mas também ajuda a construir uma sociedade mais segura na esfera digital

No Brasil, algumas das delegacias especializadas em crimes cibernéticos incluem:

- Delegacia de Repressão aos Crimes de Informática (DRCI) - Rio de Janeiro: A DRCI é uma das mais conhecidas delegacias especializadas em crimes cibernéticos no Brasil. Ela é responsável por investigar delitos relacionados à tecnologia da informação e à internet no estado do Rio de Janeiro;
- Delegacia de Crimes Cibernéticos de São Paulo (DEIC-Cyber): O estado de São Paulo também possui uma delegacia especializada em crimes cibernéticos, que se dedica a investigar casos envolvendo a internet e a tecnologia.

Contudo, os desafios enfrentados por essas delegacias não podem ser subestimados, o ritmo constante da evolução tecnológica significa que elas devem acompanhar as últimas tendências em crimes cibernéticos e métodos de investigação.

Além disso, a escassez de recursos e pessoal especializado é uma preocupação constante, dificultando a eficácia de suas operações.

Em termos de impacto no direito brasileiro e na sociedade, essas delegacias são fundamentais para a aplicação da lei e a manutenção da ordem no ambiente digital. Elas contribuem para a identificação e punição de infratores, reforçando a confiança no sistema de justiça e incentivando o cumprimento das leis cibernéticas.

> Se atentar contra bens jurídicos da União a competência é da Polícia Federal. Nos demais casos, compete à Polícia Civil que, felizmente, cada vez mais conseguem compreender a lógica desses delitos. Mas é preciso ir além. Os agentes que atuam nas delegacias especializadas precisam estar ainda melhor preparados e também é preciso aumentar o contingente, para que essas delegacias consigam acompanhar o crescimento da prática desses crimes. (2017, Daniel Burg)

Em conclusão, as delegacias especializadas em crimes cibernéticos desempenham um papel crítico no contexto do direito brasileiro e na sociedade como um todo, elas são a resposta do sistema legal à crescente complexidade dos crimes digitais, garantindo que o direito seja aplicado de maneira eficaz no mundo digital. No entanto, é fundamental que essas unidades recebam apoio contínuo para enfrentar os desafios em constante evolução e continuar protegendo os interesses legais e a segurança dos cidadãos brasileiros no espaço virtual.

13. METODOLOGIA

O presente trabalho foi realizado através de pesquisas em livros, trabalhos acadêmicos, sites internacionais e nacionais. Buscamos analisar casos recorrentes de vítimas que enfrentam o furto de seus dados e seu decorrer judicial no Brasil, com intuito de conscientizá-las sobre os crimes cibernéticos.

14. CONSIDERAÇÕES FINAIS

É notório a influência gerada pela globalização na sociedade atual em qual estamos inseridos. As mudanças advindas da globalização em sua boa parte são benéficas pois refletem o avanço tecnológico conquistado pelos seres humanos. Em vários âmbitos vemos que esse desenvolvimento fez grandes marcos para nossa qualidade de vida por ter um impacto considerável na saúde, assim como na cultura, economia, política e em diversos outros contextos.

Embora essa evolução tenha trazido grandes oportunidades, é necessário ressaltar como essa era tecnológica também influenciou na criminalidade, já que essa época fez com que se abrisse um leque de oportunidades de realização de crimes de diversas áreas. Os crimes cibernéticos foram os destaques de crimes que aumentaram em comparação anterior ao avanço tecnológico, é explicita a forma como a população foi prejudicada nesse contexto, já que os criminosos encontraram oportunidades para explorar pessoas com conhecimento limitado nessa área. Vemos que a sociedade se tornou dependente do uso da internet e a transformou em algo essencial para viver, por esse motivo criminosos estão se aproveitando desse uso excessivo para realizar crimes

O uso irresponsável da tecnologia traz um desamparo muito grande à população fazendo com que qualquer pessoa esteja vulnerável a se tornar vítima, e boa parte dessa população acredita não ter mal algum em divulgar e tornar público informações pessoais sobre sua vida, esse tipo de atitude e pensamento só facilita o trabalho dos criminosos para a prática de roubos de dados.

15. REFERÊNCIAS BIBLIOGRÁFICAS

Artigos da Internet

Competência territorial do local de hospedagem do site. Disponível em:https://www.jusbrasil.com.br/noticias/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site/2659329 **Acesso em:** 04 de out. 2023, 21h40.

Artigo 70 do Decreto Lei nº 3.689 de 03 de Outubro de 1941. Disponível em: https://www.jusbrasil.com.br/topicos/10674098/artigo-70-do-decreto-lei-n-3689-de-03-de-outubro-de-1941 **Acesso em:** 05 de out. 2023, 10h22.

Código Penal Comentado- Ed. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/art-6-lugar-do-crime-codigo-penal-comentado-ed-2022/1728397253?utm_source=google&utm_medium=cpc&utm_campaign=doutrina_dsa&utm_term=&utmcontent=capitulos&campaign=true&gclid=Cj0KCQjwpompBhDZARIsAFD_Fp-6BQi35s_XYcNxAUvpbKbQw2bNR61dZSa2udsR0jAGmgbYtADxfqcaAuI6EALw_wcB **Acesso em:** 08 de out. 2023, 12h07.

Artigo 88 do Decreto Lei nº 3.689 de 03 de Outubro de 1941. Disponível em: https://www.jusbrasil.com.br/topicos/10671922/artigo-88-do-decreto-lei-n-3689-de-03-de-outubro-de-1941 **Acesso em:** 08 de out. 2023, 13h30.

Maslow na Gestão Jurídica. Disponível em: https://www.jusbrasil.com.br/artigos/maslow-na-gestao-juridica/623888114 **Acesso em:** 15 de out. 2023, 15h45.

Crime Virtual: O que é e como se proteger das ameaças. **Disponível em:** https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm **Acesso em:** 08 de out. 2023, 21h56.

Machado, Rodrigo Bisso, **SSPD-LGPD: uma Solução para Segurança E Privacidade de Dados no cenário da Lei Geral de Proteção de Dados. Disponível em:** https://repositorio.unipampa.edu.br/bitstream/riu/4791/1/Rodrigo%20Bisso%20Machado%20-%202019.pdf **Acesso em:** 10 de out. 2023, 21h56.

Violência Virtual "Internet facilita crimes e dificulta investigação, estimulando a impunidade" Disponível em: https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais **Acesso em:** 31 de out. 2023, 22h06.

Código de Processo Penal Comentado. Capítulo VIII. Disposições Especiais. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/art-88-capitulo-viii-disposicoes-especiais-codigo-de-processopenalcomentado/1353727483#:~:text=88.,ju%C3%ADzo%20da%20Capital%20da%20Rep%C3%BAblica **Acesso em:** 07 de set. 2023, 22h00.

Lei nº 13.709, de 14 de agosto de 2018. (Marco Civil da Internet). 15 ago. 2018. **Disponível em:** https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/nl13709.htm. **Acesso em:** 22 de set. 2023, 19h57.

Lei nº 12.737, de 30 de novembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm **Acesso em:** 15 de set. 2023, 16h36.

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020 .htm **Acesso em:** 22/09/2023, 13h27.

A Evolução do Phishing: Um Exemplo da WatchGuard no mundo real. Disponível em: https://www.watchguard.com/br/wgrd-news/blog/evolucao-do-phishing-um-exemplo-da-watchguard-no-mundo-real **Acesso em:** 27 de out. 2023, 13h16.

RIBEIRO, Paulo Silvino. **“Rousseau e o contrato social”; Brasil Escola. Disponível em:** https://brasilescola.uol.com.br/sociologia/rousseau-contrato-social.htm. **Acesso em:** 15 de out. de 2023, 15:00.

Livros

Myers, D. G. (2004). **Psychology (7th ed.)** New York: Worth Publishers. p. 428.

BARATTA, A. **Criminologia crítica e crítica do direito penal**, trad. Ed. Freitas Bastos. 2ª ed. RJ: 1999.

PABLOS DE MOLINA, A. G. **Criminologia. trad. Luiz Flávio Gomes**, São Paulo: Ed. Revista dos Tribunais, 3ª ed.

Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. 4. ed. São Paulo: Saraiva, 1990.

SILVA, Carlos Afonso Gonçalves da. **Crimes cibernéticos: prevenção e repressão.** São Paulo: Editora Revista dos Tribunais, 2022.

HOBBES, Thomas. **O Leviatã. Col. Os Pensadores.** São Paulo: Ed. Abril, 1984.

16. ANEXO

Artigos da Internet

Lei nº 13.709, de 14 de agosto de 2018. (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. **Acesso em:** 22 de set. 2023, 19h57.

Lei nº 12.737, de 30 de novembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm **Acesso em:** 15 de set. 2023, 16h36.

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiOhdDL37WCAxXnqZUCHXDMD1AQFnoECBYQAQ&url=https%3A%2F%2Fwww.planalto.gov.br%2Fccivil_03%2F_ato2015-2018%2F2018%2Flei%2Fl13709.htm&usg=AOvVaw0bCB9XPoYno7EB18Jtqb4A&opi=89978449 **Acesso em:** 22 de set. 2023, 13h27.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL: promulgada em 5 de outubro ed de 1988. São Paulo: Saraiva, 1990. **Disponível em:** https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwik3J_F3bWCAxXirpUCHenJDTIQFnoECBEQAQ&url=https%3A%2F%2Fwww.planalto.gov.br%2Fccivil_03%2Fconstituicao%2Fconstituicao.htm&usg=AOvVaw3i_8717crw9PBIV4q9Jndm&opi=89978449 **Acesso em:** 20 de ago. 2023, 21h06.

Código de Processo Penal Comentado. Capítulo VIII. Disposições Especiais. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/art-88-capitulo-viii-disposicoes-especiais-codigo-de-processo-penal-comentado/1353727483#:~:text=88.,ju%C3%ADzo%20da%20Capital%20da%20Rep%C3%BAblica **Acesso em:** 07 de set. 2023, 22h00.

Artigo 88 do Decreto Lei nº 3.689 de 03 de Outubro de 1941. Disponível em: https://www.jusbrasil.com.br/topicos/10671922/artigo-88-do-decreto-lei-n-3689-de-03-de-outubro-de-1941 **Acesso em:** 08 de out. 2023, 13h30.

Código Penal Comentado- Ed. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/codigo-penal-comentado-ed-2022/1728397231. **Acesso em:** 08 de out. 2023, 12h07.

Artigo 70 do Decreto Lei nº 3.689 de 03 de Outubro de 1941. Disponível em: https://www.jusbrasil.com.br/topicos/10674098/artigo-70-do-decreto-lei-n-3689-de-03-de-outubro-de-1941 **Acesso em:** 05 de out. 2023, 10h22.