ANTONIO JUSTINO DE ALMEIDA JUNIOR

CRIMES CIBERNÉTICOS NO BRASIL

Suas causas e consequências em decorrência do crescimento da Pandemia do COVID-19.

Cuiabá-MT

2022

ANTONIO JUSTINO DE ALMEIDA JUNIOR

CRIMES CIBERNÉTICOS NO BRASIL

Suas causas e consequências em decorrência do crescimento da Pandemia do COVID-19.

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da FACULDADE FASIPE CUIABÁ, como requisito para a obtenção do título de Bacharel em Direito.
Orientador: Profº Sonny Jacyntho Taborelli da Silva

Cuiabá-MT

2022

ANTONIO JUSTINO DE ALMEIDA JUNIOR

CRIMES CIBERNÉTICOS NO BRASIL
Suas causas e consequências em decorrência do crescimento da Pandemia do COVID-19.

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito – FACULDADE FASIPE CUIABÁ como requisito para a obtenção do título de Bacharel em Direito.

Aprovado em:

Professor Orientador: Sonny Jacyntho Taborelli da Silva
Departamento de Direito – FACULDADE FASIPE CUIABÁ

Professor Avaliador: Ronildo Medeiros Junior
Departamento de Direito – FACULDADE FASIPE CUIABÁ

Professor Avaliador: Sonny Jacyntho Taborelli da Silva
Departamento de Direito – FACULDADE FASIPE CUIABÁ

Professor Avaliador: Ronildo Medeiros Junior
Departamento de Direito – FACULDADE FASIPE CUIABÁ
Coordenador do Curso de Direito

Cuiabá-MT

2022

DEDICATÓRIA

Dedico esse trabalho à minha família e aos meus familiares que torcem por mim de forma encantadora e não medem esforços para que meu sucesso seja conquistado e especialmente à memória de saudosa de minha Mãe.

AGRADECIMENTOS

Agradeço a Deus por ter me sustentado até aqui e amparado meus estudos com sabedoria.
Aos meus filhos e enteados, minha esposa, familiares e amigos, que são à fonte de inspiração para meu sucesso profissional.
Aos meus professores e ao meu orientador Sonny Jacyntho Taborelli da Silva, por seus ensinamentos, pela paciência e incentivo, sem ele não seria possível a conclusão deste trabalho.
Enfim, a todos meus colegas que de alguma forma colaboraram para que eu chegasse até aqui.
Obrigado.

EPÍGRAFE

“A injustiça em qualquer lugar é uma ameaça à justiça por toda parte.”

Martin Luther King

ALMEIDA, Antonio, **Crimes Cibernéticos No Brasil** – Suas causas e consequências em decorrência do crescimento da Pandemia do COVID-19. 2022. 30f. Trabalho de Conclusão de Curso – FACULDADE FASIPE CUIABÁ

RESUMO

O presente trabalho tem como objeto de estudo as causas e consequências dos crimes cibernéticos, como eles aumentaram durante o período pandêmico no Brasil e as legislações que foram criadas para proteger o usuário. Com a população restritamente proibida de sair de sua residência, houve um salto nos golpes aplicados pela internet, pois assim então realizavam muitas compras e serviços pela internet. A metodologia empregada foi a pesquisa em sites e livros sobre a tipificação deste crime e pesquisas informativas sobre o número de golpes. Ademais, podemos concluir que além das pessoas terem que tomar muito cuidado ao realizar compras pela internet, há a necessidade de leis mais severas para a devida punição e também é apresentado as lacunas na lei sobre o respectivo tema.

Palavras Chave: Crimes Cibernéticos. Pandemia. Segurança.

ALMEIDA, Antonio. CYBER CRIMES IN BRAZIL-Its causes and consequences as a result of the growth of the COVID-19 Pandemic. 2022. Trabalho de Conclusão de Curso – FACULDADE FASIPE CUIABÁ

ABSTRACT

The present work has as its object of study the causes and consequences of cyber crimes, how they increased during the pandemic period in Brazil and the laws that were created to protect the user. With the population strictly prohibited from leaving their homes, there was a jump in scams applied over the internet, as they made many purchases and services over the internet. The methodology used was research on websites and books on the typification of this crime and informative research on the number of scams. In addition, we can conclude that in addition to people having to be very careful when making purchases over the internet, there is a need for stricter laws for due punishment and the gaps in the law on the respective topic are also presented.

Keyword: Cyber Crimes. Pandemic. Security.

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

A Internet é uma conexão de redes em escala mundial, através de milhões de computadores que permite o acesso a informações e todo tipo de transferência de dados (PINHEIRO, 2007).

A globalização do mundo atual trouxe diversas mudanças, em meio aos diversos avanços tecnológicos, a internet se tornou fundamental na vida da população, diante da era da tecnologia da informação, percebe-se a importância que a informática possui no momento, ressaltando que a maioria das pessoas, físicas ou jurídicas, "depende do seu dispositivo informatizado, que variam de um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa" (BRITO, 2013, p. 7).

Com isso, teve-se um aumento de ações criminosas de um modo geral, com o aparecimento de grandes escândalos, como, por exemplo, as manipulações de caixas bancários, abusos em processo de telecomunicação, aparecimento em grande escala de pirataria de programas e também a pornografia infantil (OLIVEIRA JÚNIOR, 2013).

Com o isolamento causado pela Pandemia do COVID-19, as pessoas passaram a estar cada vez mais conectadas, a internet se tornou uma necessidade, porém, mesmo diante das coisas boas que ela permite que sejam realizados, existem aqueles que sempre recorrem a métodos ilícitos buscando o ganho próprio sobre os outros.

Antes da pandemia, o Brasil já se encontrava entre os países que mais sofriam ataques cibernéticos, dividindo este ***ranking*** com China, Estados Unidos, Índia e Japão, de acordo com um relatório global divulgado pela ***Symantec***. Porém entre Fevereiro de 2019 a Fevereiro de 2020, os números de casos de ciberataques cresceram em número recorde de 308,17%, de acordo com dados da empresa ***Axur***.

Deve se muito o aumento significativo à adoção do trabalho por ***home office*** por várias empresas, às aulas na modalidade de ensino a distância e às horas adicionais que cada pessoa passou no computador ou celular. O uso a mais da internet pelos usuários reacendeu o interesse dos ***cibers*** criminosos por este tipo de ataque.

O método de pesquisa a ser empregado no desenvolvimento do presente trabalho, iniciara-se pela análise dos crimes cibernéticos que mais tiveram crescimento durante a Pandemia, bem como seus conceitos.

O trabalho se desenvolverá a partir de uma pesquisa teórica a cerca do assunto, levantamentos bibliográficos, revistas, revistas eletrônicas, artigos, entre outros recursos que serão amplamente explorados.

Podemos analisar que os ciberataques vem se tornando cada vez mais frequente, mesmo com tantas Leis e políticas de proteção aos dados pessoais, principalmente neste período de pandemia que é o foco desde trabalho.

O Trabalho será voltado em estudar alguns dos principais crimes que são cometidos via internet e mostrar a importância de que estes tenham tipificação legal específica, pois a falta dela que é encontrada hodiernamente no ordenamento jurídico brasileiro faz-se gerar uma lacuna legislativa que encoraja a continuidade da prática delitiva, tornando assim difícil a punição daqueles que se aproveitam dessa falta de previsão legal.

A temática aplicada neste trabalho, deixará evidenciado que o Direito está diretamente ligado a sociedade e a evolução da mesma, conforme a sociedade se desenvolve o direito tem por objetivo de acompanhá-la.

Com os avanços tecnológicos, fez-se necessário que o Direito tutele aqueles que são vítimas dos crimes que passaram a ser perpetuados em ambiente virtual.

Assim o presente trabalho buscará verificar as formas de se analisar um crime virtual, a busca de sua autoria, suas peculiaridades.

Os objetivos específicos do trabalho são a apresentação de alguns dos crimes cibernéticos (virtuais); as tipologias de crimes cibernéticos, suas causas e consequências, analisar a legislação nacional em relação aos crimes cibernético, o questionamento sobre leis com penas mais severas contra crimes cibernético e como nos protegermos e denunciá-los.

2. CRIMES CIBERNÉTICOS

Crimes cibernéticos ou cibercrimes são práticas ilícitas que acontecem no ambiente virtual e podem envolver desde invasões de sistema, roubo de dados pessoais, falsidade ideológica, até práticas de injúria cometidas na internet.

Assim, para que eles sejam realizados, os infratores usam computadores com o objetivo de atingir redes públicas, privadas ou domésticas.

De acordo com o Departamento de Justiça dos Estados Unidos, os crimes cibernéticos podem ser divididos em três categorias principais:

- **Cibercrimes puros:** são aqueles em que o computador é o alvo dos infratores. Ou seja, quando o sistema (pessoal ou corporativo) sofre um ataque.
- **Cibercrimes mistos:** acontecem quando o sistema de computador é usado como "arma" para a prática dessas ações.
- **Cibercrimes comuns:** são aqueles em que o computador é usado como um acessório, apenas para guardar informações ilegais e roubadas.

Infelizmente, ninguém está impune a fraude e golpes na internet. Tanto pessoas físicas quanto jurídicas podem ser vítimas de ciberataques.

2.1 O que são crimes cibernéticos na Doutrina

As características sobre como os crimes virtuais são tipificados, assim, poderemos entender como as leis tendem a ser criadas em relação a crimes que ainda não estão legislados, possibilitando a prevenção e o amparo sobre esse tipo de ataque.

Então, descreverei o que é um crime virtual, qual o possível perfil dos criminosos que o praticam, quais os principais crimes cometidos no Brasil e sua relevância para que leis destinadas ao combate sejam desenvolvidas para proteção da população.

O crime cibernético, também conhecido crime virtual, refere-se as ações ilegais cometidas por meio da tecnologia ou por meio recursos informáticos, trata-se de um comportamento ilegal

onde o autor recorre a um computador, celular, ou qualquer outro aparelho de informática ou que pode ser conectado à internet, justamente pela aplicação ser realizada em ambiente virtual (JORGE; MILAGRE, 2016).

Na doutrina, os crimes cibernéticos são divididos em crimes próprios e crimes impróprios, a qualificação como crime próprio ocorre quando as ações do autor do crime visam prejudicar um sistema ou infringir dados, como por exemplo, invasão de sistemas para destruir ou impedir o funcionamento de um servidor de um site ou de uma empresa.

A qualificação como crimes impróprios ocorre quando se trata de um crime que também pode ser realizado fora da internet, como por exemplo o estelionato, nos crimes impróprios, destacam-se como mais comum na internet o discurso de ódio, neste caso, por mais que a liberdade de expressão seja um direito garantido por lei, não se pode ultrapassar os limites dos direitos de terceiros e se opor à imagem, privacidade, honra, intimidade, porque pode se figurar em crimes contra a honra, assédio ou difamação (AZEVEDO; CARDOSO, 2021).

2.2 Tipos de crimes cibernéticos

Os crimes mais populares que nós estão presentes em nosso dia a dia são:

- Fraudes por e-mail e usando a Internet;
- Interceptação de informações pessoais de terceiros ou dados sigilosos de organizações e empresas;
- Roubo de dados financeiros ou credenciais bancárias de terceiros — sejam indivíduos ou organizações;

Invasão de computadores pessoais, de empresas ou redes de computadores;
Extorsão cibernética e ***ransomware*** (sequestro de Informações);
Crimes com estrutura tipo ***phishing***, muito comum em golpes que se espalham pelas redes sociais e por ***apps*** de mensagens, como ***whatsApp***;
Violação de direitos autorais;
Venda de itens ilegais por meio da Internet;
Incitação, produção ou posse de pornografia infantil;
Discurso de ódio — publicações de teor homofóbico, xenófobo e racista — e apologia ao nazismo. (Fonte: Sakate (2020, p. 1).

Conhecidos também por ***phishing*** (roubar dados pessoais, senhas, dados financeiros, bancários, número de cartão de crédito) e por se tratar de um ataque mais comum, é possível atualizar a legislação combatendo tais crimes em particular, e mostrar que o direito penal precisa sempre estudar os crimes que estão sendo perpetrados pela Internet no mundo para que a proteção de usuários mais rápida e eficaz.

O termo ***phishing*** vem do termo ***fishing***, que significa pescar em inglês, ou seja, os criminosos recorrem a mensagens falsas que são compartilhadas entre as pessoas, servindo como isca. Assim, aguardam pacientemente até que alguém fisgue e passe suas informações pessoais.

As informações são passadas porque geralmente são utilizados sites clonados de empresas reais, então, a pessoa sem perceber, ao tentar entrar com seu acesso, acaba fornecendo sua senha sem perceber, que pode ser utilizada pelos criminosos que a registram.

Se trata, então, de uma fraude eletrônica e um ataque sério, pois quem comete a fraude pode obter da vítima as senhas, dados financeiros, cartões de crédito e outras informações.

Esse golpe ainda pode ser dividido em métodos, onde o mais comum é chamado ***Scam***, ele consiste no envio de ***e-mails*** fraudulentos de uma empresa conhecida do público, tentando persuadir a vítima que se tratam de informações verdadeiras, levando a uma página clonada que, geralmente, solicita que as informações pessoais sejam colocadas, na maioria dos casos, informações confidenciais como um número de conta, senha da conta pessoal, senha do cartão.

Além ***Scam***, também podem recorrer as outras fontes, sendo o envio via aplicativos o segundo maior, o aplicativo ***WhatsApp*** se tornaram algo cultural de uso, principalmente na interação em grupos, muitos casos de compartilhamento de ***links*** fraudulentos podem ser recebidos expondo as pessoas ao perigo.

Esse tipo de ataque aumentou muito o número de vítimas em todo o mundo. Ameaças, desvio de fundos públicos, extorsão, roubo de identidade, perseguição e clonagem de cartão são apenas algumas das ameaças representadas por esses ataques hoje.

Estima-se que, nos últimos anos, esse tipo de mídia tenha se tornado um dos favoritos para a mineração de informações e a taxa de uso dos profissionais tenha aumentado consideravelmente.

Além de usar mensagens aleatórias para esperar que alguém caia neste golpe, os criminosos que implementam ***phishing*** também combinam técnicas de engenharia social e manipulação de informações e clonagem de páginas para enganar vários perfis de usuários.

Permite manipulá-lo indiretamente simulando um site oficial, tentando roubar os dados pessoais da vítima pela sua própria ingenuidade. Portanto, o uso de nomes de bancos, lojas e empresas famosas é a base da prática deste ataque, criando réplicas quase perfeitas para obscurecer qualquer possibilidade de identificação.

Por exemplo, quando um conhecido ou parente compartilha uma mensagem no grupo falando sobre uma promoção de uma loja, sendo necessário apenas realizar o acesso para participar, a pessoa, por observar que foi enviada por conhecido, acaba confiando no ***link*** enviado, porém, ambos podem ter se tornado vítimas do criminoso, que recebe o acesso com os dados de senhas dessas pessoas, isso ocorre principalmente na versão ***mobile***, numa tentativa de golpe utilizando uma página falsa, onde o site direciona para que a pessoa coloque seus dados, que pensa que está atualizando sua conta.

Como nesses casos, o golpe pode ser enviado por aplicativos de mensagens, é mais fácil para os criminosos enganar as vítimas, que fazem menos checagens pelo celular, em comparação ao que seria o ***site*** via computador.

Conforme recomendações de segurança que são sempre informadas é possível identificar quando uma página ou aplicação fraudulenta, o primeiro passo é observar o ***site***/aplicativo, devendo observar erros gramáticas grotescos ou redirecionamento para outra página desconhecida na ***URL***.

Em pesquisa realizada pela empresa de antivírus ***Kapersky***, o Brasil ocupa a primeira posição no mundo em ataques de ***phishing,*** onde se descobriu que mais de 30% dos internautas do país haviam sofrido pelo menos uma tentativa de golpe, a posição foi assegurada., sendo que o ***phishing de WhatsApp*** é atualmente a prática mais comum.

Mesmo que a identificação dos ***sites*** fraudulentos possa ser realizada apenas observando com atenção os ***sites*** acessados, outro motivo que torna esses ataques tão propícios ao sucesso remete ao erro humano e a falta de preocupação aos possíveis problemas e vulnerabilidades do sistema.

Como o ***phishing*** consiste num golpe fácil e barato para ser aplicado, as pessoas não imaginam que o ***site*** acessado se trata de uma página clonada que visa a coleta de dados pessoais para serem usados em golpes e clonagem de cartão. (***KAPERSKY***, 2018).

Outro muito comum é o golpe do cartão de crédito ou boleto bancário. Na maioria das vezes, ele é feito com um ***software*** malicioso que infecta as máquinas com o objetivo de roubar senhas bancárias ou do cartão.

No caso do de um boleto bancário, os criminosos geram um documento simulando a compra de um ***e-commerce*** ou compra que a pessoa fizer. Nesse momento, o código de barras é trocado e o dinheiro pago vai para outra agência e conta. O consumidor só descobre que caiu no golpe quando a empresa cobra o pagamento do produto novamente.

À medida que a tecnologia se torna cada vez mais segura e eficiente para os humanos, essa prática se torna mais comum porque não necessita que o próprio criminoso invada o celular da vítima, pelo contrário, é a vítima que acaba passando seus dados sem perceber.

Essa relação entre a prática do crime e a estratégia utilizada parece difícil de entender, porém, trata-se de uma estratégia de ponte para um crime maior, seja roubo de informações pessoais, fotos privadas, clonagem de cartões, informações confidenciais da empresa. (SILVA, 2021).

2.3 Criação da Lei nº 12.737/12 – Lei Carolina Dieckmann

Em maio de 2011, o computador pessoal da atriz foi invadido e cerca de 36 fotos íntimas foram copiadas, o criminoso exigiu uma quantia de R$ 10 mil para que as imagens não fossem publicadas, com a recusa da artista, as fotos pessoais acabaram sendo divulgadas na internet e replicada por diversos internautas.

Criada e sancionada a Lei nº 12.737/12, também conhecida como Lei Carolina Dieckmann, surgiu após um grande debate popular sobre o vazamento não autorizado de imagens íntimas. Essa, inclusive, foi a primeira alteração no Código Penal Brasileiro que tipificou os chamados crimes cibernéticos.

Na ocasião, o projeto de lei, apresentado no dia 29 de novembro de 2011, acabou sendo aprovado rapidamente, já que havia uma grande pressão da mídia e debate popular sobre o assunto. Assim, a legislação foi aprovada em um período de um ano.

Essa Lei veio tipificar e alterar o Código Penal Brasileiro, acrescentando, dois artigos, o art. 154-A e 154-B, alterando também a redação dos artigos 266 e 298.

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa".
> (BRASIL, 2012).
>
> "Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos".
> (BRASIL, 2012).
>
> Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passam a vigorar com a seguinte redação:
>
> "**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
>
> Parágrafo único (Revogado).. .....
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública
> (BRASIL, 2012).
>
> Pena – detenção, de um a três anos, e multa.

> "**Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro"**
>
> Pena – reclusão, de um a cinco anos, e multa.
>
> **Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012)**
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito".
>
> (BRASIL, 2012).

Mesmo com a Lei sancionada, não foi o suficiente para diminuir o número de crimes no país, porém, em 2014 foi regulamentada a lei do Marco Civil da Internet (Lei n. 12.965/14), essa nova lei refere-se a segurança e o direito individual dos usuários e provedores da internet.

2.3 Marco Civil da Internet (Lei n. 12.965/14)

A Lei n.º 12.965/14 foi submetida à Assembleia Nacional em 2011 pelo chefe do Poder Executivo, transformando-a na Lei n.º 2.126/2011. Assim, foi publicado em 23 de abril de 2014. Seu principal objetivo é estabelecer princípios, garantias e obrigações para o uso da Internet no Brasil. A Lei n° 12.965/14, popularmente conhecida como Marco Civil da Internet certifica um procedimento mais ágil para a remoção de mídias íntimas que foram expostas no ambiente virtual, e a Lei nº 13.718/2018, que adicionou um novo delito para o art. 218-C, do Código Penal:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática –, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena – reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
> (BRASIL, 2018).

Devido a crescente funcionalidade que a internet foi adquirindo e seu acesso foi se tornando essencial à vida das pessoas, a lei foi criada com a intenção de regularizar essas utilizações e eliminar a idéia de que a internet é uma "terra sem lei". (Nascimento 2019).

Explica que o Marco Civil da Internet ficou popularmente conhecido como a Constituição da 22 Internet Brasileira e é composto de 10 (dez) princípios elaborados pelo Comitê Gestor da Internet brasileira. Os princípios previstos na Lei do Marco Civil são:

> [….] liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimputabilidade da rede; funcionalidade, segurança e estabilidade; padronização e interoperabilidade; e ambiente legal e regulatório. (NASCIMENTO, 2019, p.18)

Seguindo esses princípios, a lei também permitiu a tipificação de diversos termos informáticos, como registro de conexão, sendo o conjunto de dados sobre a hora inicial e final do acesso à internet.

E os registros de acesso a aplicações de internet, constando os dados de acessos realizados, sendo descrito a hora e a data, a partir de determinada aplicação (BRASIL, 2014).

O registro da conexão é mantido pelo provedor de acesso, composto pelas pessoas jurídicas que prestam serviços de acesso à Internet em banda larga. O registro da conexão é mantido pelo provedor de acesso, que é composto pelas pessoas jurídicas que prestam serviços de acesso à Internet em banda larga (LIMA, 2016).

Em Recurso de Habeas Corpus 117.680 do Pará, em 2020, o Superior Tribunal de Justiça entendeu que o tempo de registro se configura no fluxo de comunicações que relatam os acessos e as funcionalidades acessadas pelo terminal com internet, evitando que o autor do ato testemunhe sobre o período de tempo de uso e acesso, sendo característica estatística que pode ser utilizada nos julgados (BRASIL, 2020).

Mesmo assim, ainda é forte dificuldade na punição de criminosos virtuais, principalmente porque é um desafio investigativo encontrar quem se esconde no anonimato. Além da aplicabilidade efetiva das leis existentes, outras leis ainda precisam ser formuladas para efetivar a condição atual de combate (JESUS; MILAGRE, 2016).

Outra crítica apontada refere-se ao caráter simbólico que o Marco Civil da Internet representa, porque muito de seus artigos relatam condições jurídicas constitucionais, logo, se torna

passível de entendimento legislativo para que suas prerrogativas sejam exercidas (RODRIGUES, 2014).

Além disso, o artigo 19 da lei também estipula outros requisitos para a responsabilidade penal do cumprimento, na qual um mandato só é permitido mediante descrição clara e completa sobre o que se deseja buscar e quais os principais serviços informáticos estão sendo utilizados (BRASIL, 2014).

É por isso que no fim, uma das mais importantes atividades a serem realizadas cabe na orientação dos cidadãos, principalmente crianças e adolescentes usuários de redes digitais sobre seus direitos de dados e, principalmente, da responsabilidade dos prestadores de serviços digitais que são a base para que as instituições judiciárias enfrentem as infrações e os riscos da sociedade da informação que podem estar sujeitos a choques tecnológicos (JESUS; MILAGRE, 2016).

3. O COMBATE AO CIBERCRIME NA ATUALIDADE

Nos últimos três anos, existiram três principais condições que remetem ao cibercrime e merecem destaque, sendo o primeiro a Lei Geral de Proteção de Dados Pessoais, que visou tipificar e melhorar o controle de acesso e de armazenamento de dados, melhorando questões não avaliadas no Marco Civil da Internet.

A questão da pandemia do COVID-19 e como os cibercrimes estão sendo autuados, sendo importante para verificar se naquele momento de isolamento, onde as pessoas necessitaram estar mais conectadas na internet, se os casos reduziram ou aumentaram.

E por último, a lei que foi sancionada em 2021, buscando solucionar um dos principais problemas observados ao longo desta temática, sobre a quantidade da pena dos culpados, de forma que melhore o processo de combate ao cibercrime, principalmente no decorrer da pandemia do COVID-19.

3.1 Criação da Lei Geral de Proteção de Dados

Foi sancionada a lei nº 13.709 em 14 de agosto de 2018, que ficou conhecida como Lei Geral de Proteção de Dados (LGPD), teve como principal objetivo proteger os direitos fundamentais de liberdade e privacidade, além de possuir um respaldo na para a segurança jurídica dos usuários da internet.

A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes, esclarece ainda que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação.

Além disso, a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada.

A lei autoriza também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos.

Além disso, é necessário o consentimento do usuário para que haja o tratamento da legislação, regra excepcionada nos casos previstos no art. 11, II, da Lei.

No Brasil a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD é a responsável em fiscalizar e aplicar penalidades, ela também terá a tarefa de regulamentar e orientar preventivamente os usuários.

A Lei traz punições severas em multas, que começam a ser aplicadas a partir de 1º de Agosto de 2021, após três anos de sua sanção, vejamos:

> I – advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III – multa diária, observado o limite total a que se refere o inciso II;
>
> IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI – eliminação dos dados pessoais a que se refere a infração. “ (MPF, 2022)

Este intervalo possibilitou justamente que as empresas pudessem se adaptar, e a entrada em vigor das sanções dará ainda mais proteção ao consumidor e segurança ao mercado brasileiro que ingressa no rol de mercados internacionais com a proteção de seus dados.

As exigências valem tanto para as lojas físicas quanto para as virtuais, situadas no Brasil ou no exterior que ofereçam serviços para pessoas localizadas no País.

O órgão acaba de elaborar uma minuta submetida à consulta pública com questões sobre a contagem de prazos, atividades de fiscalização e monitoramento e diante disso, que as empresas começaram a implementar o LGPD ao seu dia a dia.

3.2 DO COMBATE AO CIBERCRIME DURANTE A PANDEMIA

A pandemia do COVID-19 nos tornou mais solitários devido ao isolamento social, porém, ficamos mais conectados na internet, em casa, estamos cada vez mais habituadas a participar de redes sociais, videochamadas, grupos da família, encontros virtuais, dentre outras habilidades obtidas pelo uso da tecnologia (BOTTINI, 2020).

O isolamento social acarretou um maior uso dos recursos tecnológicos e teve um impacto no campo do crime. Os crimes que exigem que as vítimas sejam fisicamente vulneráveis diminuíram.

Em março de 2020, São Paulo viu uma redução de 13.917 furtos, representando uma queda de 30% em relação ao total de crimes do mesmo período do ano passado.

Da mesma forma, o tráfico de drogas diminuiu devido à falta do comércio aberto e à dificuldade de obtenção de matéria-prima para a fabricação de compostos ilegais, por outro lado, o número de ataques a mulheres aumentou 44,9%, e a morte de mulheres aumentou 46,2% (BOTTINI, 2020).

Em relação aos crimes virtuais, com o isolamento, as pessoas buscam realizar a maioria de suas atividades online, seja compras, trabalho, envio de dinheiro, a insegurança e a falta de compreensão desses mecanismos de aquisição e transferência virtual de mercadorias tornam as pessoas passíveis a diversos golpes, como páginas falsas de bancos e lojas na Internet, muitas das quais veiculam anúncios promocionais imperdíveis (BOTTINI, 2020).

A ***TransUnion***, empresa global destinada a análise de dados, confirma novamente que o crime virtual mais comum no Brasil durante a pandemia de COVID-19, foi o ***phishing***, que é o uso de isca para roubar dados, como recompensas eletrônicas ou cobranças falsas (SAKATE, 2020).

Ao mesmo tempo, em análise ao estudo da ***TransUnion***, percebeu que um em cada quatro brasileiro já foi vítima de crimes envolvendo cartões de crédito.

Em entrevista realizada com a população sobre os possíveis crimes que cada pessoa já pode ter sofrido, a Tabela 1 pode perceber os seguintes dados.

Tabela 1 – Porcentagem de casos envolvendo cibercrime, com cada pessoa relatando mais de um caso

Tipo de crime	Porcentagem
Phishing (roubo de dados)	27%
Golpe de falsos vendedores varejo online	21%
Fraude envolvendo caridade de arrecadação de fundou	19%
Golpe em desempregados	18%
Vacina de COVID-19, curas e testes	15%
Fraude em seguros	15%
Fraude de envio de produtos	14%
Roubo de identidade	14%
Cartão de crédito roubado ou cobrança fraudulenta	13%
Golpe do “benefício do governo”	12%

Fonte: Sakate (2020, p. 1).

Novamente o ***phishing*** aparece na liderança, o que significa que mediante a pandemia do COVID-19, esse tipo de golpe se mantém com alta frequência na população, podendo ressaltar também alguns golpes específicos ao período, como golpes envolvendo a vacina do COVID-19 e os golpes do “benefício do governo” (SAKATE, 2020).

Infelizmente, devido à quantidade de notícias falsas espelhadas nas redes sociais e aplicativos, ataques de hackers a órgãos públicos e vazamentos de dados pessoais de milhões de brasileiros, estima-se que mais de 11 milhões de acessos e compartilhamentos foram realizados sobre golpes informáticos, observando a gravidade deste problema no país, que também se intensifica com o compartilhamento de notícias falsas (***Fake News***) (BOTTINI, 2020).

Mesmo reconhecendo avanços, como a promulgação da Lei Geral de Proteção de Dados e a criação da Autoridade Nacional de Proteção de Dados (ANPD), é ainda questionado sobre o que pode ser feito para proteger melhor os cidadãos contra esse tipo de crime, (Sen. Carlos Viana-MG,2021)

Porém, mesmo diante dessa condição, em 2021, foi aprovada mais uma lei com objetivo de aumentar a segurança frente aos cibercrimes, demonstrando que mesmo diante das dificuldades que o país enfrenta, o Direito busca adequações conforme a possibilidade legislativa.

3.3 Criação da Lei nº 14.155/2021

No dia 28 de maio de 2021, foi sancionada a Lei nº 14.155/2021, pelo presidente Jair Bolsonaro, que altera o Código Penal e torna mais graves os crimes de violação de privacidade de dispositivo informático, para furto e estelionato, aumentando o tempo de reclusão.

Conforme a nova redação do Código, o crime de invasão de dispositivo informático passará a ser punido com reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. Antes, a pena aplicável era de detenção de três meses a um ano e multa.(Fonte: Senado,2021)

A penalidade também valerá para quem invadir um dispositivo a fim de obter, adulterar ou destruir dados ou informações sem autorização do dono, ou ainda instalar vulnerabilidades para obter vantagem ilícita, se a violação tiver obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado, a pena será de reclusão de dois a cinco anos e multa, a pena anteriormente era de seis meses a dois anos e multa. Na tabela abaixo é mostrado à comparação.

Tabela 2 – Comparação da Redação Art. 154-A

Redação Original	**Redação Atual**
Art. 154-A. Invadir dispositivo informático **alheio**, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.	Art. 154-A. Invadir dispositivo informático **de uso alheio**, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico	§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico
§ 3º (…) Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.	§ 3º (…) Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa, e multa

Fonte: EstrategiaConcursos (2021).

Furto

No caso do crime de furto, não houve modificações estruturais no tipo, cabendo a análise da norma forma qualificada e da inclusão de causas de aumento de pena pela Lei 14.155/2021.

A lei acrescenta ao Código Penal o agravante do furto qualificado por meio eletrônico, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento similar. Nesse caso, a pena será de reclusão de quatro a oito anos e multa.

Se o crime for praticado contra idoso ou vulnerável, a pena aumenta de um terço ao dobro. E, se for praticado com o uso de servidor de informática mantido fora do país, o aumento da pena pode ir de um terço a dois terços. (Fonte: Senado,2021)

Estelionato

O texto inclui no Código Penal que a pena do estelionato será de reclusão de quatro a oito anos e multa quando a vítima for enganada e fornecer informações por meio de redes sociais.

Anteriormente o estelionatário — indivíduo que engana alguém e causa prejuízo a essa pessoa para obter vantagem ilícita — podia ser punido com pena reclusão de um a cinco anos e multa. (Fonte: Senado,2021)

Assim como no furto qualificado, a pena para estelionato via meio eletrônico é aumentada se for utilizado servidor fora do território nacional ou se o crime for praticado contra idoso ou vulnerável, quando o estelionato for praticado por meio de depósito, emissão de cheques sem fundos ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima.(Fonte: Senado,2021)

> “A atual orientação jurisprudencial acaba por estabelecer o império da impunidade em relação a essas fraudes, com grave prejuízo à administração da justiça e à sociedade em geral”.
> (Rodrigo Cunha)

Dessa forma, além da legislação específica para crimes no campo virtual, também devem ser respeitados os princípios e direitos básicos estipulados na Constituição Federal de 1988.

Portanto, permite o amparo sobre os direitos protegidos, enfatizando a dignidade humana e constitucionalidade das regras para lidar com o crime cibernético, é notável que a forma de sociedade vem mudando, a Legislação também deve acompanhar tais mudanças, diante disso a criação e leis mais severas em relação aos crimes cibernéticos visam garantir uma maior segurança ao usuário que utiliza a internet.

3.4 Como prevenir dos Crimes Cibernéticos

Com o isolamento social, crimes virtuais, tornaram-se cada vez mais comuns, esclareci alguns tipos de crimes, a evolução das leis e agora vou comentar como se proteger e denunciar.

Senhas roubadas, boletos falsos, computadores invadidos, ***cyberbullying***, estelionato, discurso de ódio, entre outros, seja para fins de trabalho, estudo ou lazer, o fato é que a pandemia fez com que as pessoas permanecessem cada vez mais conectadas.

Contudo, embora cada vez mais usuários tenham acesso a recursos digitais, grande parte ainda não sabe se prevenir contra crimes cibernéticos, por isso, entender o que são e como se proteger de crimes praticados pela internet é fundamental. Igualmente, é crucial saber como denunciá-los e conhecer os seus direitos, caso se torne vítima.

Por isso, fique atento a estas orientações:

- Não abra links ou anexos de e-mails desconhecidos;
- Verifique a extensão do site que deseja abrir;
- Ative a confirmação em duas etapas de seu ***whatsapp*** para aumentar a segurança;
- Evite comprar de lojas ou vendedores desconhecidos;
- Confira a reputação da loja em sites especializados, como “Reclame Aqui” ou o “***E-bi***t”;
- Jamais forneça sua senha a ninguém;
- Ao receber ligações duvidosas de seu banco, desligue e retorne para seu gerente, a fim de confirmar a informação;
- Não instale arquivos enviados pelas redes sociais ou e-mails;

- Mantenha seu antivírus e atualizações de seus dispositivos móveis em dia;

Tenha em mente que se prevenir de crimes praticados pela internet sempre será a melhor opção, todavia, é possível se tornar vítima de um crime virtual mesmo adotando as precauções cabíveis.

Se for o caso, veja de que forma é possível denunciar um crime cibernético:

- Primeiramente, colete o máximo de evidências possíveis que possam comprovar a ação criminosa;
- *Prinos* de telas, trocas de mensagens e de e-mails, documentos, fotos, número do celular que originou o golpe ou as agressões, endereços de perfis: tudo contribui para endossar sua a denúncia;
- Registre uma ata notarial em cartório, incluindo todas as provas documentais reunidas;
- Compareça a um órgão competente que poderá dar encaminhamento ao seu caso. Entre eles, estão: delegacias físicas ou virtuais (para registro de Boletim de Ocorrência), Conselho Tutelar (quando há envolvimento de menores) ou mesmo o Ministério Público.

Além disso, é possível recorrer a delegacias especializadas em crimes virtuais, disponíveis em alguns estados do Brasil.

Para crimes relacionados à pornografia infantil, discurso de ódio e apologia ao nazismo, há como realizar uma denúncia anônima no site da ***Safernet***, outra opção é ir até uma delegacia de polícia e registrar um boletim de ocorrência. (Fonte: Jus.com, 2021)

4. CONSIDERAÇÕES FINAIS

Considerando a problemática se atualmente existem leis suficientes para o combate legislativo dos cibercrimes, sabemos que ainda não existem leis suficientes baseados nos seguintes motivos: poucas leis para o setor, e sanções que não inibem a prática sobre os crimes virtuais.

Por mais que o país dispõe de três leis totalmente focadas na internet, elas ainda precisam de mais formulações para que a população seja amparada corretamente.

Tratando nas leis, é perceptível que o país precisa criar uma sanção especializada sobre a prática do phishing, que se mantêm como ataque mais frequente no país, se agravando durante a pandemia do COVID-19.

Pode-se destacar que essa lei poderia estar vinculada a LGPD, uma vez que os dados roubados pelos criminosos agora estão regidos nela.

Nesse sentido, a LGPD pode ser considerada um marco a ser adaptado para melhorar o processo de criminalização referente a conduta dos dados pessoais, ao mesmo tempo, foi observado que muitas leis possuem a conduta de violação de dados, cujos crimes estão diretamente relacionados aqueles dispostos no Código Penal.

Outro principal destaque negativo vai para a pena dos crimes virtuais, que eram de apenas 3 meses até um ano, e multa. Numa tentativa clara de melhorar essa situação, a Lei 14.155/2021 buscou aumentar a quantidade da pena possível nos crimes informáticos, porém, devido a promulgação da lei ser muito recente, ainda não é possível observar os impactos dela no combate ao crime.

O Direito brasileiro ainda caminha devagar quando se trata da criação de leis voltadas para prevenção de crimes virtuais, seja devido à dificuldade legislativa em relacionar os contextos e dificuldades que a informática traz para a análise jurídica, ou pela rápida atualização dos tipos de golpes ou de recursos informáticos utilizados que dificultam a criação de leis específicas.

5. REFERÊNCIAS

ABRUSIO, Juliana Canha; BLUM, Renato Ópice. **Crimes eletrônicos**.
Disponível em: https://www.sedep.com.br/artigos/sociedade-tem-de-se-preocupar-com-crimes-eletronicos/
Acesso em: 16 ago 2021.

ALENCAR, Morgana. **Tire as suas dúvidas sobre o Marco Civil da Internet.** 2019.
Disponível em: https://www.aurum.com.br/blog/marco-civil-da-internet/.
Acesso em: 16 ago 2021.

ANGELO, Fernanda K. **Brasil lidera ranking mundial de hackers e crimes virtuais**. Folha Online, 2002.
Disponível em: ttps://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml.
Acesso em: 13 set 2021.

AZEVEDO; J. S. de.; CARDOSO, T. M. **Crimes cibernéticos: evolução e dificuldades na colheita de elementos de autoria delitiva**. 2021. 25 f. Trabalho de Conclusão de Curso (Bacharel em Direito) – Una Bom Despacho, Bom Despacho. 2021.

BEZERRA, Rayan Vasconcelos. **O direito penal: finalidades e sanções. Revista Âmbito Jurídico**. São Paulo, setembro de 2017.
Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/o-direito-penal-finalidades-e-sancoes/.
Acesso em: 15 dez 2021.

BOITEUX, Luciana. **Crimes informáticos: Reflexões sobre política criminal inseridas no contexto internacional atual**. Revista Brasileira de Ciências Criminais – Instituto Brasileiro de Ciências Criminais – número 47 – Editora Revista dos Tribunais de 2004.

BOTTINI, P. C. **Alerta sobre lavagem de dinheiro e crimes digitais na pandemia**. Consultor Jurídico, 18 mai 2020.
Disponível em: https://www.conjur.com.br/2020-mai-18/direitodefesa-alerta-lavagem-dinheiro-crimes-digitais-pandemia#sdfootnote1sym.
Acesso em: 16 jun 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Palácio do Planalto.
Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
Acesso em: 13 set 2021.

BRASIL. **Lei nº 12.737/2012**, Brasília. Palácio do Planalto.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.
Acesso em: 24 abr 2022.

BRASIL. **Lei nº 13.709/2018**. Brasília. Palácio do Planalto.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
Acesso em: 24 abr 2022.

BRASIL. **Lei nº 12.735/2012**, Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Diário Oficial da União, 30 nov. 2012.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm.
Acesso em: 16 jun 2021.

BRITO, A. **Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"**. 2013.
Disponível em: http://politicacidadaniaedignidade.blogspot.com.br/2013/04/analise-da – lei-1273712-lei-carolina.html.
Acesso em: 19 nov 2018.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. São Paulo: Brasport, 2014.

CÂMARA DOS DEPUTADOS. Deputada Mariana Carvalho; Deputado Esperidião Amin; Deputado Sandro Alex; Deputado Rafael Motta; Deputado Daniel Coelho; e Deputado Rodrigo Martins. Câmara dos Deputados CPI – **Crimes Cibernéticos – Relatório Final**. Brasília; 04 de maio de 2016.

CHC ADVOCACIA. **Marco Civil da Internet: o que é e o que muda para o seu negócio**. 2019.
Disponível em: https://chcadvocacia.adv.br/blog/marco-civil-da-internet/.
Acesso em: 01 jul 2021.

COLLI, Maciel. **Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernético**s. Porto Alegre, 2009.

Como surgiu a Lei geral de Proteção de Dados. Acervo.
Disponível em: https://acervonet.com.br/blog/como-surgiu-a-lei-geral-de-protecao-de-dados-lgpd/.
Acesso em: 24 de abr 2022

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade**. Revista Científica Eletrônica do Curso de Direito. 13ª ed. Garça-SP, 2018.

DALL'AGNOL'. Laísa. **Os dez países que mais produzem ataques hackers no mundo**. Veja. 2021. Disponível em: https://veja.abril.com.br/coluna/radar/os-dez-paises-com-mais-ataques-hackers-no-mundo/.
Acesso em: 24 de abr 2022

DIANA, Daniela. **História da Internet**. 2011.
Disponível em: https://www.todamateria.com.br/historia-da-internet.
Acesso em: 26 set 2021.

E-COMMERCE BRASIL. **E-commerce brasileiro cresceu 40% após um ano de pandemia**, revela Conversion. 2021.
Disponível em: https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-cresceu-coronavirus/.
Acesso em: 26 out 2021.

EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da lei "Carolina Dieckmann"**. Três Passos-RS, 2019.

Disponível em: Arthur Egewarth.pdf (unijui.edu.br).
Acesso em: 21 nov 2021.

FREDERIGHI, Daniel. **Crimes virtuais: como se proteger e denunciar?**.2021.
Disponível em: https://jus.com.br/artigos/93032/crimes-virtuais-como-se-proteger-e-denunciar.
Acesso em: 21 nov 2021.

FILHO, E. G.; SILVA, G. V. da. **Reflexões sobre os cibercrimes e sua competência**. Centro Universitário Antônio Eufrásio de Toledo. v. 13, n. 13. Presidente Prudente, 2017.
Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/6354/6053.
Acesso em: 14 nov 2021.

FRANCESCO, W. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann"**. 2014.
Disponível em: https://wagnerfrancesco.jusbrasil.com.br/artigos/152372896/o-que-voce-precisa-saber-sobre-a-lei-12737-2012-conhecida-como-lei-carolina-dieckmann.
Acesso em: 19 nov 2021.

GOVERNO FEDERAL. **Proteção de Dados – LGPD**. 2020.
Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd.
Acesso em: 01 set 2021.

Lei de crimes virtuais já está em vigor. JusBrasil. 2012.
Disponível em: https://tj-mt.jusbrasil.com.br/noticias/100439956/lei-de-crimes-virtuais-ja-esta-em-vigor.
Acesso em: 24 de abr 2022

Lei que torna crimes cometidos pela internet mais graves é sancionada. Migalhas. 2021.
Disponível em: https://www.migalhas.com.br/quentes/346274/lei-que-torna-crimes-cometidos-pela-internet-mais-graves-e-sancionada.
Acesso em: 24 de abr 2022

LENZA, Pedro. **Direito Constitucional Esquematizado**. 23ª ed. São Paulo: Saraiva, 2019.

MISSE, Michel. **Crime, sujeito e sujeição criminal: aspectos de uma contribuição analítica sobre a categoria "bandido"**. Lua Nova: Revista de Cultura e Política - no.79 - São Paulo, 2010.
Disponível em: https://doi.org/10.1590/S0102-64452010000100003.
Acesso em: 15 set 2021.

PROCOPIO, Michael. **Lei 14.155/2021: a fraude eletrônica e outras alterações no Código Penal. Estrategia Concursos.**
Disponível em: https://www.estrategiaconcursos.com.br/blog/lei-14-155-2021-a-fraude-eletronica-e-outras-alteracoes-no-codigo-penal/#:~:text=A%20lei%2014.155%2C%20de%2027,mediante%20fraude%20e%20ao%20estelionato.
Acesso em: 15 set 2021.

MONCAU, Luiz Fernando; LEMOS, Ronaldo; BOTTINO, Thiago Amaral. **Projeto de Lei de Cibercrimes: há outra alternativa para a internet brasileira?** Revista de Direito Administrativo, 2008.

Disponível em: 4102-9270-1-PB.pdf (fgv.br).
Acesso em: 18 nov 2020.

MONTEIRO, Luis. **A internet como meio de comunicação: possibilidades e limitações**. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação- XXIV Congresso Brasileiro da Comunicação, 2021.

MOTTA, Artur Francisco Mori Rodrigues. **A dignidade da pessoa humana e sua definição**.
Disponível em: https://ambitojuridico.com.br/cadernos/direitos-humanos/a-dignidade-da-pessoa-humana-e-sua-definicao/.
Acesso em: 26 set 2021.

NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais**. 2019.
Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/.
Acesso em: 16 mai 2021.

O que é a LGPD?. Ministério Público Federal.
Disponível em: http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd.
Acesso em: 24 de abr 2022.

OLIVEIRA JÚNIOR, E. Q. de. **A nova Lei Carolina Dieckmann**. 2013.
Disponível em: http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina--dieckmann.
Acesso em: 19 mai 2022.

PAULO, Ton. **Em alta, crimes cibernéticos devem ser denunciados**. 2019.
Disponível em: https://www.jornalopcao.com.br/reportagens/em-alta-crimes-ciberneticos-devem-ser-denunciados-228474/.
Acesso em: 20 set 2021.

PINHEIRO, Patricia Peck. **Direito Digital**. São Paulo: Saraiva 2013.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**, Teresina, ano 7, n. 58, 1 agosto 2002. Membro do IBCCRIM.

ROCHA, Adriano Aparecido. **Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet**.
Disponível em: https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf.
Acesso em: 01 dez 2021.

RIBITTE. Leonardo. **Brasil é um dos países com mais fraudes por ataques virtuais no mundo. Combate a Fraude**. 2022.
Disponível em: https://www.combateafraude.com/post/brasil-fraudes-ataques-virtuais#:~:text=Ao%20lado%20dos%20Estados%20Unidos,ataques%20cibern%C3%A9ticos%20ano%20a%20ano. Acesso em: 24 abr 2022.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e os direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2004.

SATAKE, Marcelo. **Conheça as fraudes digitais mais comuns na pandemia e veja como evitar**. 2020.
Disponível em: https://invest.exame.com/mf/conheca-as-fraudes-digitais-mais-comuns-na-pandemia-e-veja-como-evitar.
Acesso em: 26 jul 2021.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Jus Brasil, Artigos, 2014.
Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos.
Acesso em: 15 nov 2021.

SENADO FEDERAL. **Projeto de Lei do Senado nº 236**, de 2012.
Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/106404.
Acesso em: 20 ago 2021.

SENADO FEDERAL. **Projeto de Lei do Senado nº 427**, de 2011.
Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/101252.
Acesso em: 20 ago 2021.

SENNA, Felipe; FERRARI, Daniella. **Convenção de Budapeste e crime cibernéticos no Brasil**. 2020.
Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil.
Acesso em: 18 nov 2021.

SILVA, Ana Laura Rossi. **Cibercrimes: uma análise sob a perspectiva da aplicação do direito internacional**. Minhas Gerais, 2019.
Disponível em: CibercrimesAnalisePerspectiva.pdf (ufu.br).
Acesso em: 12 nov 2021.

SILVA, José Afonso da. **A dignidade da pessoa humana como valor supremo da democracia**. Revista de Direito Administrativo, v. 212, p. 84-94, abr./jun. 1998.
Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47169/45637.
Acesso em: 12 out 2021.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. Editora Revista dos Tribunais, 2003. ISBN 8520324126, 9788520324127. Num. págs. 141 páginas.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).
Disponível em: http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468.
Acesso em: 19 ago 2021.

SOUZA, Juliane Silva de. **Crimes Virtuais**. Porto Velho – RO 2018.
Disponível em: http://repositorio.saolucas.edu.br:8080/xmlui/bitstream/handle/123456789/2836/Juliane%20Silva%20de%20Souza.%20-%20Crimes%20virtuais.pdf?sequence=1&isAllowed=y. Acesso em: 19 nov 2021.

SORRENTINO. Eduardo. **Brasil entra para a lista dos dez países com mais ataques cibernéticos do mundo**. Olhar Digital. 2021.

Disponível em: https://olhardigital.com.br/2021/10/25/videos/brasil-entra-para-a-lista-dos-dez-paises-com-mais-ataques-ciberneticos-do-mundo/.
Acesso em: 24 de abr 2022.

VALENTE, Ivan. **Morosidade do Legislativo e seletiva e responde a interesses econômicos**. Disponível em: https://noticias.uol.com.br/opiniao/coluna/2014/07/25/morosidade-do-legislativo-e-seletiva-e-responde-a-interesses-economicos.htm.
Acesso em: 20 jul 2021.

VIEIRA, Priscila Santana; BRITO, Igor Toneti de; TOLARDO, Isabella Fernanda Semprebon. Direito digital: **da regularização de um novo ambiente ao limite da liberdade de expressão**. Revista Jurídica da UniFil, [S.l.], v. 16, n. 16, p. 174-183, out. 2019. ISSN 2674-7251. Disponível em: http://periodicos.unifil.br/index.php/rev-juridica/article/view/1152.
Acesso em: 22 nov 2021.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. Disponível em: https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekl.
Acesso em: 21 jun 2021.