Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

**JOÃO MARCIO BATISTELA**

# ASCENSÃO DOS CRIMES VIRTUAIS, SUAS LEGISLAÇÕES E OS PRINCIPAIS MÉTODOS DE PREVENÇÃO.

**Assis/SP**

2022

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

**JOÃO MARCIO BATISTELA**

# ASCENSÃO DOS CRIMES VIRTUAIS, SUAS LEGISLAÇÕES E OS PRINCIPAIS MÉTODOS DE PREVENÇÃO.

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

**Orientando (a): João Marcio Batistela**
**Orientador (a): João Henrique dos Santos**

**Assis/SP**
**2022**

FICHA CATALOGRÁFICA

BATISTELA, João

**Ascenção dos crimes virtuais e os principais métodos de prevenção**/João Marcio Batistela. Fundação Educacional do Município de Assis –FEMA – Assis, 2022.

25 páginas

1. Palavra-chave. 2. Palavra-chave.

CDD:

Biblioteca da FEMA

**ASCENSÃO DOS CRIMES VIRTUAIS, SUAS LEGISLAÇÕES E OS PRINCIPAIS MÉTODOS DE PREVENÇÃO.**

JOÃO MARCIO BATISTELA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

**Orientador:**

João Henrique dos Santos

**Examinador:**

Elizete Mello da Silva

Assis/SP

2022

## DEDICATÓRIA

Dedico este trabalho aos meus pais, Rosane e Luiz e também minha namorada Sabrina que nunca deixou de me apoiar nesse momento acadêmico.

## RESUMO

Este trabalho tem como finalidade analisar os crimes realizados em ambientes virtuais em nossa sociedade atual. Buscando compreender como o criminoso furta os dados pessoais de suas vítimas, e os utiliza para benefício próprio, como exemplo senhas de bancos, cartões virtuais, dados empresariais, entre diversos outros.



**Palavras-chave: Crimes virtuais, furto de dados, dados empresariais, métodos de prevenção.**

**ABSTRACT**

This work aims to analyze the crimes committed in virtual environments in our current society. Seeking to understand how the criminal steals the personal data of his victims, and uses them for his own benefit, such as bank passwords, virtual cards, business data, among many others.

**Key-words: Cyber crimes, data theft, corporate data.**

## Sumário

## INTRODUÇÃO

O trabalho a seguir tem como proposta a analise da legislação vigente que abortam os crimes que ocorrem no ambiente digital, já que não há um código específico.

A pesquisa do seguinte trabalho utiliza meios de compilações bibliográficas, como as normas de nosso sistema jurídico e jurisprudências, sendo dividido em quatro capítulos.

O capítulo de número um, trata sobre crimes em geral, como sua identificação, sua evolução através do tempo e as nomenclaturas utilizadas para as condutas.

No segundo capítulo presente fala sobre as espécies mais recorrentes dos delitos cometidos no meio digital, dando mais ênfase para os tipos dos delitos e demonstrando como ocorrem na realidade.

O capítulo de número três ressaltará as leis que já abordam o tema, como A Lei de número 12.737/2012, “lei Caroline Dieckmann”, que inseriu os artigos 154 – A e B em nosso Código Penal. E também a Lei 12.965/14, o Marco Civil da Internet também conhecida como a constituição da internet.

## CAPÍTULO I – Os Crimes virtuais

Os Cybers crimes são um dos maiores desafios deste século imposto aos Estados no que se refere à persecução penal. A globalização vem transformando o modo como vemos nosso mundo hoje. Esse fenômeno é difícil de ser conceituado.

Boaventura de Souza Santos (1997) apresenta estudiosos que creem que a globalização é um fenômeno cujo foco está na economia, à medida que as corporações multinacionais alcançam uma posição inédita no mundo.

Para ele, no entanto é importante encontrar uma definição para a globalização mais sensível às culturas, politicas e sociedades. (SANTOS 1997, p. 108)

Junto com o desenvolvimento da globalização, as relações começaram a evoluir através de dispositivos eletrônicos, causando a colisão de culturas extremamente diferentes que se conectam a rede, contudo novas profissões começaram a surgir com esse evento e com isso o direito notou-se necessário se moldar nessa realidade, trazendo assim o ambiente digital para a área do controle do Estado.

Um dos principais movimentadores jurídicos é a tecnologia, o avanço e a existência da tecnologia são cruciais no cotidiano das pessoas, por isso é necessário regulá-la a visando facilitar a evolução das relações e os ambientes virtuais.

As características fundamentais que definem a rede é a abertura dela, isso possibilita relacionamentos não hierárquicos e horizontais entre pessoas, contudo a rede não é uma estrutura em si, já que pode fazer-se e desafazer-se de uma maneira rápida.

“É responsabilidade do Estado de direito garantir a convivência igualitária dos cidadãos e manter a ordem juntamente com o desenvolvimento dela. Deste modo, acabará por intervir na sociedade virtual que se forma, com regulamentações que limitam a Internet e as informações por meios tecnológicos” (SYDOW, 2014).

“Na mesma linha de raciocínio, as legislações do mundo todo começaram a analisar a criação de novas normas para inserir nessa nova realidade. Nesse “movimento”, o Brasil, promulgou legislações para regulamentar esse novo espaço virtual de maneira lenta, visando proteger os direitos essenciais, como a liberdade de se expressar e combater os crimes virtuais que ocorrem neste ambiente” (PINHEIRO, 2014)

Em Abril de 2014, foi sancionada a Lei de n°12.965, conhecida como Marco Civil da Internet, que define direitos, garantias e deveres, entre empresa e consumidor. Em 2016, foi apresentado o relatório final da CPI que tinha como objetivo a investigar a pratica dos crimes cibernéticos e também seus efeitos na sociedade e na economia do país.

O crime virtual deve ser analisado por várias perspectivas diferentes por conta de suas peculiaridades, como o autor do crime virtual pode estar em diversos lugares simultaneamente, de maneira discreta e silenciosa, a sociedade acaba por omitir os ataques e não realizando a denuncia deles. (SYDOW, 2009).

Como o autor do crime digital pode estar em vários lugares ao mesmo tempo, sendo discreto e silencioso o mesmo também pode cometer diversos crimes com uma só ação. Por conta disso, a sociedade acaba omitindo os ataques sofridos e não realizando a denuncia do fato.

Os crimes virtuais impróprios mais recorrentes no meio digital são velhos conhecidos do sistema penal brasileiro, como os crimes de ameaça, falsidade ideológica, fraudes entre diversos outros delitos. A possibilidade de se manter anônimo na internet acaba por incentivar a violação das regras impostas. (PINHEIRO, 2014)

O CERT. BR, conhecido com Centro de Estudos, Respostas e Tratamento de Segurança no Brasil, realiza analises e estatísticas sobre os incidentes reportados em todo o país, e segundo eles foram mais de 665 mil casos reportados no ano de 2020 (CERT. BR, 2020)

Uma das principais características da criminalidade que utiliza métodos informáticos é a conexão global, já que todos os países fazem uso da tecnologia, possibilitando o invasor cometer crimes em qualquer lugar do mundo. (FIORILLO; CONTE 2016).

A maior característica da internet é a variedade de serviços para aqueles que desejam adquirir vantagem de forma ilegal através das atividades praticadas por invasores, alguns exemplos disso é a aquisição de certificados de conclusão de curso falsos, criação de documentos falsos, falsificação de dinheiro e também a pirataria.

## 1.1 - IDENTIFICAÇÃO DOS CRIMES VIRTUAIS

No momento em que os criminosos passam a se focar na internet, a criminologia começou teorizar para definir esses crimes que ocorrem neste ambiente tecnológico,e compreender por que ocorrem (JAISHANKAR, 2007)

A infração penal no Brasil pode ser divida em crimes e contravenções, onde o legislador nomeia as ações mais lesivas como crime e as com menor potencial ofensivo como contravenções penais. (CUNHA, 2014)

Neste trabalho, não é apropriado distinguir entre crimes e contravenções penais, é importante estabelecer que ao utilizar a expressão “crime virtual”, compreende-se que esta dizendo o mesmo que infração penal.

Guilherme Souza Nucci conceitua que os crimes da seguinte forma, por mais que os cyber crimes pareça com os delitos “reais”, devido suas características,

esses crimes também são identificados por se utilizar aparelhos informáticos para serem cometidos.

Damásio de Jesus e José Antônio Milagres (2016) concordam que os crimes virtuais são fatos típicos cometidos por meio de um dispositivo tecnológico, que pode atacar sistemas ou redes de dispositivos.

O modo de agir do cracker que é contratado para invadir um sistema e roubar seus dados, utilizando seu conhecimento em explorar as falhas do sistema de segurança. Neste caso os sujeitos seriam o próprio invasor, a vítima e a pessoa que contratou o cracker. Porém, supondo que o criminoso vá até um cyber café, onde há vários computadores juntos para invadir os sistemas de seus alvos, enviando mensagens para funcionários, que encaminham aos seus superiores, assim se repetindo até que algum deles instale um software oculto que possibilita a invasão do sistema. No suposto caso, haverá diversas vítimas e autores (SYDOW, 2014)

## 1.2 EVOLUÇÃO HISTÓRICA

A convenção sobre o Cibercrime de Budapeste foi realizada em 2001 na Hungria, onde se definiu que os delitos que ocorrem por meio de computadores, contra ele ou através deles, sendo grande parte dessas praticam ser por meio da conexão à internet, serão considerados como crimes virtuais.

Na década de 1960 surgiram os primeiros delitos informáticos onde o autor espionava ou manipulava sistemas e computadores, mas somente na década de 1980 houve o aumento dessas ações criminosas e com isso passaram a cometer outros crimes, como piratarias de programas e abuso de telecomunicação além da pornografia infantil.

Junto com a aparição dos cybers crimes, surgem duas figuras, o hacker e o cracker. Embora a expressão hacker seja associada a infrações, os cracker são os verdadeiros criminosos, o que difere entre eles é o modo como utilizam seu conhecimento. Os hackers em geral são programadores que possuem um grande conhecimento sobre sistemas e não tem o propósito de causar danos ao computador.

Em contrapartida, os crackers utilizam seu conhecimento para quebrar sistemas de segurança, subtrair senhas de acessos a redes e até quebrar códigos criptografados de uma maneira ilegal. Muitos desses cracker são contratados para sabotar sistemas atrás de informações.

A sociedade humana desenvolveu há muito tempo, um modelo de regras para a convivência em harmonia social, quando as normas são objetivas e claras a aceitação pela sociedade se torna mais fácil. (PINHEIRO, 2014).

Desde que a internet foi criada, notou-se uma grande necessidade de regulamentar o ambiente digital que a principio, não possuía nenhum controle ou imposição de regras (PINHEIRO. 2014)

A partir disso, o desenvolvimento estabeleceu um padrão para a comunicação e a interação social, por meio de telefones, tablets e diversos outros dispositivos conectados na internet, facilitando a comunicação e mudando a percepção da sociedade civil sobre determinados aspectos políticos, sociais e questões econômicas, que anteriormente não atraiam interesse dos criminosos (ALVES, 2014).

O comportamento digital difere do comportamento "real", no qual o debatedor confia em sua perspicácia para vencer seu oponente e fazer com que os outros se apeguem às suas ideias sem depender de um mediador. Em um ambiente de liberdade, pressão e proteção constitucional imediata da República, "adotando 10 posições por meio de técnicas de debate, atingindo um grande público, muitas vezes

intensifica as discussões, tornando os debates uma realidade" (COELHO;BRANCO,)

A tecnologia esta cada vez mais presente no cotidiano da sociedade, tornando-se indispensável para que os indivíduos possam ter conhecimento para lidar com a própria tecnologia, que se tornou imprescindível para que os cidadãos possam estudar maneiras de melhorar as ferramentas usadas para desenvolver redes e sistemas. (SYDOW, 2014)

Crime conhecido como "ódio" - uma forma expressiva de discurso de ódio, expresso contra determinados grupos de pessoas com características únicas que os identificam, tem crescido excessivamente nos ambientes virtuais. Portanto, o Brasil mede os princípios da dignidade humana e da liberdade de expressão para manter o acesso à Internet como um espaço participativo, interativo e decisivo no atual contexto social. (PANNAIN; PEZZELLA, 2015)

## CAPÍTULO II – CRIMES VIRTUAIS E SUAS ESPÉCIES

Neste capítulo, mais ênfase será colocada nos crimes virtuais em si, tratando dos crimes próprios e também os impróprios, distinguindo-os e também os analisando.

Com o anonimato preservado no ambiente virtual, muitas pessoas pensam que estarão seguros, podendo assim incentivar a não conformidade com as regras da sociedade, as praticas envolvem desde a disseminação de vírus através de links enviados até invasões de sistemas de empresas multinacionais.

Destes, destacam-se os crimes mais comuns: crimes de ódio Geral (contra a honra, sentimento religioso, bullying), invasão Privacidade e intimidade (que podem

ou não convidar a novos comportamentos prejudiciais),corrupção, pedofilia, etc.

Com a internet, a criação de um mundo utópico e sem distâncias se tornou algo palpável, já que as pessoas podem se conectar por mais distantes que estejam. Pelas efetivas participações e a inclusão das pessoas no “cyber espaço”, é preciso que os Estados promovam sua própria proteção de direitos e garantias para que a tecnologia não possa violá-los. (PANNAIN; PEZZELLA, 2015).

Os crimes cibernéticos no geral podem afetar qualquer pessoa ou até mesmo empresa. Junto com a facilidade de pesquisa e também a realização de negócios de forma virtual, o advento da internet trouxe aos seus usuários essa preocupação. Diante disso, é necessário cuidado quando clicar em arquivos suspeitos anexados ao e-mail ou mesmo em pop-ups de sites desconhecidos ou não confiáveis.

A motivação desses crimes no mundo virtual na maioria dos casos é a busca por notoriedade e também a vingança pessoal, na qual leva os criminosos a invadirem os dispositivos de suas vítimas e consequentemente adquirir dados de suas vítimas. Contudo, também há causas oriundas do fanatismo, especialmente por meio das vertentes religiosas e políticas.

Porém, a principal causa, na maioria dos crimes é a alta condição financeira das vítimas, já que após o invasor obter os dados e as informações através da invasão de um sistema, o mesmo exige um “resgate” desses dados para devolvê-los à vítima.

## 2.1 – Tipos de Crimes Virtuais

Os crimes virtuais se dividem em diversas modalidades, como exemplo,

ATAQUES DDOS, em que o invasor ataca várias máquinas através de um único computador. Dessa forma o cracker “derruba” servidores, redes privadas. No

DDoS, um computadores pode controlar diversos outros milhões de computadores e assim coordenar um ataquem em massa a uma rede em específico.

O PHISHIN, na qual o invasor tenta “fisgar” suas vítimas utilizando links, aplicativos, ou até mesmo sites construídos especificamente para roubar os dados dos internautas, como senhas pessoais, números e cartões. O termo foi criado no início da internet, em 1990, quando os hackers atraiam usuários para roubar suas contas hospedadas no América Online (AOL).

O BULLYING VIRTUAL, como o próprio nome já diz, o cyber bullying, é uma extensão do bullying que ocorre em muitas escolas, faculdades e até mesmo locais de trabalho, a única diferença é que não há contato entre a vítima e o agressor.

O ESTELIONATO pode ocorrer nos dois ambientes, tanto o “real”, quanto o virtual, porem com o avanço da internet, sua reincidência tomou proporções antes nunca vista.

Vale ressaltar que diversos crimes não necessariamente ocorrem apenas em um ambiente digital, porém com o acesso fácil a internet, esses crimes se tornaram mais frequentes. Como exemplo o estelionato que não necessariamente precisa do ambiente virtual, mas se tornou muito recorrente.

## CAPÍTULO III – LEGISLAÇÃO CORRESPONDENTE

A Lei de número 12.737/2012 – Lei dos Crimes Cibernéticos, ou também conhecido como Lei “Caroline Dieckmann” nos trouxe as alterações necessárias para o Decreto-Lei 2.848/40 do nosso Código Penal, que formalizou e também tipificou as condutas delituosas no ambiente informático, passando a ser chamados de “crimes cibernéticos”.

O *caput* do artigo 154-A do Código Penal pode ser considerado o maior avanço proporcionado. Já que seu objetivo principal é realizar o combate às principais práticas antijurídicas, conhecidas por causar transtornos para quem utiliza essa tecnologia.

Os novos artigos adicionados ao Código Penal através da Lei 12.737/2012 que busca combater as invasões de dispositivos alheios, conectados à rede de computadores e também os dispositivos *off-line,* vale lembrar que se compreende por dispositivos informáticos: laptops, notebooks *tabletes*, celulares e computadores de mesa (Desktop), entre outros.

O tipo penal indica a necessidade de o dispositivo informático possuir algum sistema de segurança, sob a pena de ser considerado desprotegido penalmente (NUCCI, 2013, p.742).

Assim, para que o invasor cometa a conduta tipificada no artigo supracitado, o sujeito ativo deverá invadir o dispositivo, sem necessariamente estar conectado à internet, e com finalidade de destruir, alterar ou obter informações e dados.

Na previsão dada pelo **§ 1º do artigo 154.**

> "Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput." (Incluído pela Lei nº 12.737, de 2012).

Já os parágrafos 2° ao 5°, preveem qualificações para essa conduta, as quais serão configuradas se a invasão tiver como resultado a obtenção de segredos comerciais e industriais, obtenção de conteúdo privado de comunicações e controle remoto não autorizado, nestas hipóteses, a pena será reclusão de seis meses a dois anos e multa. Caso haja a divulgação, negociação ou distribuição dos dados obtidos a terceiros, a pena será aumentada de um a dois terços.

Além da citada anteriormente, no Brasil, há também a Lei 12.965/14, conhecida como Marco Civil da Internet que tem como finalidade de regulamentar o uso da internet e estabelecer normas no serviço que é oferecido no Brasil.

Além disso, incluiu o §2º-A e B, no artigo 171 do Código Penal com a Lei N° 14.155/2021 que prevê uma pena bem mais severa para fraudes eletrônicas cometidas por meio de redes sociais, contatos telefônicos e envio de correio, conhecidos como estelionato eletrônico.
Ela também inclui o §4º-B e C no artigo 155 do Código Penal, que prevê o furto mediante fraude cometida através de dispositivos eletrônicos, com uma pena maior que a forma qualificada tradicional.

## 3.1 – Convenção de Budapeste

A criação da convenção de Budapeste em 2001 na Hungria pelo Conselho Europeu prioriza uma politica criminal comum, visando proteger a sociedade da criminalidade no ambiente virtual através da adoção de legislações adequadas, melhorar a cooperação internacional e reconhece essa necessidade do Estado cooperar com a indústria privada.

O tratado de 2001 possui quatro capítulos que são Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais. Juntamente com 48 artigos encorpados em um texto de fácil compreensão, já que não traz informações técnicas.

A convenção busca facilitar o combate ao crime na internet, e listar os principais delitos realizados através da conexão de dispositivos conectados a internet, este, foi o primeiro tratado internacional que aborda a criminalidade na rede.

Este tratado já foi assinado por 66 países e ainda orienta 158 países com suas legislações.

O principal destaque da Convenção é que ela define os cybers crimes, tipificando-os como infrações contra dados e sistemas informáticos, matérias do direito processual, competência e cooperação internacional. Ou seja, cria normas de investigação e apresenta métodos para cooperação entre países.

Em 2019, o Brasil foi convidado a se juntar à convenção. Com o Marco Civil da Internet, uma grande estrutura legislativa já havia sido feita para o combate ao crime virtual, contudo esse tipo de crime se encontra em constante evolução. Por isso se torna importante o aprimoramento na coordenação e na cooperação entre os países.

## 3.2 – Marco civil da internet

A Lei 12.965/14, conhecida como Marco Civil da Internet é uma lei ordinária federal de iniciativa do Poder Executivo.

A Lei anteriormente citada foi criada para nortear as relações entre empresas e clientes, estabelecendo princípios no ambiente virtual, dentre eles:

### 3.2.1 - O princípio da privacidade

Garante a inviolabilidade das comunicações dos seus usuários. A quebra dessa garantia deve ocorrer somente através de ordem judicial, quando forem indispensáveis para a confirmação de ações ilícitas, e na identificação dos autores.

Empresas estrangeiras que pretender adentrar ao país devem se adaptar ao ordenamento jurídico brasileiro, que não envolve o Marco Civil, mas também todas as outras legislações que abordam o tema.

Os provedores de internet são empresas que fornecem diversas funcionalidades que podem ser acessadas através de um terminar conectado à internet, para que o usuário possa utilizar dos serviços online, como sites, blogs, e-mails, plataformas de streaming entre outros vários serviços.

De forma geral, o provedor é o instrumento necessário para a conexão com a rede mundial de computadores.

### 3.2.2 - Princípio da neutralidade da rede

Tal princípio tem como finalidade de inibir as ações abusivas praticadas pelas empresas que prestam o serviço de telefonia e internet, como exemplo limitar os clientes ao acessar serviços ou sites.

Um dos objetivos da lei é justamente proporcionar um tratamento isonômico entre os consumidores. Embora não tenha sido aderida com grande entusiasmo pelas empresas, a neutralidade da rede permitiu que a competitividade fosse estimulada, já que a regulamentação garante as mesmas condições na oferta de seus produtos. Fazendo com que os provedores de menor tamanho não sofram com a discrepância do poder econômico.

Ainda sobre a neutralidade da rede, vale destacar a possibilidade de exceções, tendo em vista determinados tipos de atividades que possuem as prerrogativas de discriminar o tráfego da internet. Segundo a legislação, as empresas podem descartar a neutralidade da rede para a manutenção da estabilidade da rede, priorizar o tráfego de serviços emergenciais, segurança, integridade e priorizar o tráfego em situação de risco.

### 3.2.3 - Princípio da fiscalização dos acessos

Esse princípio trata da regulamentação dos processos de armazenamento dos dados de conexão, sendo de responsabilidade da empresa que fornece o serviço que possui o prazo mínimo de um ano de obrigação. Em casos em que alguns dados cadastrais se façam necessário, as autoridades podem exigi-los ao provedor, esses dados podem ser nome completo, estado civil, filiação, endereço e profissão.

Devido ao seu objetivo, essa lei foi conhecida como a “Constituição da Internet”. Por mais demorada que fora sua construção início em 2009, foi necessário cinco anos até sua publicação em 2014

O Marco Civil da internet foi criado a partir dos três princípios já citados anteriormente

## CAPÌTULO IV – CONSIDERAÇÕES FINAIS.

Por mais que os crimes que ocorrem no ambiente virtual se pareçam com os crimes cometidos sem o uso das tecnologias devido suas características, os cybers crimes também são identificados através do uso de um dispositivo tecnológicos para serem cometidos.

O tema abordado possui uma grande relevância, tanto no dia-a-dia quanto na legislação brasileira, com a presença da globalização e a tecnologia cada vez mais forte nos ambientes profissionais e pessoais.

As leis já existentes amparam e tratam sobre os crimes virtuais, mas há uma grande fragilidade na legislação visando a grande demanda dos processos que necessitam de um posicionamento eficaz nas tipificações.

Com a adesão do Brasil na convenção de Budapeste é de grande importância para o avanço no combate e na prevenção dos crimes virtuais, isso possibilita discussões sobre o assunto e aperfeiçoar nossas leis uniformizando os procedimentos tomados. Facilitando o combato contra os mesmos.

É clara a evolução brasileira nesse cenário tecnológico, porém ainda há muito que evoluir, tanto na informação por parte das vítimas, quanto na legislação que trata o tema.

A Lei 12.965/14, conhecida como Marco Civil da Internet é uma lei ordinária federal de iniciativa do Poder Executivo. Que estabelece princípios para a relação de consumo entre empresa e consumidor final buscando equilibrar essa relação.

Contudo, para efetivar o combate deve se manter o foco na informação, já que grande parte dos crimes cometidos pode ser evitada pela própria vítima ao evitar realizar compras online em sites desconhecidos, acessar links em e-mails marcados como spam, não salvar senhas de bancos no celular, ativar o autenticador em dois fatores e utilizar um bom serviço de segurança. Sendo essas as ações são as mais comuns no dia-a-dia dos brasileiros.

## REFERÊNCIAS BIBLIOGRÁFICAS

Lei nº 12.965, de 23 de abril de 2014. Estabelece Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a Tipificação Criminal de Delitos Informáticos; Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências

Senado Federal. “O Senado e os Crimes cibernéticos”. Rev. Em Pauta. Ano V - nº 235 - Brasília, 10 de setembro de 2012.

CERT.COM. Incidentes Reportados ao CERT.br Janeiro a Dezembro de 2021

CAPEZ, Fernando Prado. Código Penal Comentado.

JESUS, Damasio de; MILAGRE, José Antonio. Manual de Crimes Informáticos.

NUCCI, Guilherme de Souza. Manual do Direito Penal. 7. ed. São Paulo: Revista dos Tribunais, 2011.

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)

TRENTIN, Taise Rabelo Dutra; TRENTIN, Sandro Seixas. Internet: Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais. Revista Direitos Emergentes da Sociedade Global, Santa Maria, n. 1, p. 79-93, jan.jun/2012.

SYDOW, Spencer Toth. Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009.

PINHEIRO, Patrícia Peck. Regulamentação da Web. Cadernos Adenauer XV, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: < http://www.kas.de/wf/doc/16471-1442-5-30.pdf>

JAISHANKAR, Karuppannan. Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, v. 1, p. 7-9, 2007

Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm.

Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético

Fonte: Agência Senado disponível em: https://www12.senado.leg.br/noticias/materias