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

**MATHEUS LIMA DOS SANTOS**

# AS LIMITAÇÕES ENCONTRADAS PELA ATUAL LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS.

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

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

**MATHEUS LIMA DOS SANTOS**

# AS LIMITAÇÕES ENCONTRADAS PELA ATUAL LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS.

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):** Matheus Lima dos Santos

**Orientador(a):** Prof. Claudio José Palma Sanchez

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

S232i SANTOS, Matheus Lima

Limitações encontradas pela atual legislação brasileira no combate aos crimes cibernéticos / Matheus Lima dos Santos. – Assis, 2022.

29p.

Trabalho de conclusão do curso (Direito). – Fundação Educacional do Município de Assis - FEMA

Orientador: Prof. Claudio José Palma Sanchez

1. Direito Digital. Direito Civil. Marco Civil da Internet, Crimes Cibernéticos.

CDD 340

# AS LIMITAÇÕES ENCONTRADAS PELA ATUAL LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS.

MATHEUS LIMA DOS SANTOS

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:** _____

Prof. Claudio Jose Palma Sanchez

**Examinador:** _____

Inserir aqui o nome do examinador

Assis/SP
2022

# DEDICATÓRIA

Aos meus heróis que, carinhosamente, chamo de pais, por me acompanharem em cada uma das minhas conquistas, grandes ou pequenas. Aqui estamos em mais uma delas.

# AGRADECIMENTOS

Primeiramente, Agradeço a Deus por ter me dado a graça de estar com saúde e disposição para que eu pudesse galgar mais um degrau em minha vida pessoal e profissional através de um curso superior.

Ao meu orientador Claudio José Palma Sanchez pelo incentivo e norteamento na elaboração deste projeto de pesquisa

Aos meus pais por terem me orientado na vida de maneira a sempre buscar as coisas boas e fazer o bem aos meus semelhantes.

Aos meus amigos e colegas de sala e ao meu grupo de estudos da faculdade que sempre serviu de estímulo para estudar.

A justiça não consiste em ser neutro entre o certo e o errado, mas em descobrir o certo e sustentá-lo, onde quer que ele se encontre, contra o errado.

*Theodore Roosevelt*

# RESUMO

Conforme a civilização avança nós criamos diferentes meios de nos comunicar, armazenar nossos dados, informações, lembranças e afins. Com a chegada da Internet, nossos dados ficam, a cada dia, mais e mais expostos, sujeitos a invasões e extorsões. Neste mesmo sentido também avança as práticas delituosas que visam tomar vantagens quanta a essas informações. Os crimes cibernéticos surgem da falha destes mecanismos de informação e segurança, permitindo com que infratores abusem destes mecanismos defeituosos. Assim sendo, nossa legislação avanço exponencialmente, vindo a proporcionar métodos para julgar e condenar tais crimes, através de leis nº. 12.695/2014, Lei n. º 12.737/2012, e a mais recente lei n. º 13.709/2018. Nosso ordenamento jurídico, agora preparado, delimita a atuação do poder Estatal, definindo e qualificando os crimes e suas incisões, formas de investigação, propiciando ferramentas para que o poder público possa atuar.



**Palavras-chave:** Direito Digital. Direito Civil. Marco Civil da Internet, Crimes Cibernéticos.

## ABSTRACT

As civilization advances we create different ways to communicate, store our data, information, memories and the like. With the arrival of the Internet, our data becomes more and more exposed every day, subject to invasion and extortion. In the same way, criminal practices that aim to take advantage of this information are also advancing. Cybercrimes arise from the failure of these information and security mechanisms, allowing offenders to abuse these faulty mechanisms. Therefore, our legislation has advanced exponentially, providing methods to judge and convict such crimes, through laws no. 12,695/2014, Law no. 12,737/2012, and the most recent law no. 13,709/2018. Our legal system, now prepared, delimits the actions of the State power, defining and qualifying the crimes and their incisions, forms of investigation, providing tools for the public power to act.



**Keywords:** Digital Law. Civil Law. M Brazil's Internet Bill of Rights, Cybercrimes.

**SUMÁRIO**

# INTRODUÇÃO

O presente trabalho tem propósito de discutir e analisar questões relacionadas à prática de crimes cibernéticos, o impacto social causado por eles e as soluções encontradas pelo governo brasileiro para prevenção e combate aos crimes conexos.

O capítulo 1 deste trabalho apresenta brevemente as definições sobre os crimes cibernéticos e os métodos que os criminosos utilizam para cometer tal delito.

O capítulo 2 classifica estes crimes, explanando suas modalidades: desde casos de crimes comuns cometidos no ambiente virtual por qualquer cidadão, até os crimes de maior complexidade que necessitam de alto conhecimento da ferramenta utilizada pelo criminoso para consumar o delito.

O capítulo 3 analisa o contexto histórico evolutivo das leis dos crimes cibernéticos criadas e atualizadas no Brasil, como a lei n.º 12.695/2014 – marco civil da internet, lei n.º 12.737/2012 – lei carolina dieckmann e, a mais recente, lei n.º 13.709/2018 – lei geral da proteção de dados (lgpd).

O capítulo 4 expõe a criminalidade cibernética no mundo diante da ascensão da internet em escala global e mostra as medidas que alguns países adotaram para combater esta nova modalidade de crime, devido ao aumento de seus registros, como a convenção européia de crimes cibernéticos – convenção de

Budapeste, que foi uma iniciativa levantada a partir da reunião de alguns países com o intuito de combater os crimes virtuais.

O capítulo 5 analisa os principais aspectos do trabalho, apontando a evolução da legislação de combate ao *cibercrime*, principalmente no Brasil, mostrando também a necessidade de regulamentar leis específicas para garantir maior eficácia contra estes crimes.

# 1. A CRIMES CIBERNETICOS

## 1.1. CONCEITO

Os crimes cibernéticos são aqueles praticados no ambiente virtual com o uso da internet, evolvendo um computador, uma rede de computadores ou dispositivos móveis que são invadidos, ainda que sem autorização para a prática do delito, com o objetivo de modificar, subtrair ou danificar dados.

> Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes. (PINHEIRO, 2010, p. 46)

Nesta nova modalidade de crime, considerada como crime de meio, o criminoso tem o objetivo de causar algum tipo de prejuízo financeiro, de imagem ou alterar dados da vítima, que pode ser pessoa física ou jurídica, objetivando ter qualquer tipo de vantagem ilícita sobre elas.

> As denominações que fazem referência aos crimes praticados no mundo virtual são inúmeras, não há uma concordância referente a melhor denominação para se usar para com os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, fraude informática, assim os conceitos ainda não englobam todos os crimes ligados à tecnologia". (CRESPO, 2011, p. 48).

Dentro dos crimes cibernéticos, os criminosos utilizam métodos e técnicas informáticas por meio de softwares ou hardwares para a consumação do crime, que consiste na criação de vírus, *trojan, sniffing,* dentre outros.

## 1.2. O VÍRUS

Consiste em programa de computador classificado como *malware* (produzido com a intenção de causar danos a um computador, rede de computadores, servidor ou cliente), podendo alterar dados do sistema, arquivos e programas, destruir dados e até executar funções de um computador.

### 1.3. TROJAN

Popularmente conhecido como “cavalo de tróia", também é classificado como malware, aparentando ser seguro, mas na realidade é malicioso. O usuário ao instalar ou executar este arquivo infecta seu computador, alastrando este arquivo malicioso em todo seu sistema.

Pode ser inserido em arquivos de execução de softwares, como programas e jogos e até mesmo em uma apresentação de slides, sem que a vítima tome conhecimento do problema. Este arquivo atua na execução de funções conhecidas como keyloggers (gravam os conteúdos digitados em um teclado de computador), além da possibilidade de acessar um sistema bem como tornar administrador do mesmo, podendo realizar cópias de dados contendo informações confidenciais.

### 1.4. *SNIFFING*

Técnica que consiste em gravar pacotes de dados que trafegam em uma rede não criptografada que pode conter dados importantes como senhas, dados bancários, além de outras informações

## 2. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A doutrina traz inúmeras classificações para os crimes cibernéticos. Para Damásio de Jesus, são classificados como crimes informáticos próprios, impróprios, mediatos e mistos.

### 2.1. CRIMES VIRTUAIS PRÓPRIOS

Para Damásio, nos crimes informáticos próprios “o bem jurídico ofendido é a tecnologia da informação em si”, ou seja, são crimes consumados somente com o uso de um computador vinculado à internet, que é elemento essencial para a prática do delito, e o bem jurídico tutelado são os dados.

Para exemplificar crime virtual próprio, podemos citar a invasão de sistemas, a invasão de softwares, de dispositivos móveis, de computadores, sendo por meio de vírus e malwares.

Nota-se que o indivíduo que utiliza desta ferramenta para cometer os delitos tem um conhecimento maior sobre o computador e/ou internet, sendo indivíduos específicos, como os *hackers* e os *crackers*.

### *2.1.1. Hackers x Crackers*

São indivíduos com grande conhecimento técnico e/ou especializado na *internet*, que sabem qual a melhor maneira de agir ilegalmente para a obtenção de informações e dados de suas vítimas.

Os *Crackers*, do verbo inglês *"to crack"*, que significa quebrar, são pessoas que tem conhecimentos de informática e os utilizam para violar sistemas de segurança e, assim, roubar dados e senhas de acesso, além de, ilegalmente, invadir redes para fins criminosos.

O *hacker* é um programador de sistemas, não necessariamente um criminoso. Atualmente, podem até mesmo auxiliar na investigação policial de crimes cibernéticos e cooperar no desenvolvimento de *softwares* de segurança.

Portanto, pode-se dizer que todo cracker é um hacker, mas nem todo hacker é um cracker.

## 2.2. CRIMES VIRTUAIS IMPRÓPRIOS

Já os crimes impróprios, que possuem um computador como ferramenta para sua prática, são crimes tipificados no Código Penal, classificados como crimes comuns que podem ser praticados tanto no mundo real, quanto no virtual, que envolvem, por exemplo, ameaça, calúnia, difamação, injúria, estupro virtual, pedofilia, fraudes, violação de propriedade intelectual, dentre outros.

Damásio traz a seguinte explicação: “Como sabemos, a informática trouxe em seu bojo novas formas de realizar velhos crimes. Ameaça será sempre ameaça, difamação sempre será difamação, estelionato sempre será estelionato, não importando se praticados por intermédio do computador ou não”.

## 2.3. O CRIMES VIRTUAIS MISTOS

Os crimes virtuais mistos são complexos e protegidos pela lei por mais de um bem jurídico, ou seja, resguarda o bem jurídico informático e outro distinto.

> Para delitos Informáticos Mistos ou crimes complexos, pode-se afirmar que são crimes que contem a fusão de mais de um tipo penal, em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar o bem jurídico de natureza diversa. (HIPPLER. 2012)

## 2.4. CRIMES VIRTUAIS MEDIATOS OU INDIRETOS

Os crimes informáticos mediatos ou indiretos tem início no mundo cibernético e são consumados no mundo real, como por exemplo o criminoso que invade o sistema de um banco com o intuito de transferir indevidamente valores para sua conta.

Neste sentido, é o entendimento de VIANNA:

> O acesso não autorizado será executado como delito-meio para se poder executar o delito-fim que consiste na subtração da coisa alheia móvel. Desta forma, o agente só será punido pelo furto, aplicando-se ao caso o princípio da consunção. (VIANNA, 2003)

# 3. DE QUEM É A RESPONSABILIDADE?

Inicialmente, no Brasil, o tema fora tratado como direito penal econômico e, em 18 de dezembro de 1987, fora editada a Lei n° 7.646/87, cujo objetivo era proteger a propriedade intelectual sobre softwares e sua comercialização no país.

Na década de 90 foi sancionada a Lei 8.137/90, que delibera sobre os crimes praticados contra a ordem tributária. Além disso, somente com a promulgação da Lei 9.883/2000 que os legisladores passaram a abranger a regulamentação de outros crimes não econômicos relacionados à Internet.

A respectiva legislação visa proteger os dados e os sistemas de informação, principalmente punindo os atos criminosos cometidos por agentes públicos que violem os sistemas de informação da administração pública.

Por fim, a Lei n.º 12.695/2014, comumente conhecida como “Marco Civil da Internet”, regulamenta o uso da Internet, estabelecendo princípios e normas que garantem melhor proteção aos internautas.

## 3.1. LEI N.º 12.695/2014 – O MARCO CIVIL DA INTERNET

Com o avanço da tecnologia na informática, aumentou cada vez mais a necessidade da sociedade de utilizar o ambiente virtual para diversos fins: trabalho, estudo, comercialização, prestação de serviços, comunicação, entre outros.

O "Marco Civil da Internet" foi criado a partir da fusão de diversos projetos com ideias semelhantes, e consolidou-se através da descoberta da espionagem que o governo americano fazia contra o Brasil e outras nações.

Assim, no dia 23 de abril de 2014, a Lei nº 23. 12.695/2014 foi aprovada pela Presidente Dilma Rousseff, estabelecendo princípios, garantias, obrigações e direitos para os internautas.

O capítulo I dos dispositivos legais citados estabelece conceitos, princípios, direitos e obrigações do uso da Internet em nível nacional e estabelece diretrizes para a atuação do poder público neste sentido.

O Capítulo II define os direitos e garantias dos usuários, assegurando a proteção da privacidade e da vida privada dos usuários, garantindo que estes tenham o direito de obter informações esclarecidas sobre as políticas de uso de sites, provedores e redes sociais.

O Capítulo III especifica a conectividade e os aplicativos encontrados na Internet, definindo vários padrões. A neutralidade da rede, diretriz estabelecida neste capítulo, é importante, pois faz com que os responsáveis pela transmissão, comutação ou roteamento tratem imparcialmente sobre qualquer pacote, independentemente de origem, destino, conteúdo, serviço ou aplicação.

Além disso, conforme acima mencionado, é proibido o impedimento, monitoramento, filtragem ou análise do conteúdo dos pacotes de dados, sob pena de multa para reparação do dano causado.

Outrossim, dados pessoais e registros de comunicações privadas são especialmente protegidos, pois determinam que o provedor cuide da proteção da intimidade, da vida

privada, da honra e da imagem de todas as partes direta ou indiretamente relacionadas, estando sujeito a penalidades civis e criminais.

Prevê também a responsabilidade por danos causados a terceiros, estipulando que os provedores não são civilmente responsáveis pelos danos causados por conteúdo de terceiros, salvo se, em descumprimento de ordem judicial, o provedor não tomar as providências necessárias no prazo legal.

Em contrapartida, o Capítulo IV trata das diretrizes para a atuação dos entes públicos no desenvolvimento da Internet no Brasil.

Finalmente, o Capítulo V traz as disposições finais que estabelecem a liberdade de escolha dos usuários no uso de programas de computador, além de incentivar a manutenção dos interesses e direitos previstos nesta Lei nas esferas administrativa e judicial.

## 3.2. LEI N.º 12.737/2012 – LEI CAROLINA DIECKMANN

Popularmente conhecida como “Lei Carolina Dieckmann”, a Lei n° 12.737/2012 foi reconhecida no dia 03 de dezembro de 2012 pela presidente Dilma Rousseff, que além de alterar os artigos do Código Penal Brasileiro, os tipificou como delitos praticados por meios virtuais.

Esta lei tramitou pelo Congresso Nacional mediante Projeto de Lei n° 2793/2011 diante do que sofreu a atriz brasileira Carolina Dieckmann, que teve todos os dados de seu computador pessoal copiados e, posteriormente, fotos íntimas replicadas na internet.

Apesar de esta Lei ter sido criada pelos fatos ocorridos com Carolina Dieckmann, ela visa proteger os dados pessoais de todos os cidadãos brasileiros.

Diante da falta de uma lei específica, houve dificuldade em enquadrar e punir estes infratores. Assim, o legislador acrescentou no Código Penal brasileiro os artigos 154-A e

154-B, novo tipo penal denominado de “Invasão de dispositivo Informático”. Também foi inserido no artigo 266 o parágrafo 1°, que prevê como crime a conduta de interromper serviço telemático ou de informação de utilidade pública e também foi criado no artigo 298 do Código Penal o parágrafo único, estabelecendo que também configura crime de falsidade de documento particular a conduta de falsificar ou alterar cartão de crédito ou de débito.

Conforme o avanço da tecnologia, algumas leis são criadas para poder preencher essa lacuna no ordenamento jurídico. Foi sancionada a Lei n° 14.155/2021 que atualizou o artigo 154-A, trouxe algumas mudanças importantes, como o aumento de pena. No antigo texto legal, a pena para quem cometesse este crime era de 3 (três) meses a 1 (um) ano de detenção, e multa, podendo ainda ser aumentada de um sexto a um terço quando da invasão resultarem prejuízos financeiros. Com esta atualização no texto da Lei, houve um aumento de pena para 1 (um) a 4 (quatro) anos de reclusão, e multa, e se for qualificado, aumento de um terço a dois terços da pena, com aumento de pena de 2 (dois) a 5 (cinco) anos de reclusão. Ainda em seu parágrafo 5° há um aumento de um terço à metade se o crime for praticado contra Presidente da República, governadores, prefeitos, presidente do Tribunal Federal, entre outros dirigentes máximos da administração pública direta ou indireta, de competência federal, estadual, municipal ou distrital.

A Lei de Invasão Informática estabelece a tipificação penal dos crimes informáticos, faz alterações simples ao Código Penal Brasileiro, acrescenta ao Código Penal de 1940 os artigos 154-A e 154-B e modifica os artigos 266 e 298. A redação, nestes termos, segue da seguinte maneira:

> CP - Decreto Lei nº 2.848 de 07 de Dezembro de 1940
>
> **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: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> **§ 1º** 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) Vigência **§ 2º** Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> **§ 3º** Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> **§ 4º** Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência
> **§ 5º** Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência

> **I** - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> **II** - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> **III** - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
> **IV** - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência Ação penal (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012) Vigência.
>
> **Art. 266**. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.
>
> **§ 1 o** Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012) Vigência
> **§ 2 o** Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) vigência
>
> **Art. 298** - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
>
> **Parágrafo único**. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) Vigência Falsidade ideológica. (BRASIL, 2012).

A grande importância desta atualização está no aumento de pena e no objetivo, que é esclarecer que o sujeito passivo do crime não é apenas o dono do aparelho, mas também alguém que utiliza tal aparelho e teve sua privacidade violada.

O artigo 154-B narra que somente se procede mediante representação os crimes previstos no artigo 157-A, que como regra é de ação penal pública condicionada a representação, porém se o crime for cometido contra algum dos representantes descritos no parágrafo 5° do artigo 157-A esta ação será pública incondicionada.

Estudiosos acreditam que a Lei Básica específica carece de maior proteção, é de tipificação vaga, ainda está subordinada ao Direito Penal e que não traz mudanças importantes no

ordenamento jurídico, precisando de legislação mais aprofundada para comprovar e delimitar efetivamente os diversos crimes informáticos não reconhecidos pela Lei.

## 3.3. Lei N.º 13.709/2018 – Lei Geral da Proteção De Dados (LGPD)

O objetivo desta lei é colocar regras para proteger os dados pessoais, inclusive em meios digitais (dados que identificam de alguma forma uma pessoa, direta ou indiretamente) e quem deve cumprir esta lei são as pessoas (físicas ou jurídicas, de direito público ou privado) que fizerem tratamentos de dados pessoais com algum fim lucrativo.
Destaca o Artigo 1° da LGPD:

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

Com o aumento dos usuários em plataformas digitais, houve aumento proporcional da preocupação em regulamentar e garantir maior segurança jurídica dos dados destes usuários. A LGPD surgiu com a finalidade de tratar de forma adequada os dados pessoais no meio digital, normatizando tudo o que tem dados pessoais no meio digital.

> A proteção de dados é uma das formas para se proteger a privacidade da pessoa. Esse direito é parcela do Direito à Privacidade que está positivado em nossa Constituição Federal. É importante destacar que em 2020 o STF já se posicionou informando que o direito à proteção de dados é um direito fundamental e no final de 2021, a PEC n. 17/2019 incluiu este direito expressamente no art.5º, da Carta Magna, em razão da sua previsão difusa atualmente no texto constitucional (GALERA, 2021, p. 9).

Observando o artigo 2° que narra sobre o tratamento dos fundamentos da LGPD:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;

> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

A LGPD modificou a forma de como as empresas e órgãos públicos devem tratar dos dados pessoais das pessoas que estão associadas aos empreendimentos, abrangendo os dados de clientes, dados de colaboradores, prestadores de serviços e demais. Ou seja, todo o público que se faz essencial para o desenvolvimento de uma empresa devem ter seus dados, em geral, tratados de maneira adequada.

Porém, nesta Lei ainda há exceções às adequações que não são aplicadas dentro daquilo que aponta o art. 4°, conforme segue:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> I- Realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> II- realizado para fins exclusivos de:
> a) segurança pública;
> defesa nacional;
> segurança do Estado; ou
>
> b) atividades de investigação e repressão de infrações penais; ou
> I - Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (BRASIL, 2018).

Em seu artigo 7° estabelece o tratamento de dados pessoais, que de acordo com o doutrinador Ricardo Oliveira (2021):

> A LGPD estabeleceu dez bases legais de tratamento de dados pessoais não sensíveis ou comuns, tais como nome, CPF, RG, números identificadores, etc., conforme consta no seu artigo 7º, bem com estabeleceu nove bases legais para o tratamento de dados pessoais sensíveis, assim considerados os dados pessoais "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, inciso II)". (OLIVEIRA, 2021, p.11).

Com o avanço da tecnologia sob a ótica do mundo digital, o Brasil vem avançando, ainda que lentamente, em soluções para combater os crimes cometidos neste meio.

A LGPD é configurada como um marco importante para a legislação do nosso país, emitindo limites para a privacidade e o uso responsável de dados pessoais utilizados por empresas, que devem se adequar a Lei para que não haja violação ou o não cumprimento das normas que resultarão no cumprimento das sanções previstas. "Os agentes em razão de infrações cometidas estão sujeitos às sanções administrativas, que vão desde advertência, multas até a proibição parcial ou total do exercício das atividades ligadas ao tratamento de dados. " Art. 52 da Lei 13.709, de 14 de agosto de 2018 (Brasil, 2018).

# 4. UMA VISÃO DA CRIMINALIDADE CIBERNÉTICA EM OUTROS

Os primeiros casos de crimes cibernéticos ocorreram em meados de 1960, onde os criminosos manipulavam dados presentes nos computadores, que consistia no abuso ilegal de sistemas, espionagem, sabotagem, sendo, para a época, de difícil localização e punibilidade destes criminosos.

No entanto, no ano de 1980, o tema passou por mudança radical, pois alguns crimes foram identificados e divulgados por meios virtuais, como por exemplo a pirataria de software, manipulação de valores em caixas eletrônicos, abuso de telecomunicações, dentre outros.

Diante das práticas de crimes informáticos nestas épocas, começaram a surgir as primeiras legislações a fim de regulamentar a prática destes delitos. Os Estados Unidos da América, no ano de 1984, foram os primeiros a criar legislações em seu ordenamento jurídico, como *"Crime Control Act"* e "*Computer Fraud and Abuse Act"*, no ano de 1986.

Após, a Alemanha, em 1986, criou a Lei *"Computer Kriminalitat"*, em seguida, no ano de 1988 a França criou a Lei *"Godfrain"*. Posteriormente a Espanha integrou os crimes informáticos na reforma de seu Código Penal.

## 4.1. CONVENÇÃO EUROPÉIA DE CRIMES CIBERNÉTICOS – CONVENÇÃO DE BUDAPESTE

Em 23 de novembro de 2001, na Hungria, por meio do Conselho da Europa (*Council of Europe*) que reúne 45 Estados membros, até mesmo membros da União Europeia, desenvolveu a Convenção de Budapeste, que trata do crime no ambiente virtual global. Esta convenção visa promover a cooperação internacional contra o cibercrime.

O documento, elaborado pela Comissão Europeia de Assuntos Criminais, com o apoio de um comitê de especialistas, lista os principais crimes cometidos por meio da rede global de computadores, sendo o pioneiro a tratar internacionalmente sobre os crimes cibernéticos.

Além disso, a referida convenção está dividida em quatro capítulos com cinco títulos. O capítulo I objetiva padronizar algumas terminologias, como "*Computer System*" (sistema de computador), "*Service Provedor*" (provedor de serviços), dentre outros.

Os próximos capítulos apresentam medidas a serem tomadas sob a ótica das legislações nacionais, posteriormente estabelecendo leis e sanções penais diante das condutas que configurarem crime.

O título I precisa, a nível nacional, quais infrações serão definidas aos países assinantes em discordância a disponibilidade de sistemas, dados informáticos, confidencialidade e integridade. Já o título II consagra os delitos relacionados a computadores, como modificações ou eliminações de dados.

O título III é responsável especialmente pela regulamentação dos crimes de pornografia infantil, além de instituir outras infrações. O título IV trata de infrações relacionadas à violação de direito de conexos e de autor.

Por último, o título V estabelece os deveres e sanções os quais abordam matérias de ordem processual, como busca e apreensão de dados alocados em sistemas, além de firmar a obrigação do provedor de serviços manter os registros de todos os dados, além de transferi-los às autoridades competentes quando solicitado.

Ainda, destaca-se que, em casos que houver pluralidade partes ocorrendo a reivindicação de competência para processar e julgar infração supostamente cometida, todos precisam se reunir para acordar da jurisdição mais adequada.

A convenção teve a assinatura de mais de 60 países e é utilizada como diretriz para a legislação local por aproximadamente 160 outros países. O Brasil teve sua adesão à Convenção de Crimes Cibernéticos na capital húngara em novembro de 2001, porém só teve a aprovação do Senado apenas em 2021

# 5. CONSIDERAÇÕES FINAIS

O avanço da tecnologia e a ascensão dos computadores e da internet propiciou um novo mundo para a população global. Este “cibermundo” abriu portas para pessoas físicas e jurídicas, com inúmeros campos de atuação, transformando o cotidiano de cada um, o modo de agir e pensar, além dos benefícios das demandas do dia-a-dia, seja pessoal ou comercial.

Contudo, essa inovação trouxe consigo um lado obscuro: com o avanço da tecnologia também houve o aumento de crimes comuns e novos crimes, todos praticados no “ciberespaço”, mostrando ao judiciário global a necessidade de atualizar o ordenamento jurídico.

Em sua maioria, os crimes praticados na internet envolvem a utilização de softwares criminosos, como a criação de vírus, que são popularmente conhecidos. Geralmente, estes crimes podem ser cometidos por pessoas comuns, mas, em também são praticados por indivíduos específicos que tem um conhecimento superior sobre as ferramentas virtuais, como os *hackers*, *crakers e cyberterrorists*.

Por tempos considerado “terra sem lei”, o ambiente virtual é de difícil localização e precisão de tempo e local do crime e do criminoso, o qual por vezes age de qualquer lugar do mundo, atingindo uma ou milhares de pessoas ou empresas ao mesmo tempo, muitas vezes sem deixar pistas, dificultando que as autoridades o encontrem e apliquem devida punição.

É essencial a informação de localização e identificação, pois a partir destas, poderá encontrar o território para que a sanção penal seja aplicada. No entanto, ainda são poucas as leis representadas por comportamentos criminosos no âmbito virtual, o que na verdade dificulta a punição dos infratores.

No brasil já foram aprovadas algumas leis, como, lei n. º 12.737/2012 – lei Carolina Dieckmann, lei 12.695/2014, lei n.º 12.695/2014 – marco civil da internet, e ratificou recentemente a lei n.º 13.709/2018 – lei geral da proteção

DE DADOS (LGPD), que trouxe muitos avanços nos direitos e obrigações dos usuários e provedores de Internet, mas, infelizmente, ainda não é o suficiente para combater a alarmante taxa de crescimento do crime cibernético.

Por isso, é necessário desenvolver leis específicas para combater o cibercrime e assegurar os dados dos usuários.

# BIBLIOGRAFIA

BELLOTTO,Tony. DOM, editora Companhia das Letras

BRASIL, *Estatuto da Criança e adolescente* - Lei nº 8.069/90.

BRASIL. *Constituição da República Federativa do Brasil* de 1988

CARVALHO, André. *Os impactos sociais da lei áurea*, intranet da camara,. Disponivel em https://www.cms.ba.gov.br/intranet/artigo/5 acesso em: 10/07/2022

CAPEZ, Fernando; PRADO, Stela. Código Penal Comentado. 6. ed. São Paulo: Saraiva, 2015.

DEL-CAMPO, Eduardo Roberto Alcântara; OLIVEIRA, Thales Cezar de. Estatuto da Criança e Adolescente. 6ª ed. São Paulo: Editora Atlas, 2009. (Série Leituras Jurídicas: Provas e Concursos, v. 28).

DOWDNEY, Luke. Crianças do tráfico – um estudo de caso de crianças em violência armada organizada no Rio de Janeiro. Rio de Janeiro: 7 Letras, 2004.

FERNANDES, Daniela. 4 dados que mostram por que Brasil é um dos países mais desiguais do mundo, segundo relatório, BBC news Brasil, 07/12/2021. Disponivel em https://www.bbc.com/portuguese/brasil-59557761#:~:text=Os%2010%25%20mais%20ricos%20do%20mundo%20ganham%2052%25%20da%20renda,possuem%2076%25%20da%20fortuna %20global acesso em: 22/06/2022

GOMES, Luiz Flávio. Lei de Drogas Comentada. Revista Dos Tribunais, 2013.

GOMES, Luis Flavio. O conceito de organização criminosa é um fantasma, coluna do LFG, 3 de março de 2011, 12h20. Disponivel em https://www.conjur.com.br/2011-mar 03/coluna-lfg-brasil-conceito-organizacao-criminosa-fantasma#:~:text=Dentro%20do%20Direito %20Penal %20brasileiro,e%20dos%20autores % 2 0de%20fic%C3%A7%C3%A3o). acesso em 05/04/2022

GONÇALVES, Alexandre Cebrian Araújo; GONÇALVES, Victor Eduardo Rios; Lenza, Pedro. Direito Processual Penal Esquematizado. 2. ed. São Paulo: Saraiva, 2013

GRUMICHÉ, Mônica Cristina Dutra. Da ideia de infância em jean-jacques rousseau ou do “sono da razão” universidade federal de santa catarina programa de pós-graduação em educação, 2012.Disponivelem:https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/100465 /309796.pdf?sequence=1&isAllowed=y acesso em: 02/03/2022

JUSBRASIL. Informação Jurídica que Transforma. Disponivel em https://www.jusbrasil.com.br/

MENEZES, Leilane. Meninos-Soldados: a infancia a serviço do trafico de drogas, Metropole, 29/09/2019. Disponivel em https://www.metropoles.com/materias-especiais/crime-ou-exploracao-criancas-e-adolescentes-trabalham-como-soldados-para-o-trafico-de-drogas

PAIVA, Giovana Ayres Arantes, artigo de doutoranda do programa san tiago dantas (unesp. Unicamp e puc - sp) reflexões sobre crianças e adolescentes no tráfico do rj, unesp 2018. Disponivel em https://www2.unesp.br/portal#!/noticia/32965/reflexoes-sobre-criancas-e-adolescentes-no-trafico-do-rj/ acesso em 02/04/2022

PYL,Bianca. O trabalho infantil no tráfico de drogas e a punição das vítimas, Rese Peteca. Disponivel em https://livredetrabalhoinfantil.org.br/especiais/trabalho-infantil-sp/reportagens/o-trabalho-infantil-no-trafico-de-drogas-e-a-punicao-das-vitimas/

Relatório mundial sobre drogas 2021 avalia que pandemia potencializou riscos de dependência, viena, 24/05/2021, unodoc. Disponivel em https://www.unodc.org/lpo-brazil/pt/frontpage/2021/06/relatorio-mundial-sobre-drogas-2021-do unodc_-os-efeitos-da-pandemia-aumentam-os-riscos-das-drogas--enquanto-os-jovens-subestimam-os-perigos-da-maconha-aponta-relatorio.html acesso em : 24/06/2022

Rocha,andréa pires. Proibicionismo e a criminalização de adolescentes pobres por tráfico de drogas,scielo2013.Disponívelem:https://www.scielo.br/j/sssoc/a/5qhqgrm7crznqc5j33xtfkc/?lang=pt

SOUZA, Percival. O sindicato do crime: PCC e outros grupos. São Paulo: Ediouro, 2006.

Tráfico de drogas: pior forma de trabalho infantil. Site Prioridade Absoluta, 12/07/2020. Disponivel em https://prioridadeabsoluta.org.br/noticias/trafico-de-drogas-pior-forma-de-trabalho-infantil/ acesso em: ecesso em: 09/05/2022

Varella, drauzio. Dependência química –entrevista, site uol, 19/12/2021. Disponivel em https://drauziovarella.uol.com.br/entrevistas-2/dependencia-quimica-entrevista/ acesso em: 29/04/2022

VADE MECUM, 21. Saraiva, 2021

ZALUAR, Alba; NORONHA, José C. de; ALBUQUERQUE, Ceres. Violência: pobreza ou fraqueza institucional? Rio de Janeiro, Instituto de Medicina Social da Universidade Estadual do Rio de Janeiro, 1994.Disponivel em https://www.scielo.br/j/csp/a/hz4z5dBHdrnChgffvBQWRZR/abstract/?lang=pt acesso em: 25/04/2022