UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS III - GUARABIRA
CENTRO DE HUMANIDADES
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

JAILSON DA SILVA ALVES

# A INTERNET DE TODAS AS COISAS E OS CIBERCRIMES

GUARABIRA/PB
2022

JAILSON DA SILVA ALVES

# A INTERNET DE TODAS AS COISAS E OS CIBERCRIMES

Trabalho de Conclusão de Curso (Artigo Científico) apresentado ao Departamento de Ciências Jurídicas da Universidade Estadual da Paraíba - Campus III/CH, como requisito parcial à obtenção do título de Bacharel em Direito.

**Área de concentração:** Direito Penal.

**Orientador:** Prof. Me. Glauco Coutinho Marques.

**GUARABIRA/PB**

**2022**

A474i Alves, Jailson da Silva.
A internet de todas as coisas e os cibercrimes [manuscrito] / Jailson da Silva Alves. - 2022.
26 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Humanidades , 2022.
"Orientação : Prof. Me. Glauco Coutinho Marques , Coordenação do Curso de Direito - CH."

1. Internet. 2. Cibercrimes. 3. Código Penal. I. Título

21. ed. CDD 345

Elaborada por Milena F. Monteiro - CRB - 15/890 BSC3/UEPB

JAILSON DA SILVA ALVES

**A INTERNET DE TODAS AS COISAS E OS CIBERCRIMES**

Trabalho de Conclusão de Curso (Artigo Científico) apresentado ao Departamento de Ciências Jurídicas da Universidade Estadual da Paraíba - Campus III/CH, como requisito parcial à obtenção do título de Bacharel em Direito.

**Área de concentração:** Direito Penal.

Aprovada em: 01 / 08 /2022.

**BANCA EXAMINADORA**

Prof. Glauco Coutinho Marques (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. Geraldo Batista Júnior (Avaliador)
Universidade Estadual da Paraíba (UEPB)

Prof. Ramon Pontes de Freitas Albuquerque (Avaliador)
Universidade Estadual da Paraíba (UEPB)

A minha esposa Maria das Dores, a minha filha Rebeca, ao meu irmão Valmir e ao amigo Abraão Falcão de Carvalho, DEDICO.

“É melhor prevenir os crimes do que ter de puni-los. O meio mais seguro, mas ao mesmo tempo mais difícil de tornar os homens menos inclinados a praticar o mal, é aperfeiçoar a educação.”

[Cesare Beccaria]

## SUMÁRIO

# A INTERNET DE TODAS AS COISAS E OS CIBERCRIMES

# THE INTERNET OF EVERYTHING AND CYBERCRIMES

Jailson da Silva Alves


## RESUMO

O objetivo deste artigo consiste em averiguar se o delito de invasão de dispositivo informático tipificado no Código Penal brasileiro é efetivo para contemplar os cibercrimes que podem ser praticados face ao uso da tecnologia ofertada pela Internet de Todas as Coisas que compreende coisas, processos, dados e pessoas. Os procedimentos metodológicos consistiram sobretudo em pesquisa bibliográfica e utilizou-se o método dedutivo. O Direito é produto social e deve atualizar-se conforme o avanço tecnológico da sociedade, visando estabelecer a ordem, paz, segurança e justiça. E óbvio, o Código Penal necessita também ser analisado em face de tal contexto.


**Palavras-chave:** Internet. Cibercrimes. Código Penal.


## ABSTRACT

The purpose of this article is to investigate whether the offense of hacking into a computer device defined in the Brazilian Penal Code is effective in addressing cybercrimes that can be committed in the face of the use of technology offered by the Internet of Everything, which comprises things, processes, data and people. The methodological procedures consisted mainly of bibliographic research and the deductive method was used. Law is a social product and must be updated according to the technological advance of society, aiming to establish order, peace, security and justice. Of course, the Penal Code also needs to be analyzed in this context.


**Keywords:** Internet. Cybercrimes. Penal Code.

## 1. INTRODUÇÃO

Vivemos numa época em que a sociedade é dependente da conexão à Rede Mundial de Computadores para a realização das mais diversas tarefas do dia a dia: trabalho convencional, teletrabalho, home office, estudo, uso de Smartphones, Computadores, Smartwatches, Smart TVs, compras, pagamentos, vendas, relacionamentos, uso das redes sociais, automação comercial, automação residencial, etc. Para a maioria das pessoas, é impossível viver sem a Internet.

A Internet é tão fundamental para a sociedade deste século que a ONU - Organização das Nações Unidas, no ano de 2011, declarou que o acesso à ela é um direito humano básico e que desconectar a população da Web viola a referida política.

Atualmente, essa dependência da sociedade em relação à Internet, deve-se, sobremaneira, à Internet das Coisas (IoT - Internet of Things) e a sua evolução, a

Internet de Todas as Coisas (IoE - Internet of Everything), haja vista que a Internet passou a abarcar além dos computadores, objetos do cotidiano, bem como a interação do ser humano com tais.

Diante dessa hiperconexão e interação, abre-se um leque de possibilidades ainda maior para o cometimento de delitos de forma virtual nas mais diversas esferas.

Sabemos que o Direito necessita adaptar-se às transformações ocorridas na sociedade, conforme informa Nader (2014, p. 51) …'o Direito é um engenho à mercê da sociedade e deve ter a sua direção de acordo com os rumos sociais'.

O objetivo deste artigo consiste em averiguar se o delito de invasão de dispositivo informático tipificado no Código Penal brasileiro é efetivo para contemplar os cibercrimes que podem ser praticados face ao uso da tecnologia ofertada pela Internet de Todas as Coisas.

Para elaboração deste trabalho, os procedimentos metodológicos consistiram em pesquisa bibliográfica (notícias, artigos, monografias, dissertações, livros, leis, etc.), sobretudo na Internet. Sendo desenvolvido de forma qualitativa, descritiva e utilizado o método dedutivo.

Abordar-se-á a evolução da Internet (definição, origem e fases), o conceito e características da IoT, bem como da IoE e suas diferenças, a partir de noções do Magrani (2018), do Santos (et al. 2016, *apud* Marques e Vilar, 2019); da Oracle e da Cisco, do Plano Nacional de Internet das Coisas e da Sakovich (2019). Em seguida, abordaremos o conceito dos cibercrimes de acordo com o pensamento de Lima (2012, *apud* Lucchesi e Hernandez, 2018), a ideia de ciberespaço segundo Lévy (1999), a classificação doutrinária dos crimes virtuais, segundo Jesus (*apud* Carneiro, 2012) e Pinheiro (2016, *apud* Lucchesi e Hernandez, 2018) e citaremos exemplos dos tipos de cibercrimes 'dispostos' no Código Penal. Posteriormente, analisaremos e traçaremos comentários acerca da Lei Carolina Dieckmann, da Lei nº. 14.155/2021, do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, valendo-se de ideias do Rogério Grego (2019), do Jorio e do Boldt (2021) e da Lins (2021). Por fim, tecemos apontamentos acerca dos cibercrimes, baseando-se em concepções da Lins (2021), do Nader (2014), do Coelho (2017 *apud* Lóssio e Santos, 2020), do Magrani (2018), do Greco (2017) e do Nucci (2020).

## 2. EVOLUÇÃO DA INTERNET

### 2.1 Definição/origem

A Internet, rede mundial de computadores e mecanismo de comunicação instantânea e em escala mundial, teve sua origem nos Estados Unidos da América, na segunda metade do Século XX, especificamente no ano de 1969, quando Lawrence G. Roberts ingressou na DARPA (Defense Advanced Research Projects Agency - Agência de Projetos de Pesquisa Avançada de Defesa) e teve a brilhante ideia do projeto ARPANET (Advanced Research Projects Agency Network - Rede da Agência de Pesquisas em Projetos Avançados) junto ao Robert Kahn e ao Howard Frank. Assim, desenvolveram a primeira rede de comutação de pacotes que

inicialmente só tinha conexão com algumas universidades americanas e era basicamente para uso militar.

> A primeira rede de computadores (Arpanet) tinha seus quatro nós localizados na Universidade da Califórnia em Los Angeles, no Stanford Research Institute, na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah... O governo permitia que centros de pesquisa que colaboravam com o Departamento de Defesa dos EUA tivessem acesso à rede para fins de estudos direcionados ao departamento. A Arpanet continuou a se expandir: em 1972 contava com 37 nós e em 1983 com 562. (MAGRANI, 2018, p. 62).

A conexão entre os computadores da ARPANET era possível graças ao protocolo NCP (Network Control Protocol) que possibilitou o desenvolvimento de aplicativos a partir de tais máquinas. E graças a ele, no ano de 1972, Ray Tomlinson desenvolveu o e-mail, fato que mudou radicalmente a comunicação e interação entre pessoas e o homem e a máquina. Devido ao e-mail, a Internet foi saindo do seu papel original (uso militar) e ganhando terreno no uso científico da propagação de informações.

Devido à expansão da Internet para navegação em rede com arquitetura aberta e à necessidade de entrega mais confiável de pacotes de dados, em 1983 a ARPANET adota o protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) que em 1985 consolidou a Internet como a principal rede de comunicação com alcance global.

No ano de 1989, nasce a World Wide Web (WWW) graças ao Tim Berners-Lee que trabalhava dentro do CERN (Conseil Européen pour la Recherche Nucléaire - Organização Europeia para a Pesquisa Nuclear) possibilitando a criação dos primeiros sites e que foi aberto ao público em geral em 1991 e o seu uso despontou a partir de 1993 com o surgimento do browser Mosaic. Este criado pelo NCSA (National Center for Supercomputing Applications - Centro Nacional de Aplicações de Supercomputação) localizado na Universidade de Illinois em Urbana-Champaign, Estados Unidos da América.

A partir de então, a Internet expandiu-se e evolui cada vez mais. Essas fases de evolução são chamadas de era (Web 1.0, Web 2.0, Web 3.0 e atualmente Web. 4.0).

A Web 1.0 foi a fase inicial da propagação da Web, a Web 2.0 pode ser entendida como a Web das Redes Sociais, a Web 3.0 como a Web Semântica e a Web 4.0 tem como características diante da novas emergências atuais, o Big Data, Cloud (computação em nuvem) e IA (Inteligência Artificial).

A Internet aportou no Brasil em setembro de 1988 quando o Laboratório Nacional de Computação Científica - LNCC, localizado em Petrópolis/RJ, estabeleceu conexão com a Universidade de Maryland/EUA, através da rede Bitnet (rede remota norte americana voltada para o meio acadêmico). Meses depois a Internet chega a algumas universidades, a exemplo da USP, da Unicamp, da Unesp, dentre outras.

A Internet no Brasil ultrapassou as fronteiras acadêmicas na metade do ano de 1994, entrando nos lares e sedes de empresas. E Segundo Muller (2008) foi apenas no final do referido ano que o Governo brasileiro voltou o olhar à Internet e decidiu investir em tal campo, colocando a Embratel (Empresa Brasileira de Telecomunicações) e a RNP (Rede Nacional de Ensino e Pesquisa) como

responsáveis pela criação da estrutura básica e exploração comercial da nova tecnologia. Tendo a sua expansão real ocorrida em 1996.

## 2.2 A Internet das Coisas

A ideia da Internet das Coisas está atrelada à Web 3.0, termo concebido por John Markoff, jornalista do New York Times, que é uma evolução da Web 2.0, conceito propagado no ano de 2004 por Tim O'Reilly e Dale Dougherty. Ao passo que esta possibilita a interação de pessoas, aquela utiliza a Internet para cruzamento de dados, que são lidos através de dispositivos que por conseguinte propiciam informações mais precisas.

O termo IoT - Internet of Things, foi alicerçado em 1.999 pelo pesquisador do MIT - Massachusetts Institute of Technology, Kevin Ashton. Não trata-se de uma nova tecnologia, mas de uma nova fase da Internet.

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços. (SANTOS, *et al*. 2016, *apud* MARQUES & VILAR, 2019, p. 04).

De acordo com a Oracle[1], a IoT descreve a rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela Internet.

Essas coisas (objetos) são munidos de chips e processamento e contém o RFID (Radio-Frequency IDentification - Identificação por radiofrequência) e estão presentes em nosso cotidiano, a exemplo, em nossas casas (Smart TV, geladeiras, fechaduras inteligentes, etc.) e de nosso uso, como por exemplo, automóveis, smartwatches, fones de ouvido, etc.

### 2.2.1 Plano Nacional de Internet das Coisas

O Decreto nº. 9.854, de 25 de junho de 2019 institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.

Segundo o Ministério da Ciência, Tecnologia e Inovações, o referido plano busca implementar e desenvolver a Internet das Coisas no País, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais.

De acordo com o disposto no artigo 2º do supracitado Decreto, considera-se Internet das Coisas - IoT:

> I - Internet das Coisas - IoT - a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual

[1] Oracle Corporation é uma empresa multinacional de tecnologia e informática norte-americana, especializada no desenvolvimento e comercialização de hardware e softwares e de banco de dados.

> de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade;
>
> II - coisas - objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação;
>
> III - dispositivos - equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados; e
>
> IV - serviço de valor adicionado - atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos do disposto no art. 61 da Lei nº 9.472, de 16 de julho de 1997.

Um dos objetivos do plano é melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT (art. 3º, I).

## 2.3 A Internet de Todas as Coisas

A concepção da Internet de Todas as Coisas - IoE (Internet of Everything), vem sendo difundida, sobretudo pela Cisco. Para ela, é a conexão de ‘absolutamente’ tudo: coisas, processos, pessoas e dados de todos os tipos, gerando incontáveis conexões de valor diariamente, tanto para os usuários quanto para as empresas.

Enquanto IoT se concentra apenas em objetos físicos a IoE engloba quatro componentes (coisas, processos, dados e pessoas).

Para Sakovich (2019), a IoT, em essência, é a interconectividade de objetos físicos que enviam e recebem dados, enquanto a IoE é um termo mais amplo que inclui, além da IoT, inúmeras tecnologias e pessoas como nós finais.

O surgimento do 5G dará mais crescimento à IoE, pois a conexão ficará mais rápida, estável e possibilitará uma maior quantidade de usuários finais. O 5G aportou oficialmente no Brasil no dia 06 de julho de 2022, em Brasília/DF e segundo a Anatel - Agência Nacional de Telecomunicações, logo mais chegará em Belo Horizonte, Porto Alegre, João Pessoa e São Paulo. A estimativa é que até janeiro de 2026, as áreas urbanas estejam contempladas com tal tecnologia. Apesar de estar em fase inicial de implementação em nosso país, em diversas outras nações a sua existência já é real, a exemplo dos Estados Unidos da América que iniciou o seu uso comercial em janeiro de 2020.

O 5G é uma evolução da atual rede de celulares, a 4G e vem com a promessa de elevar a banda larga móvel a altíssimos padrões de velocidade de conexão e um aumento significativo de usuários simultâneos. Para termos uma ideia, enquanto o 4G confere ao usuário final, velocidade média 33 Mbps, o 5G poderá fornecer conexões que podem alcançar até 10 Gbps.

# 3. CIBERCRIME

## 3.1 Definição

Cibercrime é sinônimo de crime cibernético, crime virtual, crime informático, crime digital, crime eletrônico, dentre outros. Neste trabalho utilizar-se-á o termo ‘cibercrime’.

Partindo da ideia da corrente finalista, a majoritária no nosso país e no exterior, que define crime como fato típico, antijurídico e culpável (NUCCI, 2020), chegamos ao conceito do cibercrime.

> [...] qualquer conduta humana (omissiva ou comissiva) *típica*, *antijurídica* e *culpável*, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, tenha facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo às pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor embora não prejudique de forma direta ou indireta à vítima.
> Portanto, considera-se condutas delituosas contra ou utilizando-se um sistema de informática (LIMA, 2012, *apud* LUCCHESI & HERNANDEZ, 2018, p. 03).

Segundo Andrion (2021), o termo cibercrime surgiu no fim da década de 1990 em Lyon, na França, logo após uma reunião de um subgrupo das nações do G8 que discutiu o tema. Por conseguinte, a referida palavra passou a designar as infrações penais praticadas no espaço digital.

Para termos um entendimento mais claro da ideia de cibercrime é importante sabermos o que é o ciberespaço. Na concepção de Pierre Lévy, o ciberespaço é tido como:

> [...] o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Essa definição inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações. Consiste de uma realidade multidirecional, artificial ou virtual incorporada a uma rede global, sustentada por computadores que funcionam como meios de geração de acesso (LÉVY, 1.999, p.92).

## 3.2 Classificação

A doutrina costuma classificar os crimes virtuais em próprios e impróprios.

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (JESUS *apud* CARNEIRO, 2012).
>
> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado

> naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática (JESUS *apud* CARNEIRO, 2012).

Assim, os crimes cibernéticos puros são tipificados sobretudo na Lei nº. 12.737/2012 e na Lei nº 14.155/2021 e os que em grande parte ainda não possuem tipificação na nossa legislação e os impuros, os crimes comuns tipificados no Código Penal e que o agente delituoso emprega-se do espaço virtual para executá-los. Ainda, Pinheiro (2016, p. 172, *apud* Lucchesi e Hernandez, 2018, p. 03), considera os impróprios como “(...) um crime de meio, ou seja, utiliza-se do meio virtual”.

Vejamos os ‘cibercrimes próprios’ tificados no CP: contra a inviolabilidade dos segredos - Invasão de dispositivo informático (art. 154-A); contra a segurança dos meios de comunicação e transporte e outros serviços públicos - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública [*defacement*] (art. 266, § 1º); contra o patrimônio - Furto qualificado [*furto mediante fraude*] (art. 155, § 4º-B); estelionato e outras fraudes - Fraude eletrônica (art. 171, § 2º-A); crimes sexuais contra vulnerável - Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia [*revenge porn - pornografia de vingança*] (art. 218-C); crimes praticados por funcionário público contra a administração em geral - Inserção de dados falsos em sistema de informações (art. 313-A); Modificação ou alteração não autorizada de sistema de informações (art. 313-B).

São exemplos de ‘cibercrimes impróprios’ dispostos no Código Penal Brasileiro: contra a vida - Homicídio (art. 121); Induzimento, instigação a suicídio ou a automutilação (art. 122); contra a honra - Calúnia (art. 138); Difamação (art. 139, CP); Injúria (art. 140); contra a liberdade pessoal - Ameaça (art. 147); Perseguição [*Stalking*] (art. 147-A); contra a inviolabilidade do domicílio - Violação de domicílio (art. 150); contra a inviolabilidade dos segredos - Divulgação de segredo (art. 153); contra o sentimento religioso - Ultraje a culto e impedimento ou perturbação de ato a ele relativo (art. 208); contra a liberdade sexual - Estupro (art. 213); lenocínio e tráfico de pessoa para fim de prostituição ou outra forma de exploração sexual - Favorecimento da prostituição ou outra forma de exploração sexual (art. 228); ultraje público ao pudor - Ato obsceno (art. 233); Escrito ou objeto obsceno (art. 234); contra a paz pública - Incitação ao crime (art. 286); Apologia de crime ou criminoso (art. 287); de outras falsidades - Falsa identidade (art. 307).

## 4. EVOLUÇÃO LEGISLATIVA DOS CIBERCRIMES

### 4.1 Lei nº. 12.737/2012

A Lei nº. 12.737, de 30 de novembro de 2012, foi o divisor de águas da tipificação criminal de delitos informáticos na legislação brasileira, pois antes dela o Código Penal era omisso quanto à tal matéria. Essa norma legal ficou conhecida como a Lei Carolina Dieckmann, em alusão à referida atriz que 36 (teve trinta e seis) fotos íntimas hackeadas do seu computador e que foram divulgadas na Internet sem o seu consentimento, alcançando grande repercussão nacional.

A Lei Carolina Dieckmann acrescentou ao Código Penal os artigos 154-A e 154-B, bem como alterou a redação dos artigos 266 e 298. Tificou-se o crime de invasão de dispositivo informático.

> 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.
>
> § 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.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 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:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 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.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> 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
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> 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.
>
> Art. 266.. .....
>
> § 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.
>
> Art. 298.. .....
>
> Falsificação de cartão

> Parágrafo único. Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito.

A lei em comento veio a tipificar os cibercrimes chamados de próprios ou puros pelos doutrinadores. Ela foi um embrião da ‘segurança’ no ambiente virtual, uma luz no fim do túnel à proteção da privacidade de dados pessoais de determinado indivíduo na Internet.

Para Grego (2019), o núcleo invadir do artigo 154-A do CP tem o sentido de violar, penetrar, acessar. Segundo ele, dispositivo informático é todo aquele aparelho capaz de receber os dados, tratá-los, bem como transmitir os resultados, a exemplo do que ocorre com os computadores, smartphones, tablets etc. e que tanto a obtenção, adulteração e a destruição de dados ou informações devem ser levadas a efeito sem a autorização expressa ou tácita do titular do mecanismo.

## 4.2 Lei nº. 14.155/2021

A Lei nº. 14.155, de 27 de maio de 2021, oriunda do Projeto de Lei nº. 4.554/2020 de iniciativa do Senador Izalci Lucas (PSDB/DF), alterou o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela Internet.

> 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 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> “Art. 155. .....
>
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
>
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
>
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.
>
> “Art. 171. .....
>
> Fraude eletrônica

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

A Lei supracitada também alterou o Código de Processo Penal, acrescentando o parágrafo 4º ao artigo 70 (competência do lugar da infração):

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

Percebemos com essa lei mais atual que foi removido do artigo 154-A o termo ‘mediante violação indevida’. Doravante para o entendimento do referido crime, basta invadir o dispositivo com o fim delituoso e sem a autorização da vítima. A citada norma legal adicionou o § 4º-B e o § 4º-C (furto mediante fraude cometido por meio de dispositivo eletrônico ou informático) ao artigo 155 (furto [qualificado]) e acrescentou o § 2º-A e § 2º-B (fraude eletrônica) ao artigo 171 (crime de estelionato). Bem como, a pena imposta à transgressão penal do *caput* do artigo 154-A ficou bem mais severa: antes era detenção de três meses a máximo um ano e multa, agora é de reclusão de um até quatro anos e multa.

Assim, estabelecida a pena de reclusão, o regime inicial de cumprimento passou a ser o fechado. No entanto, com base na pena mínima de 01 (um) ano, cabe a suspensão condicional do processo (art. 89 da Lei 9.099/1995) e o Acordo de Não Persecução Penal - ANPP (art. 28-A do Código de Processo Penal).

Essa lei mostra que a legislação penal deve atualizar-se face às evoluções tecnológicas da sociedade.

> A nova Lei surge em um contexto de profundas modificações da esfera pública a partir da reestruturação dos meios de comunicação e da existência de um novo processo, materializado por intermédio da proliferação das mídias sociais, potencializadas pelo avanço da tecnologia e da cultura digital (Jorio; Boldt, 2021).

### 4.3 Lei nº. 12.965/2014

A Lei nº. 12.965, de 23 de abril de 2014 é mais conhecida com o Marco Civil da Internet e conforme dispõe em seu artigo 1º, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

De acordo com a lei em comento, a Internet no nosso país tem como princípios, dentre outros, a garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; proteção dos dados pessoais, na forma da lei e preservação e garantia da neutralidade de rede (art. 3º, I, II, III e IV).

Ao usuário de Internet, nos termos do artigo 7º incisos I ao III, são assegurados ao usuário o direito de: inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

Os registros de conexão e de registros de acesso às aplicações da Internet, devem ser guardados pelo provedor sob sigilo e em ambiente seguro, pelo prazo de 01 (um) ano e de 06 (seis) meses, respectivamente (arts. 13 e 15). O vazamento de tais registros, bem como o de dados pessoais e do conteúdo de comunicações privadas, condiciona o autor do fato às seguintes sanções, aplicadas de forma isolada ou cumulativa: advertência, com indicação de prazo para adoção de medidas corretivas; multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; suspensão temporária das atividades; ou proibição de exercício das atividades (art. 12).

Observamos apesar que, para alguns, essa lei veio para dizer que a ‘Internet no Brasil não é terra sem lei’ e para outros é considerada uma espécie de ‘Constituição da Internet’, ela volta sua atenção ao direito de privacidade, deixando em segundo plano o aspecto penal e as sanções aplicadas são brandas.

> A legislação buscando garantir tanto a proteção dos dados dos usuários, quanto permitir acesso a esses mesmos dados em caso de ilícitos, acabou pendendo mais para o lado da proteção de dados, deixando principalmente os aspectos criminais das relações na internet descobertos de maior proteção, pois como já dito, esse tempo de guarda de dados pelos provedores, que foi estabelecido pela legislação passa muito longe do tempo necessário na realidade das investigações de cibercrimes, mesmo mas mais rápidas das diligências policiais são necessários meses para elucidação desses tipos de crimes, tendo em vista a demanda é altíssima (LINS, 2021).

Segundo Amaral (2008, p. 306 *apud* Lins, 2021) o direito de privacidade vista pelo Direito Civil é “o direito de isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa.”

A ideia de privacidade enfatizada na lei aqui explanada, é baseada nos direitos e deveres individuais e coletivos previstos na Constituição Federal de 1.988.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

### 4.4 Lei nº. 13.709/2018

A Lei nº. 13.709, de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), 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.

Em suma, normatiza a forma de como os dados pessoais dos clientes/consumidores devem ser tratados por profissionais liberais e pessoas jurídicas e o cuidado/responsabilidade que devem ter para não vazarem tais informações.

Caso o responsável pelo tratamento deixe escapar determinado dado pessoal do cliente e venha a prejudicá-lo, responderá por sanções administrativas, conforme preconiza o artigo 52 e seus incisos, a exemplo da advertência, com indicação de prazo para adoção de medidas corretivas e a multa simples, de até 02% (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. Ainda, o § 2º do referido artigo informa que o disposto nele não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078/1990 (Código de Defesa do Consumidor) e em legislação específica.

Assim como o Marco Civil da Internet, essa lei coloca em primeiro plano o direito à privacidade.

## 5. APONTAMENTOS ACERCA DOS CIBERCRIMES

É mais que comum e perceptível, a cada década que se decorre, a nossa dependência do mundo informatizado. Quanto mais as pessoas se conectam à Internet, com maior intensidade ficam expostas e sujeitas a serem vítimas de crimes virtuais. Isso é uma tendência natural.

Consoante o site Olhar Digital, durante o primeiro ano (2020) da Pandemia ocasionada pelo vírus da COVID-19, no Brasil os ataques cibernéticos aumentaram mais de 300% (trezentos por cento), tendo como alvos tanto usuários comuns como órgãos públicos.

De acordo com Lins (2021), o Brasil é o 5º país com mais ocorrências de crimes cibernéticos do mundo, segundo o levantamento da consultoria alemã Roland Berger, no nosso país apenas no primeiro semestre de 2021, totalizou 9,1 milhões de casos de crimes cibernéticos.

Diante desse panorama, a CTT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal tem se preocupado e seus especialistas afirmaram em audiência pública realizada em 15 dezembro de 2021 que o combate ao cibercrime deve ser urgente. A referida audiência ocorreu por requerimento do senador Carlos Viana (PSD-MG).

> Isso nos leva a discutir com muito mais seriedade [o problema]. As ameaças aos países não serão mais clássicas, como no passado. As guerras serão de dados. As nossas hidrelétricas, por exemplo, são todas elas automatizadas. Os aeroportos de todo o mundo também são controlados por dados, que fazem toda a segurança de voos. Numa possível guerra digital, criar confusões nos sistemas internos de um país pode gerar uma defesa muito menor - alertou Carlos Viana.

Em 17 de dezembro de 2021, o Brasil ratificou o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, através do Decreto Legislativo nº. 37/2021, entrando em vigor na data de sua publicação. A Convenção de Budapeste foi o primeiro tratado internacional sobre os cibercrimes e objetiva facilitar a cooperação internacional para combater o crime no espaço virtual. É um importante passo para o Brasil, servindo como norte na orientação de elaboração de legislações sobre o tema.

O Ministério da Justiça e Segurança Pública lançou em 24/03/2022 o primeiro primeiro Plano Tático de Combate a Crimes Cibernéticos do país, visando prevenir e reprimir tal tipo de transgressão. Adotando também medidas educativas, no intuito que o ciberespaço torne-se um ambiente mais seguro.

Para ser efetivo, o Direito necessita andar de mãos dadas com as transformações pelas quais passa a sociedade. Vejamos o que informa Paulo Nader.

> As instituições jurídicas são inventos humanos que sofrem variações no tempo e no espaço. Como processo de adaptação social, o Direito deve estar sempre se refazendo, em face da mobilidade social. A necessidade de ordem, paz, segurança, justiça, que o Direito visa a atender, exige procedimentos sempre novos. Se o Direito se envelhece, deixa de ser um processo de adaptação, pois passa a não exercer a função para a qual foi criado. Não basta, portanto, o ser do Direito na sociedade, é indispensável o ser atuante, o ser atualizado. Os processos de adaptação devem-se renovar, pois somente assim o Direito será um instrumento eficaz na garantia do equilíbrio e da harmonia social (NADER, 2014, p. 53).

É o que podemos reafirmar: *ubi societas, ibi jus* (onde [está] a sociedade aí [está] o direito).

Segundo Coelho (2017 *apud* Lóssio e Santos, 2020), os principais perigos que essa nova roupagem de sociedade com IoE (grifo nosso), a digital, poderá causar são: 1) Danos físicos ou estragos materiais, incluindo ferimentos e morte; 2) Redução ou inibição de sistemas de segurança; 3) Danos de Imagem; 4) Perda de Confiança; 5) Indisponibilidade de Serviços; e, 6) Roubo de Propriedade Intelectual.

A sociedade deve voltar o seu olhar não apenas para as coisas da Internet, mas também para as pessoas, pois elas são os nós finais.

> Ainda que a internet esteja sendo levada às coisas, estas estão conectadas a nós, as pessoas a quem essas coisas passarão a prover serviços e funcionalidades. É nesse sentido que devemos compreender que estamos falando sempre de uma internet das pessoas. Devemos evoluir também na análise crítica a respeito da utilidade dessas criações e nas questões de privacidade e segurança que elas implicam (MAGRANI, 2018, p. 58).

O princípio da legalidade, positivado no artigo 5º, inciso XXXIX, da CRFB/1988 e reiterado no artigo 1º do Código Penal, estabelece que não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal. Ele é a base para aplicação real da lei penal.

> O princípio da legalidade, sem dúvida alguma, o mais importante do Direito Penal. Conforme se extrai do art. 1º do Código Penal, bem como do inciso XXXIX do art. 5º da Constituição Federal, não se fala na existência de crime se não houver uma lei definindo-o como tal. A lei é a única fonte do direito penal quando se quer proibir ou impor condutas sob a ameaça de sanção. Tudo o que não for expressamente proibido é lícito em direito penal. Por essa razão, Von Liszt diz que o Código Penal é a Carta Magna do delinquente (GRECO, 2017, p. 174).

Sabemos que há diversos crimes cibernéticos que não são tipificados no nosso Código Penal. Logo, como punir quem comete suposto delito? Para suprir tal lacuna é necessário nos valermos da analogia *in malam partem*? Vejamos o que informa o Guilherme de Souza Nucci.

> O emprego de analogia não se faz por acaso ou por puro arbítrio do intérprete; há significado e lógica na utilização da analogia para o preenchimento de lacunas no ordenamento jurídico. Cuida-se de uma relação qualitativa entre um fato e outro. Entretanto, se noutros campos do Direito a analogia é perfeitamente aplicável, no cenário do Direito Penal ela precisa ser cuidadosamente avaliada, sob pena de ferir o princípio constitucional da legalidade (não há crime sem lei que a defina; não há pena sem lei que a comine). Assim sendo, não se admite a analogia *in malam partem*, isto é, para prejudicar o réu (NUCCI, 2020, p. 123).

A investigação dos cibercrimes não é uma atividade fácil, haja vista que o Estado *jus puniendi* não oferece mecanismos eficazes para a referida finalidade. As delegacias especializadas da Polícia Civil são poucas e na maioria das vezes são determinados servidores públicos que buscam conhecimento na área por despertarem interesse, chegando a pagarem cursos/especializações com o dinheiro do seu próprio bolso.

Atualmente o perfil do infrator do crime virtual não é mais de um cracker (hacker do mal), isto é um indivíduo com alto grau de conhecimento no mundo da informática, capaz de quebrar um sistema de segurança.

## 6. CONSIDERAÇÕES FINAIS

Percebemos que no atual contexto em que estamos inseridos, a dependência da conexão com a rede mundial de computadores é gritante. Essa hiperconexão cada dia mais visível e real é produto da Internet das Coisas e o seu aprimoramento, a Internet de Todas as Coisas. Ambas não são uma nova tecnologia, mas um novo estágio da Internet. A última é responsável pela conexão de coisas, dados, processos e pessoas, criando uma interação entre tais.

O ciberespaço cada vez mais movimentado é campo visível e propício às práticas dos delitos cibernéticos, podendo o infringente empreender atos contra o sistema informático ou através dele.

Nesse quadro, vem ocorrendo de forma exponencial o aumento dos casos de ataques e crimes aos usuários do mundo virtual, mais perceptível em nosso país, sobretudo a partir da Pandemia da Covid-19. Fato que reflete na realidade cotidiana.

Passos importantes vêm sendo dados no Brasil acerca de medidas ao combate aos cibercrimes, como exemplo a edição de leis, adesão à convenção internacional e recentemente, plano tático de combate, porém tudo ainda de forma tímida. Devemos perceber que o real e o virtual andam de mãos dadas, são complementares, que há uma fusão desses dois mundos.

Alguns crimes cibernéticos ainda não são tipificados do Código Penal, fato que faz com que os infratores desses delitos fiquem à espreita, sem a devida punição legal, pois não podemos considerar crime o que não está definido em lei.

Sabemos que o Direito deve moldar-se às transformações da sociedade. Logo, é imprescindível que o Estado *jus puniendi* promulgue leis para redação de novos tipos penais de cibercrimes ou alteração da redação de alguns crimes de meio, acrescentando até qualificadoras, dê o suporte adequado à Polícia Civil, crie cargos nessa instituição voltados aos profissionais de TI e aumente o número de delegacias especializadas, tudo isso com o objetivo de efetiva punição dos criminosos.

## REFERÊNCIAS

ANDRION, Roseli. **História da segurança virtual: a origem do cibercrime**. Disponível em: <https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-cibercrime-203073/#:~:text=O%20termo%20cibercrime%2C%20entretanto%2C%20surgiu,penais%20praticadas%20no%20%C3%A2mbito%20digital.>. Acesso em junho de 2022.

ALBERTIN, Alberto Luiz; ALBERTIN, Rosa Maria de Moura. A Internet das Coisas irá muito além das coisas. **GV-Executivo**, São Paulo, vol. 16, n. 2, p. 15-19, março/abril, 2017. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/issue/view/3851/1808>. Acesso em fevereiro de 2022.

BARCELLOS, Marco. **Internet de Todas as Coisas: uma 'nova' internet para uma nova era**. Publicado em 15 de Julho de 2013. Disponível em: <https://canaltech.com.br/internet/Internet-de-Todas-as-Coisas-uma-nova-internet-para-uma-nova-era/#:~:text=Quando%20utilizarmos%20esta%20transforma%C3%A7%C3%A3o%20de,Internet%20de%20Todas%20as%20Coisas>. Acesso em fevereiro de 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em janeiro de 2022.

_____. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em janeiro de 2022.

_____. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm>. Acesso em março de 2022.

_____. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em fevereiro de 2022.

_____. **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>. Acesso em fevereiro de 2022.

_____. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em março de 2022.

_____. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14155.htm>. Acesso em março de 2022.

_____. Senado Federal. **Projeto de Lei nº. 4554, de 2020**. Combate a prática de fraude eletrônica, modifica o art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e apresenta hipóteses agravantes. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/144667>. Acesso em 17 de março de 2022.

CAPEZ, Fernando. **Parte especial arts. 121 a 212**. Coleção Curso de direito penal.

V. 2. 20. ed. São Paulo: Saraiva Educação, 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em março de 2022.

CISCO. **The Internet of Everything**. Disponível em: <https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf>. Acesso em fevereiro de 2022.

EVANS, Dave. **A Internet das Coisas: Como a próxima evolução da Internet está mudando tudo**. Cisco Internet Business Solutions Group (IBSG), 2011. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Acesso em fevereiro de 2022.

FACCIONI FILHO, Mauro. **Internet das coisas: livro digital**. Palhoça: UnisulVirtual, 2016. 56 p. Disponível em: <https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things>. Acesso em fevereiro de 2022.

GILLIS, Alexander S. **What is the internet of things (IoT)?** Disponível em: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>. Acesso em março de 2022.

GOMES, Ana Gláucia Lobato Campos. **A Função Social do Direito**. Disponível em: <https://anaglc.jusbrasil.com.br/artigos/450535880/a-funcao-social-do-direito>. Acesso em janeiro de 2022.

GRECO, Rogério. **Curso de Direito Penal: parte geral, volume I**. 19 ed. Niterói, RJ: Impetus, 2017.

_____. **Direito Penal Estruturado**. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2019.

i-SCOOP. **What the Internet of Everything really is – a deep dive**. Disponível em: <https://www.i-scoop.eu/internet-of-things-iot/internet-of-everything-2/>. Acesso em janeiro de 2022.

JORIO, Israel Domingos; BOLDT, Raphael. **Comentários à Lei 14.155/2021**. Disponível em: <https://raphaelboldt.jusbrasil.com.br/artigos/1227518895/comentarios-a-lei-14155-2021#:~:text=COMENT%C3%81RIOS%20%C3%80%20LEI%2014.155%2F2021&text=155%2C%20de%2027%20de%20maio,forma%20eletr%C3%B4nica%20ou%20pela

%20internet%E2%80%9D.>. Acesso em junho de 2022.

JESUS, Damásio de. **Parte especial: crimes contra a pessoa e crimes contra o patrimônio – arts. 121 a 183 do CP**. Direito penal vol. 2. 36. ed. São Paulo: Saraiva Educação, 2020.

LÉVY, Pierre. **Cibercultura**. (Trad. Carlos Irineu da Costa). São Paulo: Editora 34, 1999.

LINS, Emily Bezerra. **A investigação dos crimes cibernéticos em face do marco civil da internet**. Disponível em: <https://www.conteudojuridico.com.br/consulta/artigos/57707/a-investigao-dos-crimes-cibernticos-em-face-do-marco-civil-da-internet#:~:text=A%20investiga%C3%A7%C3%A3o%20dos%20crimes%20virtuais,fraudes%20banc%C3%A1rias%3B%20os%20crimes%20contra>. Acesso em junho de 2022.

LÓSSIO, Claudio Joel Brito; SANTOS, Coriolano Aurélio Almeida Camargo. Breve comentário sobre a Internet das Coisas à luz do Direito Penal Brasileiro. **De Fato e de Direito**: Revista Jurídica da Universidade do Sul de Santa Catarina, Ano IX, nº. 16, janeiro a julho, p. 16-24, 2018. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/UNISUL-Fato-Direito_n.16.pdf#page=16>. Acesso em março de 2022.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. Crimes virtuais: ciberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium**: estudos de direito, v. 1, n. 1, p. 2, 2018. Disponível em: <https://facdombosco.edu.br/wp-content/uploads/2018/12/%C3%82ngela-Tereza-Lucchesi-Erika-Fernanda-Tangerino-Hernandez-crimes-virtuais-Copia.pdf>. Acesso em março de 2022.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. 192 p.

MARTINS, Aislan Bruno da Silva. **Crimes virtuais**. 2017. 44 f. Monografia (Bacharelado em Direito) - Faculdade de Sabará/MG, 2017. Disponível em: <https://www.faculdadesabara.com.br/media/attachments/monografias/Monografia_Crimes-Virtuais_Aluno-Aislan.pdf> Acesso em março de 2022.

MARQUES, Karine da Silva; VILAR, Kaiana Coralina do Monte. **A Internet das Coisas e o Direito no Brasil: reflexos e desenvolvimento regulatório para a privacidade dos usuários**. Disponível em: <https://bdtcc.unipe.edu.br/wp-content/uploads/2019/09/TCC-Karine-da-Silva-Marques.pdf. Acesso em março de 2022.

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. **Crimes**

**cibernéticos: atipicidade dos delitos**. Disponível em: <https://joaoademar.com.br/3cbpj.pdf>. Acesso em março de 2022.

MULLER, Nicolas. **O começo da internet no Brasil**. Disponível em: <https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil>. Acesso em junho de 2022.

NADER, Paulo. **Introdução ao estudo do direito**. 36. ed. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 16. ed. Rio de Janeiro: Forense, 2020.

NUNES, Karine Lopes; COSTA, Larissa Aparecida. **O surgimento de um novo crime: estupro virtual**. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7739>. Acesso em março de 2022.

OLIVEIRA, Bruno Bastos de; PISSOLATO, Solange Teresinha Carvalho. Direito e tecnologia no ambiente de hiperconectividade: aspectos jurídicos da internet das coisas e seus desafios. **Relações Internacionais no Mundo Atual**, Curitiba, v. 1, n. 26, p. 223-241, janeiro/março, 2020. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/4076/371372384>. Acesso em março de 2022.

OLIVEIRA, Jorge Rubem Folena de. O direito como meio de controle social ou como instrumento de mudança social. **Revista de Informação Legislativa**, Brasília, a. 34, n. 136, p. 377-381, outubro/dezembro, 1997. Disponível em: <https://www2.senado.leg.br/bdsf/item/id/324>. Acesso em fevereiro de 2022.

ORACLE. **O que é IoT?** Disponível em: <https://www.oracle.com/br/internet-of-things/what-is-iot/>. Acesso em março de 2022.

PEREIRA, Patrick Alves et al. Internet das Coisas e suas aplicabilidades no dia a dia e no campo jurídico. **JNT - Facit Business and Technology Journal**, v. 1, n. 33, p. 55-58, janeiro, 2022. Disponível em: <https://jnt1.websiteseguro.com/index.php/JNT/article/view/1407/939>. Acesso em fevereiro de 2022.

PIRANI, Mateus Catalani et al. **O direito digital aplicado ao consumo sustentável: internet das coisas e sustentabilidade**. 2021. 301 f. Tese (Doutorado em Direito Ambiental Internacional) - Universidade Católica de Santos, Santos, 2021. Disponível em: < https://tede.unisantos.br/bitstream/tede/7643/1/Mateus%20Catalani%20Pirani.pdf>. Acesso em março de 2022.

SAKOVICH, Natallia. **What Is the Internet of Everything (IoE)?** Publicado em 16/02/2019. Disponível em: <https://www.sam-solutions.com/blog/what-is-internet-of-everything-ioe/>. Acesso em março de 2022.

SANTOS, Daniel Ivonesio. **Internet das Coisas, a prova do futuro: exame da legalidade do uso de dados coletados por dispositivos de internet das coisas, sem consentimento do usuário, como prova acusatória no processo penal brasileiro**. 2019. 65 f. Monografia (Bacharelado em Direito) - Universidade do Sul de Santa Catarina, Florianópolis, 2019. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7139/1/Monografia%20Daniel%20Ivonesio%20Santos.pdf. Acesso em março de 2022.

SILVA, Karine Marques da; VILAR, Kaiana Coralina do Monte. **A Internet das Coisas e o Direito no Brasil: reflexos e desenvolvimento**. Disponível em: <https://bdtcc.unipe.edu.br/wp-content/uploads/2019/09/TCC-Karine-da-Silva-Marques.pdf>. Acesso em fevereiro de 2022.

TANGERINO, Dayane Fanti. **O papel do Direito na Sociedade em Rede: Internet das Coisas (IoT)**. Publicado em 04/05/2018. Disponível em: <https://canalcienciascriminais.com.br/direito-internet-das-coisas-iot/>. Acesso em fevereiro de 2022.

## AGRADECIMENTOS

Imensamente a minha mãe Lúcia por ter priorizado a minha educação escolar, sobretudo na minha infância e pelo seu esforço empenhado para tal.

Ao meu eterno pai José Aderaldo (*in memoriam*) pelo seu carinho e apoio, sobretudo na minha adolescência e fase adulta, pelo exemplo de ser humano e por transmitir paz e ternura.

A minha esposa Maria das Dores pelo amor, companheirismo e apoio.

Ao meu irmão Valmir pelo companheirismo e força de sempre.

À Julieta Avelino ‘Pretinha’ pelo apoio dado, acolhendo-me em sua residência quando necessitei.

Aos meus sogros Jovelina (*in memoriam*) e Manoel Ângelo (*in memoriam*) pelo grande apoio ofertado.

Ao Excelentíssimo Abraão Falcão de Carvalho pelo apoio, amizade e por ser um exemplo de profissional do Direito e de ser humano ímpar.

Ao Hermes Sales pela amizade, ajuda no translado e por sua bondade imensurável.

Ao Roberto Rodrigues de Souza (*in memoriam*) pela ajuda constante de transporte durante boa parte deste curso e por ser um exemplo de ser humano.

Ao Joselito Menezes pelo apoio no translado, quase que diário, em parte considerável deste curso e pela amizade.

Ao meu cunhado Zezito Alves pela consideração e apoio sempre que possível de transporte ao meu trabalho e estudo.

Aos meus professores pelos ensinamentos transmitidos e experiências compartilhadas.

Aos colegas que conheci e firmei amizade durante o transcorrer deste curso.