CURSO DE BACHARELADO EM DIREITO

MARCIELE DOS SANTOS FERREIRA

CRIMES CIBERNÉTICOS:
EVOLUÇÃO E DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA

Apucarana
2022

MARCIELE DOS SANTOS FERREIRA

CRIMES CIBERNÉTICOS:
EVOLUÇÃO E DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Apucarana – FAP, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Profª Esp. Fernanda de Freitas Araújo.

Apucarana
2022

MARCIELE DOS SANTOS FERREIRA

CRIMES CIBERNÉTICOS:
EVOLUÇÃO E DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Apucarana – FAP, como requisito parcial à obtenção do título de Bacharel em Direito, com nota final igual a _____, conferida pela Banca Examinadora formada pelos professores:

COMISSÃO EXAMINADORA

Prof.ª Esp. Fernanda de Freitas Araújo
Faculdade de Apucarana

Prof. Rodolfo Motta.
Faculdade de Apucarana

Prof. Danylo Acioli.
Faculdade de Apucarana

Apucarana, 06 de dezembro, de 2022.

Dedico este trabalho aos meus familiares e amigos, que sempre me apoiaram no decorrer do curso, e a Deus pela oportunidade.

AGRADECIMENTOS

Agradeço, em primeiríssimo lugar, a Jesus e à Santíssima Virgem por me quererem onde estou, e por me darem forças para chegar até aqui. Os méritos são deles!

Agradeço a toda minha família, principalmente ao meu tio Ailton e a minha avó Delair, que sempre me apoiaram e foram meu alicerce, não permitindo que eu desistisse de enfrentar as dificuldades e perseguir meus sonhos.

Agradeço também a minha mãe, que faleceu no ano de 2010 e não pode estar fisicamente acompanhando essa nova etapa da minha vida, mas eu sei que lá do céu ela acompanha todas as minhas conquistas, e que deve estar orgulhosa, da sua única filha sendo a primeira da família a completar uma graduação.

Mesmo meu tio também não estando mais aqui, agradeço a ele por ser além de tio, meu pai, meu padrinho minha referência como pessoa, que sempre apoiou meus sonhos, e sempre me deu força, se não fosse por ele não estaria onde estou.

A minha avó agradeço por cuidar de mim desde bebe, sempre me educando, ensinando, por sempre estar comigo quando mais precisei, mesmo diante de todas as perdas e dificuldades que enfrentamos, continuamos firmes cuidando uma da outra.

Agradeço à minha orientadora Fernanda, por quem tenho grande carinho e estima, por sua ajuda e dedicação, por me apoiar desde o princípio na construção desse monologo, sempre me responder minhas dúvidas com maior carinho e atenção, sem ela, com certeza, seria muito mais difícil passar por essa etapa.

Agradeço a todos os professores que fizeram parte da minha formação acadêmica, especialmente, ao professor Coordenador Paulo Henrique Pavolak.

Agradeço à Instituição pela qualidade no ensino e pela excelência que desempenha na capacitação de profissionais.

“A verdade, porém, é que os maiores males e crimes são criados, arquitetados e executados em escritórios bem limpos, atapetados, refrigerados e bem iluminados por homens de colarinho branco, unhas bem cuidadas; estão sempre bem barbeados e jamais precisam elevar seu tom de voz”.

C. S. LEWIS

FERREIRA, Marciele dos Santos. **Crimes Cibernéticos: Evolução e Dificuldades na colheita de Elementos de Autoria Delitiva.** 82 p. Trabalho de Conclusão de Curso (Monografia). Curso de Bacharelado em Direito da Faculdade de Apucarana – FAP. Apucarana. Pr. 2022.

RESUMO

Com a globalização da internet e seu aumento no número de usuários, abriu-se espaço para os cybers criminosos agirem, de forma que os investigadores enfrentam dificuldades na hora de se colher e provar a autoria delitiva. Pesquisa-se sobre os Crimes Cibernéticos: Evolução e dificuldades na colheita de Elementos de Autoria Delitiva, a fim de apresentar a evolução da internet com o passar dos anos, e também tratar do crescimento dos crimes virtuais, e as dificuldades encontradas em relação a autoria desses delitos. Para tanto, é necessário saber que no início à internet era usada como um meio de espionagem e sabotagem em plena Guerra Fria, mas com o passar dos anos passou a ser um dos meios mais utilizados, para compra e venda, para anúncio e para a comunicação das pessoas ao redor do mundo inteiro, dessa forma como todo avanço tem seu lado positivo, também possui um lado negativo, sendo este, os indivíduos de má-fé, que se utilizam desse meio para praticarem delitos de diversas modalidades, ou seja, praticam os crimes cibernéticos, mesmo com o avanço em relação às leis que tratam desses delitos ainda existem grandes lacunas, seja em relação a obtenção das provas, seu tempo, local, e principalmente em relação a prova da autoria, onde está a maior dificuldade encontrada pelos investigadores para se provar o delito, visto que as provas podem ser alteradas, excluídas e até mesmo sumir. Realiza-se então uma pesquisa bibliográfica, onde será realizada uma coleta de dados a partir de artigos, livros, revistas e revistas virtuais, entre outros recursos que serão explorados. Diante disso, verifica-se que a internet passou de um meio para tirar vantagem de um país inimigo, para a maior rede que liga usuários do mundo inteiro, o que impõe a constatação de que se faz necessário a criação de um Código de Processo Penal Informático, para tratar desses delitos de forma clara, para que não haja mais lacunas, e que esses cybers criminosos realmente responsabilizados por seus delitos cometidos.

Palavras-chave: Crimes Cibernéticos. Evolução Histórica. Princípios Processuais Penais. Autoria Delitiva.

FERREIRA. Marciele dos Santos. Crimenes Cibernéticos. **Evolución y Dificultades en la Recolección de Elementos de Autoría Criminal.** 82 p. Realización del trabajo de curso (monografía). Licenciado en Derecho por la Facultad de Apucarana – FAP. Apucarana Pr. 2022

RESUMEN

Con la globalización de internet y su aumento en el número de usuarios, se ha abierto espacio para que los ciberdelincuentes actúen, de manera que los investigadores enfrentan dificultades para recolectar y probar la autoría criminal. Investigación sobre Delitos Cibernéticos: Evolución y dificultades en la recolección de Elementos de Autoría Criminal, con el fin de presentar la evolución de internet a lo largo de los años, y también para tratar el crecimiento de los delitos virtuales, y las dificultades encontradas en relación a la autoría. de estos delitos. Por ello, es necesario saber que en sus inicios se utilizó internet como medio de espionaje y sabotaje en plena Guerra Fría, pero con el paso de los años se ha convertido en uno de los medios más utilizados, para comprar y vender, para publicitar y para comunicarse con personas de todo el mundo, de esta manera, como todo avance tiene su lado positivo, también tiene su lado negativo, siendo esto, los particulares de mala fe, que utilizan este medio para cometer delitos de diversas modalidades, es decir, practican delitos cibernéticos, aun con el avance en relación a las leyes que atienden estos delitos aún existen grandes vacíos, ya sea en relación a la obtención de la prueba, su tiempo, lugar, y especialmente en relación a la prueba de autoría, donde es donde se encuentra la mayor dificultad que encuentran los investigadores para probar el delito, ya que la prueba puede ser alterada, excluida e incluso desaparecer. Luego se realiza una investigación bibliográfica, donde se recolectarán datos de artículos, libros, revistas y revistas virtuales, entre otros recursos que se explorarán. Ante esto, parece que internet ha pasado de ser un medio para aprovecharse de un país enemigo, a la red más grande que conecta a usuarios de todo el mundo, lo que impone la toma de conciencia de que es necesario crear un Código Procesal Penal. .computadora, para abordar estos delitos con claridad, para que no haya más lagunas, y que estos ciberdelincuentes realmente rindan cuentas por sus delito.

Palablas-clabe: Crímenes Cibernéticos. Evolución Histórica. Principios Procesales Penales. Autoría Criminal.

LISTA DE SIGLAS

ARPA Advanced Research Projects Agency

BO Boletim de Ocorrência

CDC Código de Defesa do Consumidor

CPP Código de Processo Penal

EUA Estados Unidos da América

FAPESP Fundação de Amparo à Pesquisa do Estado de São Paulo

INPI Instituto Nacional da Propriedade Industrial

IP Internet protocol

JF Justiça Federal

LGPD Lei Geral de Proteção de Dados

MP Ministério Público

NSF Network File System

RNP Rede Nacional de Ensino e Pesquisa

WWW World Wide Web

SUMÁRIO

1 INTRODUÇÃO..... 11

2 CRIMES CIBERNÉTICOS..... 12
2.1 Conceito..... 12
2.2 Classificação dos Crimes..... 13
2.2.1 Crimes cibernéticos próprios ou puros..... 13
2.2.2 Crimes Cibernéticos impróprios ou mistos..... 14
2.3 Evolução Histórica..... 15

3 PRINCÍPIOS CONSTITUCIONAIS NORTEADORES..... 21
3.1 Princípio da Legalidade..... 21
3.2 Princípio da Intervenção Mínima..... 23
3.3 Princípio do Estado de Inocência e da Culpabilidade..... 24

4 PRINCÍPIOS PENAIS NORTEADORES..... 26
4.1 Princípio da Responsabilidade Penal Subjetiva e Responsabilidade Penal da Pessoa Jurídica..... 26
4.2 Princípio da Insignificância da Bagatela..... 26
4.3 Princípio da Exclusiva Proteção dos Bens Jurídicos..... 27
4.4 Princípio da Ofensividade ou Lesividade..... 28

5 PRINCÍPIOS DO DIREITO PENAL INFORMÁTICO..... 29
5.1 Princípio da Dupla Presunção de Inocência..... 29
5.2 Princípio da Insignificância na Invasão de Dispositivo Informático..... 29
5.3 Princípio da Relativização dos Elementos Informáticos..... 30
5.4 Princípio da Sigilosidade Reflexa de Dados Armazenados..... 31

6 LEIS QUE REGEM OS CRIMES CIBERNÉTICOS..... 32
6.1 Lei Geral de Proteção de Dados..... 32
6.2 Harmonização entre a LGPD e a Lei de Acesso à Informação..... 34
6.3 Lei Carolina Dieckmann - Lei nº 12.737/2..... 35
6.4 Marco Civil da *Internet* - Lei nº 12.695/14..... 36
6.5 Convenção Europeia sobre os Crimes Cibernéticos – Convenção de Budapeste..38

6.6 Leis que tratam de Crimes Específicos.....40

7 PROVAS, AUTORIA E COMPETÊNCIA.....49
7.1 Dificuldade na Colheita de Provas.....49
7.2 Obtenção das Provas Digitais 57
7.3 Da Autoria dos Crimes.....60
7.4 Tempo, Local do Crime e Competência.....62
7.5 A Escassa Previsão Legal quanto a Prática de Cibercrimes Via *Internet*.....65

8 COMO EVITAR CAIR NOS CRIMES CIBERNÉTICOS.....66
8.1 Quais procedimentos tomar se sofreu Crime Cibernético.....69

9 CONCLUSAO.....71

REFERÊNCIAS.....73

1 INTRODUÇÃO

O presente trabalho analisa as questões relativas à prática dos crimes cibernéticos, sua evolução histórica, e as dificuldades encontradas na hora de se provar a autoria delitiva desses crimes.

Assim, inicialmente, no primeiro capítulo pesquisou-se o conceito de crimes cibernéticos e sua classificação.

Já o segundo capítulo trata de um breve histórico do surgimento e desenvolvimento da *internet*, que atualmente se transformou em uma importante ferramenta de compartilhamento de informações pessoais e comerciais, bem como é um grande espaço para a prática de atos ilícitos.

No capítulo terceiro apresenta os Principais Princípios Constitucionais que norteiam o Direito Penal.

Já no capítulo quarto, pesquisou-se os Princípios Penais Norteadores e no capítulo quinto pesquisou-se sobre os Princípios que regem o Direito Penal Informativo, sendo esses escassos.

O capítulo sexto trata das legislações que regem os crimes cibernéticos, com ênfase nas legislações brasileiras, como A Lei Geral de Proteção de Dados, a Harmonização entre a LGPD e a Lei de Acesso à Informação, a Lei Carolina Dieckmann – Lei nº 12.737/2, e o Marco Civil da *Internet* - Lei nº 12.695/14, por último a Convenção Europeia sobre os Crimes cibernéticos – Convenção de Budapeste.

O capítulo sétimo, expõe as dificuldades encontradas pelos investigadores em se colher e obter as provas digitais, pois essas provas podem ser alteradas, modificadas e excluídas, devendo assim ter um devido cuidado na sua colheita, também se discute a autoria desses crimes, o tempo, local e a competência, por último discute-se sobre a escassa previsão legal desses crimes.

Por fim, o oitavo capítulo, apresenta as formas de se evitar cair nesses crimes cibernéticos e quais procedimentos tomar caso caiam neles.

2 CRIMES CIBERNÉTICOS

2.1 Conceito

Atualmente não existe uma única nomenclatura que defina os crimes cibernéticos, e sim várias, podendo ser encontrados tanto na mídia como em textos técnicos.

Desta forma esses delitos podem ser denominados de Crimes Virtuais, Crimes Digitais, Crimes Computacionais dentre vários outros tipos, não havendo um consenso sobre a melhor denominação que relacionam os delitos com a tecnologia.[1]

Crimes cibernéticos possuem uma noção ampla, mas que inclui algumas ofensas criminais cometidas através das redes de computadores e, mais especificamente, através da *Internet*. Com o governo, indústrias, mercados e consumidores cada vez mais dependentes de conectividade, eles são propensos a uma série de ameaças.[2]

Já no conceito analítico, o crime informático, que também é uma espécie de delito cibernético é "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão".[3]

Dessa forma os crimes cibernéticos são as condutas típicas, antijurídicas e culpáveis contra ou praticadas com a utilização de instrumentos eletrônicos que podem entrar em rede, através da *internet*.[4]

Sabe-se então que o ato delitivo seria contra a máquina, o computador em si, ou seja, são os crimes cometidos contra os dados existentes no dispositivo, sendo este a destruição de software e dados, furto de informações, dentre outros são exemplos de alguns danos que o seu PC pode vir a sofrer.

Existe uma classificação que divide os crimes cibernéticos em dois tipos: os Crimes Cibernéticos Próprios e os Crimes Cibernéticos Impróprios. Os quais a seguir adentramos no assunto.

---

[1]SANTOS, Karl Heisenber Ferro. **Crimes Digitais**. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. p. 60. Acesso em: 22 jun. 2022.

[2]SILVA, Eduardo Soares da; BARAKAT, Najah Jamal Daakour. **Crimes Cibernéticos**, **Cyber Crimes**. [2013]. Disponível em: http://conpedi.danilolr.info/publicacoes/05sx3fe1/3z060c4n/N501YUJ08DF11b96.pdf. Acesso em: 28 jun. 2022.

[3]VELLOZO, Jean Pablo Barbosa. **Crimes Informáticos e Criminalidade Contemporânea.** [2015]. Disponível em: https://www.jurisway.org.br/v2/dhall.asp?id_dh=15756. Acesso em: 20 jun. 2022. p. 210.

[4]ALMEIDA, Jessica de Jesus. **Crimes cibernéticos**. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/download/2013/1217. Acesso em: 22 jun. 2022. p. 9.

2.2 Classificação dos Crimes

2.2.1 Crimes cibernéticos próprios ou puros

Os crimes cibernéticos próprios ou puros são os que nasceram através da informatização dos dados.

Dessa forma, os crimes cibernéticos próprios, são crimes específicos dessa seara, essa modalidade de crime exige conhecimentos técnicos especiais/avançados na área da computação e informação de dados, para que possam ser realizados.[5]

O ataque operado será contra o próprio sistema de dados, atingindo-o quanto à privacidade e inviolabilidade das informações, à acessibilidade e disponibilidade e à veracidade das mesmas, lesando de forma ampla a seguridade informática.[6]

Como leciona o mestre Damásio de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que são praticados por computador e se realizam ou se consumam 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.[7]

Os delitos cibernéticos puros são mais raros, na medida em que requerem, obrigatoriamente, o uso do sistema informático não apenas como meio para a realização do crime, mas como o próprio objeto material visado com a conduta delituosa.

Inevitavelmente, nessas ações ocorrerão agressões diretas ao software do computador da vítima, propiciando o acesso a dados não autorizados, bem como à senhas e documentos, permitindo a alteração, inclusão e destruição dessas informações.[8]

Dessa forma, essas condutas são praticadas pelos chamados "*hackers*"[9], que invadem, modificam/alteram ou inserem dados ou informações falsas, ou seja, são os casos que irão

---

[5]SILVA, Debora Cristina da. **Cibercriminalidade e a (in)suficiência legislativa pátria para a repressão dos crimes cometidos por meio da internet**. [2020]. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/218882/TCC%20-%20FINAL.pdf?sequence=1&isAllowed=y. Acesso em: 15 jun. 2022.

[6]*Ibidem*. p. 30.

[7]JOANONE, Bruno. **Crimes virtuais e a necessidade de uma legislação especifica**. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/49970/crimes-virtuais-e-a-necessidade-de-uma-legislacao-espeficica. Acesso em: 25 jun. 2022.

[8]SILVA, *op. cit*., p. 30.

[9]Hacker – no sentido original da palavra, um hacker é alguém que passa longas horas programando computadores para executar tarefas avançadas. No sentido mais comum, o termo passou a denominar a pessoa que tenta violar ou atacar sistemas. Outros termos comuns são violador, cracker e intruso. TORMEN, Chalidan Adonai Callegari. **Crimes Cibernéticos**: (IM)possibilidades de coerção. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4078.pdf. Acesso em: 31 jul. 2022.

atingir diretamente o softwares dos computadores, geralmente essa invasão de computadores acontece através do *pendrive, e-mails*, ou em forma de arquivos que são baixados em *sites* não confiáveis que contém "vírus"[10], a qual danifica diversos arquivos ou programas, chegando até em alguns casos ter de efetuar a formatação do computador em virtude do vírus.

2.2.2 Crimes Cibernéticos impróprios ou mistos

Os crimes virtuais impróprios, impuros ou virtuais comuns são os delitos comuns cometidos por meio de sistema de dados informatizados.

Nos cibercrimes, os meios digitais são utilizados como instrumento delitivo.[11]

O cometimento desses delitos não requer grandes conhecimentos técnicos especializados sobre computadores e infiltração de sistemas de dados juridicamente protegidos, nesses casos não é a inviolabilidade da informação automatizada de dados, senão bens jurídicos diversos, tradicionais, já tipificados para punir ações atentatórias realizadas cotidianamente. [12]

Com relação aos crimes cibernéticos impróprios, tem-se uma dificuldade em se reconhecer, pois não se consegue tipificar a informação armazenada como um bem material, mas sim um bem imaterial, insuscetível de apreensão como objeto.

Um exemplo desses crimes impróprios são os crimes de transferência de valores em contas bancárias, no qual os criminosos utilizam-se dos sistemas informáticos apenas como *animus operandi*, ou seja, furtando dinheiro da conta da vítima através de um sistema interligado a internet.

Conforme, Rita de Cássia Lopes da Silva explica:

> A informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio.[13]

---

[10]Vírus – trecho de um programa de computador que se reproduz embutindo-se em outros programas. Quando esses programas são executados, o vírus é ativado e pode se espalhar ainda mais. *Ibidem.*

[11]SILVA, 2020, p. 18.

[12]*Ibidem*, p. 19.

[13]SILVA, Rita de Cássia Lopes da. U**ma análise da lei de crimes cibernéticos no ordenamento jurídico brasileiro.** Faculdade da Cidade de Maceió Bacharelado em Direito Pedro Henrique Silva dos Santos. 2003. Disponível em: https://www.passeidireto.com/arquivo/102445430/analise-da-lei-de-crimes-ciberneticos. Acesso em: 25 jul. 2022.

Quando a conduta do agente se amolda aos tipos de crimes virtuais impuros, essa ação lesiona, por intermédio de um computador, outros bens jurídicos, diversos dos informáticos, visando atingir o resultado naturalístico pretendido.

De acordo com Damásio de Jesus:

> (...) 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.[14]

A maioria dos cibercrimes é impróprio, consistentes em realizar práticas ilícitas com o auxílio de um instrumento tecnológico, atingindo o meio jurídico já tipificado, praticando condutas já conhecidas, mas com *modos operandi* [15]completamente inovador, a exemplo disso temos o tráfico de drogas *online* e a promoção da pedofilia.[16]

Definindo assim os crimes próprios e impróprios, trataremos agora sobre a Evolução Histórica dos Crimes Cibernéticos.

2.3 Evolução Histórica

Neste subcapítulo, pesquisou-se sobre a evolução histórica da *internet*, e dos crimes cibernéticos com o passar dos anos.

Os Crimes Cibernéticos surgiram na década de 1960 durante a Guerra Fria em uma disputa entre os Estados Unidos da América e a União Soviética, que utilizava esse meio de comunicação para a espionagem e sabotagem, para garantir vantagens contra seus inimigos ou até mesmo vitórias.[17]

---

[14]JOANONE, 2022.

[15]Modus operandi é um termo utilizado no Direito Penal, o qual se refere a forma como o crime é praticado pelo agente, ou seja, o meio pelo qual ele determina seus atos para realizar a prática do crime e, consequentemente, a sua consumação. Deste modo, o modus operandi é a forma pela qual o crime é praticado pelo agente. BOLQUE, Elisa. **Modus operandi**. Disponível em: https://direito.legal/dicionario-juridico/modus-operandi-significado/. Acesso em: 25 jun. 2022.

[16]MESQUITA FILHO, Jose Pires. **Crimes Digitais**. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. Acesso em: 25 jun. 2022. p. 49.

[17]ALEXANDRE JUNIOR, Júlio Cesar. Cibercrimes: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso em: 25 jun. 2022.

Dessa forma, nota-se que inicialmente a internet surgiu com a finalidade de proteger os dados do governo americano, idealizando assim uma rede de troca e compartilhamento de informações criada pela empresa ARPA[18].

Em 1969, ocorreu o surgimento da rede ARPANET[19] (*Advanced Research Projects Agency*)[20]. Nesse período, a utilização da *internet* era restrita a áreas militares e universitárias.[21]

Somente ao final da década de 1970 e começo de 1980, com o surgimento da Rede Minitel da França a internet passou a ser utilizada no comércio.[22]

A primeira conexão internacional envolvendo a ARPANET ocorreu em 1973, ocasião em que Inglaterra e Noruega tiveram a oportunidade de se intercomunicar utilizando o novel sistema pela primeira vez.[23]

Foi durante a década de 80 que ocorreu o surgimento do padrão IP/TCP (Protocolo de *internet* e Protocolo de Controle de Transmissão[24]), onde permitia-se o tráfego de informações de uma rede para outra, proporcionando uma troca de mensagens entre todas as redes conectadas pelo endereço de IP na *internet*.

A partir desse momento, o IP passou a ser distribuído para diferentes equipamentos, onde poderiam ser interligados mesmo que produzidos por fabricantes diferentes.[25]

Nos anos 90 ainda houve a substituição da rede ARPANET pela rede NSF (*Network File System*), popularmente conhecida como "*internet*".

---

[18] Average Revenue per Account. Em livre tradução, ARPA significa **Receita Média por Conta**. Ou seja, trata-se de um indicador de desempenho que mostra quanto de receita cada conta ativa representa para o caixa da empresa, em média, a cada mês.

[19]ARPANET – rede, criada em 1969 pelo Departamento de Defesa dos Estados Unidos, que depois se tornou a Internet. SOUZA, Thiago. **História da Internet**: quem criou e quando surgiu. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 25 jul. 2022.

[20]VALVERDE, Danielle Novaes de Siqueira. Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE**, Recife, v. 15, n. 32, p. 236, jul./dez. 2010.

[21]T. FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira**. Almedina (Portugal): Grupo Almedina, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556271705/. Acesso em: 19 out. 2022.

[22]PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. [2000]. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2014;001018201. Acesso em: 25 jul. 2022.

[23]ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes do Direito**. Disponível em: https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/23590106.2017v4n2p191#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime. Acesso em: 27 ago. 2022.

[24]IP é um acrônimo para a expressão inglesa Internet Protocol (ou Protocolo de Internet), que é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados.

[25]ABDALLA, Samuel L.; GUESSE, André. **Informática para Concursos.** São Paulo: Saraiva, 2012. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502180642/. Acesso em: 25 set. 2022.

Durante a década de 1970, já era possível ouvir menções ao termo *hacker*.

Daniel Bell (1979) fez menção ao termo "sociedade da informação" no final dos anos 1970. "A informação é necessária para organizar e fazer funcionar tudo, desde a célula até a General Motors".[26] Em 1970, a IBM já realizava propagandas em torno da "sociedade da informação".

Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática.[27]

Ainda durante os anos 80 foram identificadas e divulgadas diversas ações criminosas com a utilização de meios virtuais, tais como pirataria de programas, manipulação de valores nos caixas eletrônicos, abuso de telecomunicação.[28]

Em 1995, os *sites* Tripod.com e Geocities permitiam que pessoas criassem suas próprias páginas pessoais na rede.

Nesse mesmo ano, o serviço TheGlobe.com disponibilizava salas de conversa *online* para seus utilizadores. Entretanto, foi apenas nos anos de 2003 e 2004 que as primeiras plataformas sociais com os modelos atuais surgiram, com o *MySpace* e o *Orkut*. Dessas, a plataforma *Orkut* tornou-se particularmente popular no Brasil, tendo os brasileiros como o seu maior público no mundo.[29]

Com o início da exploração mercadológica da internet, na década de 90, o físico e professor britânico, Tim Berners – Lee desenvolveu o serviço chamado *World Wide Web*, atualmente conhecido como "www", criando, assim, o que se denominou de rede de acesso.

E com certas melhorias em sua *interface* gráfica passou a ser mais acessível ao público de forma geral, tornando-se um meio de comunicação popular, iniciando-se um constante e veloz aperfeiçoamento da *internet* e das tecnologias de *software*.[30]

Após 30 anos, na década de 1991 as primeiras redes começaram a circular no Brasil, devido ao vínculo da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), com as instituições dos Estados Unidos, envolvendo o compartilhamento de informações.[31]

---

[26]BELL. **Índices para catálogo sistemático**: Informática e criminalidade: Direito penal. [1979]. Disponível em: https://docplayer.com.br/69154805-Isbn-indices-para-catalogo-sistematico-1-informatica-e-criminalidade-direito-penal-004-3.html. Acesso em: 25 jul. 2022. p. 169.

[27]JESUS, Damásio D.; MILAGRE, José A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 25 set. 2022.

[28]NASCIMENTO, Natalia Lucas do. **Crimes Cibernéticos**. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf. Acesso em: 19 out. 2022.

[29]T. FILHO, 2021.

[30]DIANA, Daniela. **História da internet**. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 10 ago. 2022.

[31]NASCIMENTO, *op. cit*.

Gerou-se assim um ciclo de mudanças frenético em toda a estrutura da *internet*, deixando de ser um sistema de acesso restrito às minorias, para se tornar o meio de comunicação mais utilizado pelas pessoas, sendo chamada de rede mundial de computadores[32].

Com a intensa prática desses delitos, foram surgindo as primeiras legislações que regulamentavam a prática desses atos ilícitos

A primeira iniciativa internacional sobre Cibercrime foi a Conferência sobre Aspectos Criminológicos do Crime Econômico, ocorrida no âmbito do Conselho da Europa, em 1976, em Estrasburgo.[33]

Entretanto, foi nas décadas de 1980 e 1990 que grande parte dos cibercrimes se propagou, já que a criptografia (meio utilizado para proteger dados digitais do mundo corporativo) se tornou objeto de atenção dos cibercriminoso.

Com todas essas mudanças e o aumento dos crimes, o Brasil chegou ao ranque número 1 de registros desta modalidade de crime, sendo seu *mods operant*, ou seja, o modo como é praticado e sofre mudanças todos os dias.

O Ministério da Ciência e Tecnologia do Brasil define a *internet* como um:

> Sistema de rede de computadores – uma rede de redes – que pode ser utilizado por qualquer pessoa em qualquer parte do mundo, onde haja um ponto de acesso, e que oferece um amplo leque de serviços básicos, tais como correio eletrônico, acesso livre ou autorizado a informações em diversos formatos digitais e transferência de arquivos.

Sendo assim os EUA também foram os pioneiros ao criarem legislações acerca desses crimes, no ano de 1988 editou-se a Lei Godfrain, já em 1995 a Espanha incluiu crimes de informática na reforma do seu Código Penal, e no ano de 2001 o Conselho da Europa, elaborou a Convenção Europeia de Crimes Cibernéticos com o objetivo de uniformizar a legislação europeia quanto à política criminal dos crimes cibernéticos.[34]

Em 1992 foi instituída a Rede Nacional de Ensino e Pesquisa (RNP), organização social ligada ao Ministério de Ciência, Tecnologia, Inovações e Comunicações do Governo Federal Brasileiro, a qual de fato moveu seus esforços no sentido de integrar a *internet* ao Brasil e fomentar sua difusão na sociedade.[35]

---

[32]VALVERDE, 2010, p. 236.

[33]BRASIL. Senado Federal. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em: 10 ago. 2022.

[34]NASCIMENTO, 2022, p. 17.

[35]RNP. Rede Nacional de Ensino e Pesquisa. **Nossa História**. Disponível em https://www.rnp.br/sobre/nossa-historia. Acesso em: 10 ago. 2022.

Em 1997, criou-se as "redes locais de conexão" expandindo, dessa forma, o acesso a todo território nacional.[36]

No Brasil inicialmente o tema em si, foi tratado no ano de 1987, com a lei nº 7.646/87 como uma questão de direito penal econômico, sua finalidade era a proteção à propriedade intelectual sobre programas de computador e sua comercialização no país, sua alteração ocorreu com a lei nº 8.137/1990, o qual define crimes praticados contra a ordem tributária.[37]

Assim, a *internet* passou a desempenhar um *status* significativo na sociedade em geral. Das relações interpessoais às negociais, passando pelas esferas do Governo, segurança pública, educação, saúde ou cultura, todas as ligações estabelecidas na sociedade atual passam, de alguma forma, pela informatização, sejam de dados ou da própria comunicação.[38]

Atualmente a *internet* desempenha um papel que ultrapassa seu objetivo principal de comunicação, e após o de entretenimento, passando a ser atualmente uma das plataformas mais eficientes impulsionando a economia mundial, com mecanismos disponíveis nesse espaço virtual, desde pequenos espaços virtuais até transações bilionárias de empresas multinacionais.[39]

São inegáveis os benefícios que a informatização trouxe para os Governos e para a sociedade em geral, nos seus mais diversificados aspectos existentes.

Contudo, em contrapartida, não se pode olvidar que esse meio de acesso volátil propiciou o aumento, e em certo grau o próprio surgimento, de uma série de crimes.

> [...] Apesar das facilidades e benefícios oferecidos pela internet, esse cenário também é propício para a prática de crimes. Cada vez mais, os criminosos se valem desse meio para praticar os mais variados tipos de crime. Pois, com o advento da internet, os crimes já tipificados pelo Código Penal passaram a ser praticados também no meio virtual, assim como, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio.[40]

Observamos também o grande aumento no teletrabalho, ou como chamamos atualmente de *Home Office*, após o surgimento da pandemia de Covid-19, estima-se que o percentual de empresas que adotaram o *home office* foi maior do que o do ramo de serviços hospitalares, sendo 53% em grandes empresas e 31% nas pequenas, os hospitais ficaram em 53% e as industrias em 47%, com base no estudo realizado pela Fundação Instituto de

[36]DIANA, 2022.
[37]NASCIMENTO, 2022, p. 17.
[38]SILVA, 2022, p. 10.
[39]*Ibidem*, p. 11.
[40]*Ibid*.

Administração (FIA) coletou em Abril de 2020, dados de 139 empresas de pequeno, médio e grande porte em todo o Brasil.[41]

Dessa forma, a *internet* passou a ser uma necessidade na vida das pessoas, seja em um *notebook, tablet* ou *smartphones*, sendo a frequência com que as pessoas se mantêm conectadas aumenta a cada dia, os aparelhos, principalmente o celular tornou-se essenciais e prevalentes na vida das pessoas, assim, com as facilidades que o ambiente virtual nos dá, sobretudo no anonimato, tornou essa ferramenta um meio propício para atos criminosos, tornando-se cabível elucidar quais são os impactos jurídicos dos crimes virtuais, e quais instrumentos legais podem ser considerados no julgamento dos mesmos.

Desse modo, os crimes cibernéticos tornaram-se comuns em decorrência da inexistência de entendimento público acerca dos seus impactos jurídicos e sociais.[42]

Portanto, um dos principais desafios atualmente é conseguir monitorar e reprimir a prática de condutas ilícitas via internet, regulamentando leis eficazes no combate a crimes cometidos sob a utilização da rede mundial de computadores.

[41]MELLO, Daniel. **Home Office foi adotado por 46% das empresas durante a pandemia**. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia#:~:text=O%20trabalho%20em%20casa%20foi,atuam%20em%20todo%20o%20Brasil. Acesso em: 10 ago. 2022.

[42]SANTANA, Roque Felipe da Silva**. Crimes Cibernéticos**: Análise Evolutiva da Legislação Penal Brasileira e seus Desafios. Disponível em: http://ri.ucsal.br:8080/jspui/bitstream/prefix/4456/1/TCCROQUESANTANA.pdf. Acesso em: 25 jul. 2022.

3 PRINCÍPIOS CONSTITUCIONAIS NORTEADORES

3.1 Princípio da Legalidade

Considera-se este princípio como um dos mais importantes, encontrado na Constituição Federal de 1988, disposto no artigo 5º, inciso XXXIX.

Está disposto também no artigo 1ºdo Código Penal Brasileiro "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal",[43]. Ao elaborar tal dispositivo, o legislador se inspirou na expressão "*nullum crimen, nulla poena sine praevia lege"* deveu-se a Feuerbach.[44]

Dessa forma, esse princípio trata-se da previsão de que não há infração penal se não houver previsão legal, levando assim a entender que o que não estiver descrito em lei como proibido, será permitido por lei.[45]

A origem deste princípio se dá na Carta Magna Inglesa, redigido em seu artigo 39.[46]

De acordo com Rogério Greco [47] o Princípio da Legalidade possui quatro funções: a Proibição da retroatividade da lei penal, a Proibição da criação de crimes e penas pelos costumes; a Proibição do emprego de analogia para criação de crimes e para fundamentar ou agravar penas; e também Proibir incriminações vagas e indeterminadas.

O Princípio da Reserva Legal e um Princípio derivado do Princípio da Legalidade pode ser denominado de "Estrita Legalidade", encontra-se disposto no artigo 5º, inciso XXXIX da Constituição Federal, seu surgimento se deu para delimitar e estabelecer algumas condutas, dessa forma quando falamos em crime, somente a lei poderá legislar sobre.[48]

---

[43]"Ninguém poderá ser condenado por atos ou omissões que, no momento em que foram cometidos, não constituam delito, de acordo com o direito aplicável. (1) Tampouco poder-se-á impor pena mais grave que a aplicável no momento da ocorrência do delito. Se depois de perpetrado o delito, a lei estipular a imposição de pena mais leve, o delinquente deverá dela beneficiar-se" (art. 9.º, Convenção Americana sobre Direitos Humanos).

[44]NUCCI, Guilherme de Souza. **Aplicação da Lei Penal Militar**: princípio de legalidade. Disponível em: http://genjuridico.com.br/2021/04/14/lei-penal-militar-legalidade/. Acesso em: 25 jul. 2022.

[45]NUCCI, Guilherme de S. **Princípios Constitucionais Penais e Processuais Penais**. 4. ed. São Paulo: Grupo GEN, 2015. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/978-85-309-6296-8/. Acesso em: 25 set. 2022.

[46]Art. 39. Nenhum homem livre será detido, nem preso, nem despojado de sua propriedade, de suas liberdades ou livres usos, nem posto fora da lei, nem exilado, nem perturbado de maneira alguma; e não poderemos, nem faremos pôr a mão sobre ele, a não ser em virtude de um juízo legal de seus pares e segundo as leis do País.

[47]GREGO, Rogerio. **Curso de Direito Penal**: Parte Geral. 18. ed. Niterói, RJ: Impetus, 2016. p. 96.

[48]PARDAL, Rodrigo. **Direito penal**: Princípios. Disponível em: file:///C:/Users/MARCIELE%20FERREIRA/Downloads/71683560-principios-e1656501927.pdf. Acesso em: 14 jul. 2022.

Dessa forma, não importa a reprovabilidade da conduta do agente, se não existir previamente uma lei definindo essa conduta como crime e apontando a sansão que corresponda ao delito cometido, este agente não poderá ser punido, será como se não houvesse cometido crime. [49]

É vedado ao legislador utilizar-se de decretos, medidas provisórias ou outras formas legislativas para incriminar condutas. Basta que uma conduta seja prevista como criminosa para que haja punição penal do infrator

O Princípio da Anterioridade e derivado do Princípio da Legalidade também, prevista no inciso XL, do artigo 5º da Constituição Federal, neste princípio a lei penal incriminadora deve ser anterior ao fato, veda-se assim a condenação do sujeito, sendo que no momento que ocorreu o fato ilícito, o mesmo não estava tipificado, e também prevê o agravamento da pena pela lei que entrou em vigor posteriormente ao delito.[50]

A exceção se dá no caso da retroatividade da lei penal, em favor do benefício do agente.

O Princípio da Taxatividade também é um derivado do Princípio da Legalidade, é vedada a criação de leis que contenham previsões e conceitos que sejam vagos, imprecisos e subjetivos os quais podem gerar punições injustas, a lei deve ser clara e precisa em seu texto, de forma que quem leia possa compreendê-la, dessa forma, a lei deve se taxativa[51].

A importância desse princípio está relacionada ao legislador, que durante a elaboração da lei penal, exige técnica na escrita, com uma linguagem correta e uniforme, restritiva e rigorosa, evitando que várias condutas delitivas se enquadrem naquela tipificação, até as que não correspondam a delito algum.

De se ressaltar que a criação de tipos penais com excesso de termos valorativos e com redação dúbia pode levar ao abuso do Estado na invasão da intimidade e da esfera de liberdade dos indivíduos.[52]

Dessa forma, vemos então que com toda mudança no mundo tecnológico vem acompanhada também da mudança cultural, e consequentemente o direito passa a ser influenciado por essas mudanças, tendo o dever de se adaptar à nova realidade social.

---

[49]MINTO, Rafael. **Saiba tudo sobre o princípio constitucional da reserva legal**. Disponível em: https://masterjuris.com.br/saiba-tudo-sobre-o-principio-constitucional-da-reserva-legal/. Acesso em: 16 jul. 2022.

[50]NUCCI, 2015, p. 186.

[51]*Ibidem*.

[52]GOMES, Genevieve Aline Zaffani Grablauskas. **Princípios do Direito Penal Brasileiro**. Disponível em: https://semanaacademica.org.br/system/files/artigos/principios_do_direito_penal_brasileiro.pdf. Acesso em: 25 jul. 2022.

.

Assim, como direito fundamental inerente aos cidadãos o princípio da legalidade, imperioso se faz lembrar que é de extrema importância que o legislador brasileiro se debruce sobre as novas ameaças decorrentes do processo de inovação tecnológica, visando criar normas penais e processuais que englobam toda a problemática relativa aos cibercrimes, não deixando lacunas sobre o tema.[53]

A legislação brasileira sobre essa temática é, em sua esmagadora maioria, inexistente. Quando existe, contudo, contém falta de técnica legislativa adequada, dando margem a interpretações dúbias, dificultando sua aplicabilidade.

Não se pode afirmar que a problemática está concentrada na falta de criação de tipos penais exclusivos aos crimes cibernéticos, pois, em sua excelência, o objeto material do crime virtual já é tutelado penalmente.

A dificuldade se concentra em normas relativas ao procedimento cabível para apuração desses crimes, que devem levar em conta as peculiaridades do meio pelo qual tais delitos foram praticados.

3.2 Princípio da Intervenção Mínima

Este Princípio terá sua aplicação nos casos em que houver extrema necessidade, sendo uma forma de intervenção mais extrema do Estado.

A atuação deste princípio acontecerá de forma subsidiária, ou seja, quando os outros ramos de direito não forem suficientes para resolver tal situação. Trata-se da garantia da autonomia e liberdade do indivíduo, atuando como um "*Ultima Ratio*", somente nos casos em que ocorrer ataques graves aos bens jurídicos mais importantes.[54]

O Princípio da Intervenção Mínima é estritamente ligado ao Princípio da Reserva Legal, de modo que um não vive sem o outro.

Assim, sinaliza Cezar Roberto Bitencourt [55]

> O princípio da intervenção mínima, também conhecido como ultima ratio, orienta e limita o poder incriminador do Estado, preconizando que a criminalização de uma conduta só se legitima se constituir meio necessário para a prevenção de ataques contra bens jurídicos importantes. Ademais, se outras formas de sanção ou outros meios de controle social revelarem-se suficientes para a tutela desse bem, a sua criminalização é inadequada e não recomendável. Assim, se para o restabelecimento da ordem jurídica violada

[53]SILVA, 2022.
[54]NUCCI, 2015, p. 214.
[55]BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte geral. 19. ed. São Paulo: Saraiva, 2013. v. 1. p. 54.

> forem suficientes medidas civis ou administrativas, são estas as que devem ser empregadas, e não as penais. Por isso, o Direito Penal deve ser a última ratio do sistema normativo, isto é, deve atuar somente quando os demais ramos do Direito se revelarem incapazes de dar a tutela devida a bens relevantes na vida do indivíduo e da própria sociedade.

De acordo com Capez, a subsidiariedade como característica do princípio da intervenção mínima, norteia a intervenção em abstrato do Direito Penal. Para intervir, o Direito Penal deve aguardar a "ineficácia" dos demais ramos do direito, isto é, quando os demais ramos se mostrarem incapazes de aplicar uma sanção à determinada conduta reprovável. É a sua atuação "*última ratio*".[56]

Isso se justifica porque a punição penal é muito severa. Se houver uma mais branda e que gere resultados positivos, a favor da sociedade, esta é a penalidade a ser aplicada.

O princípio da Fragmentariedade se dirige ao legislador e determina que o direito penal deve ser a última etapa de proteção, ou seja, uma conduta só deve ser descrita como criminosa quando os demais ramos do direito não conseguirem tutelá-la com eficácia.[57]

Dessa forma, este princípio atua quando outros ramos do direito não foram suficientes para proteção do bem jurídico.

3.3 Princípio do Estado de Inocência e da Culpabilidade

Está previsto no artigo 5º, LVII da Constituição Federal, "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória".

De acordo com Cesare Beccaria[58]:

> Um homem não pode ser considerado culpado antes da sentença do juiz; e a sociedade apenas lhe pode retirar a proteção pública depois que seja decidido que ele tenha violado as normas em que tal proteção lhe foi dada. Apenas o direito da força, pode, portanto, dar autoridade a um juiz para infligir uma pena a um cidadão quando ainda se está em dúvida se ele é inocente ou culpado.

Dessa forma cabe, portanto ao Estado, não somente promover a investigação, denúncia, processamento e julgamento do acusado, como também, aguardar o trânsito em

---

[56]BECCARIA, Cesare. **Dos delitos e das penas**. Tradução: Torrieri Guimarães. 2. ed. São Paulo: Martin Claret, 2008. p. 37.

[57]NUCCI, Guilherme de S. **Manual de Direito Penal**. São Paulo: Grupo GEN, 2021a. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993566/. Acesso em: 16 set. 2022.

julgado da condenação para a definitiva imputação da condição de culpado, para efeitos penais e extrapenais, ou seja, para que o Estado possa efetuar sua ação, é necessário que o agente tenha perdido sua condição de inocente.

O princípio da culpabilidade tem seu fundamento disposto no artigo 1º inciso III da Constituição Federal[59], está vinculado ao Princípio da Dignidade da Pessoa Humana, tem como objetivo proibir a incriminação do indivíduo sem que o mesmo tenha agido com culpa ou dolo, com a reforma da parte geral do código penal, no seu artigo 19 passou-se a exigir a comprovação do dolo e da culpa para que pudesse ocorrer a imputação da pena, devendo ocorrer assim de acordo com a concepção tripartite: um fato típico (ação ou omissão), ilícito e que tenha a culpabilidade (um juízo de reprovação social). [60]

A pena aplicada deve ser proporcional ao crime cometido, assim quando ocorrer aplicação considerada desproporcional da pena, passa a não ser mais uma imposição de castigo ao delito e sim uma maneira de alcançar outros objetivos ou intimidar terceiros, essa proporcionalidade da pena se relaciona com a individualização da pena.[61]

Dessa forma, se não houver dolo ou culpa do agente, não haverá conduta culpável, e consequentemente não haverá crime.

O próximo capitulo trata dos principais princípios constitucionais penais.

[59]Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
III - a dignidade da pessoa humana;

[60]FARIAS, Dermeval. **Direito Penal Parte Geral**: Princípios Penais e Jurisprudência do STF e STJ. Disponível em: file:///C:/Users/MARCIELE%20FERREIRA/Downloads/38021265-principios-penais-e-jurisprudencia-do-stf-e-stj.pdf. Acesso em: 15 jul. 2022.

[61]NUCCI, 2021a.

4 PRINCÍPIOS PENAIS NORTEADORES

4.1 Princípio da Responsabilidade Penal Subjetiva e Responsabilidade Penal da Pessoa Jurídica

O Princípio da Responsabilidade Penal subjetiva, também pode ser chamado de Primeira Acepção do Princípio da Culpabilidade.

Este princípio condiciona a responsabilidade penal a existência de dolo ou culpa da conduta, inclusive em crimes qualificados pelo resultado**.** Dessa forma não basta somente existir um nexo causal relevante deve também existir uma vontade de consciente da realização do crime, ou seja, um liame psicológico.[62]

Já a Responsabilidade Penal da Pessoa Jurídica reconheceu a possibilidade de processar uma pessoa jurídica, mesmo que não haja ação penal em curso contra pessoa física com relação ao crime, só é possível se estiver caracterizada ação humana individual. [63]

Sendo assim, as pessoas jurídicas serão responsabilizadas penalmente pelos crimes ambientais, não podendo ser responsabilizadas por crimes contra a saúde pública.

4.2 Princípio da Insignificância da Bagatela

Este Princípio da Insignificância da Bagatela decorre do Princípio da Fragmentariedade, sendo considerado um "instrumento de interpretação restritiva do Direito Penal".

Dessa forma, pode haver casos onde a ofensa será incapaz de atingir de forma concreta ou relevante bens juridicamente tutelados pelo Direito Penal, afastando assim a tipicidade do delito, excluindo o crime. [64]

Para que esse Princípio seja utilizado, devemos observar quatro requisitos básicos:

---

[62]COSTA, Fernando José da; COSTA JÚNIOR, Paulo José da. **Código penal comentado**. São Paulo: Saraiva, 2011. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502133914/. Acesso em: 24 out. 2022.

[63]SANTORO FILHO, Antônio Carlos. **Princípio da Responsabilidade Penal Subjetiva e Responsabilidade Penal da Pessoa Jurídica**. Disponível em: https://www.sedep.com.br/artigos/responsabilidade-penal-da-pessoa-juridica-e-principio-da-responsabilidade-pessoal/#:~:text=O%20princ%C3%ADpio%20da%20responsabilidade%20pessoal,conduta%20apenas%20em%20virtude%20do. Acesso em: 20 ago. 2022.

[64]GOMES, Caio. **Princípios do Direito Penal**: resumo e jurisprudência. Disponível em: https://www.direcaoconcursos.com.br/artigos/principios-do-direito-penal-resumo-e-jurisprudencia/. Acesso em 20 ago. 2022.

1- Mínima ofensividade da conduta;

2- Ausência de periculosidade da conduta;

3- Reduzido (reduzidíssimo) grau de reprovabilidade;

4- Inexpressividade da lesão/dano.

4.3 Princípio da Exclusiva Proteção dos Bens Jurídicos

Trata-se da mera intenção do agente em cometer tal delito, ou seja, o indivíduo pensa em cometer tal crime, mas não o faz, não o comete, tratando-se assim de uma mera cogitação pessoal.

De acordo com este Princípio somente o bem jurídico relevante será protegido pelo Direito Penal.[65]

Isso significa que o direito não pode punir formas de existência e suas expressões, devendo reconhecer no indivíduo sua autodeterminação (âmbito de autonomia moral), daí que não deveria incriminar situações que interditem liberdades constitucionais como:[66]

a) No discutido caso do uso de drogas, onde haveria apenas autolesão (ofensa a própria saúde);

b) Em casos em que haja consentimento do ofendido, ou seja, em que embora objetivamente tenha havido uma lesão, o lesionado tenha anuído expressamente (intervenções cirúrgicas, por exemplo);

c) Pensamentos e suas expressões, garantindo a liberdade de expressão e informação contra a censura;

d) Manifestação política, como a criminalização da greve em tempos passados;

e) Expressões socioculturais de minoria

[65]SILVA, Douglas. **Princípio da Exclusiva proteção do Bem Jurídico.** Disponível em: https://djus.com.br/principio-da-exclusiva-protecao-do-bem-juridico-dp80/#:~:text=Princ%C3%ADpio%20da%20exclusiva%20prote%C3%A7%C3%A3o%20do%20bem%20jur%C3%ADdico%3A,ser%C3%A1%20protegido%20pelo%20direito%20penal. Acesso em: 20 ago. 2022.

[66]LUZ, Josuel Pedroso da. **Princípio da exclusiva proteção de bens jurídicos**: como se proteger do direito penal ou quem vigia o vigia? Disponível em: https://jornaltribuna.com.br/2022/07/principio-da-exclusiva-protecao-de-bens-juridicos-como-se-proteger-do-direito-penal-ou-quem-vigia-o-vigia/. Acesso em: 20 ago. 2022.

4.4 Princípio da Ofensividade ou Lesividade

Este Princípio proíbe a incriminação de uma atitude interna, ou seja, de uma conduta que não exceda o âmbito do próprio agente, dessa forma não há crime se a conduta não é capaz de causar lesão ou no mínimo perigo de lesão ao bem jurídico.

O Direito Penal não se ocupa com questões políticas, étnicas, morais, religiosas e filosóficas. [67]

Para Claus Roxin "um conceito de bem jurídico vinculante político-criminalmente só pode derivar dos valores garantidos na lei fundamental, do nosso Estado de Direito baseado na liberdade do indivíduo, através dos quais são marcados os limites da atividade punitiva do Estado".[68]

Este Princípio funciona como fator de legitimação, quando protege os bens intitulados pela Constituição Federal.

[67]SANTOS, Rafael Baltazar Gomes dos. **Princípio da lesividade (ou ofensividade).** Disponível em: http://www.blogladodireito.com.br/2016/05/principio-da-lesividade-ou-ofensividade.html#.yzyixhbmjpy. Acesso em: 20 ago. 2022.

[68]RESUMO de Direito Penal: Princípio da lesividade ou da ofensividade. Disponível em: https://www.questoesestrategicas.com.br/resumos/ver/principio-da-lesividade-ou-da-ofensividade#:~:text=Para%20Claus%20Roxin%20%E2%80%9Cum%20conceito,da%20atividade%20punitiva%20do%20Estado%E2%80%9D. Acesso em: 21 ago. 2022.

5 PRINCÍPIOS DO DIREITO PENAL INFORMÁTICO

5.1 Princípio da Dupla Presunção de Inocência

Está previsto no art. 5º, LVII da Constituição de 1988, que nos diz o seguinte: "ninguém será considerado culpado até trânsito em julgado de sentença penal condenatória".

Desse modo, o acusado será tratado como inocente desde o início do processo até o trânsito em julgado onde com a sentença será admitida sua inocência diante do fato, ou sua culpa. Quem deve provar a culpabilidade do crime cometido é o acusador, não se admitindo que recaia sobre o indivíduo acusado o ônus de "provar a sua inocência".[69]

Deste princípio, derivam duas regras fundamentais: a regra probatória, ou de juízo, a qual trata do ônus da prova do direito penal; e, a regra de tratamento, segundo a qual ninguém será considerado culpado antes do trânsito em julgado da sentença, o que impede a antecipação de qualquer juízo condenatório ou de culpabilidade.[70]

Dessa forma, dependendo do crime cometido o agente será considerado inocente até que se possa provar o contrário.

5.2 Princípio da Insignificância na Invasão de Dispositivo Informático

A doutrina admite a teoria do direito penal mínimo, onde o princípio da insignificância em determinados delitos informáticos, onde somente os bens que possuem maior relevância deveriam ser protegidos.

Assim, temos os delitos de lesão mínima, onde o direito penal somente irá intervir em casos que haja certa gravidade, reconhecendo a atipicidade do fato nas hipóteses de perturbações jurídicas de pequena relevância.[71]

Este princípio tem sido aplicado em casos de furtos de objetos que possuem material insignificante, lesão insignificante ao fisco, maus tratos de importância mínima, descaminho e

---

[69]NOVO, Benigno Nunez. **O princípio da presunção de inocência**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-171/o-principio-da-presuncao-da-inocencia/. Acesso em: 16 de agosto de 2022.

[70]CAVALCANTE, Gercina Alves Moraes. **A relativização do princípio da presunção de inocência frente ao cumprimento antecipado da pena**: análise jurisprudencial. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/22546/1/INACIO%20E%20RENATO%20dep%C3%B3sito.pdf. Acesso em: 08 set. 2022.

[71]JESUS; MILAGRE, 2016.

dano de pequena monta, lesão corporal de extrema singeleza, se aplicando também a alguns delitos informáticos, onde o juiz irá apontar a questão da violação jurídica.[72]

Atualmente tudo pode ser considerado dado eletrônico, mas nem todo dado eletrônico será considerado relevante a ponto de incidir uma pena sobre aquele que teve a intenção ou que conseguiu obtê-lo, dessa forma um indivíduo que invade uma rede para alterar informações, não será punido da mesma forma que um cidadão que acessou um site de vendas a fim de clonar os dados dos cartões dos usuários. [73]

Há, em outro cenário, de se cogitar em princípio da insignificância nos casos do § 2º do art. 154-A do Código Penal, que prevê uma causa de aumento quando da invasão ocorre prejuízo econômico. Se o prejuízo for insignificante, não haverá que se cogitar da aplicação da causa de aumento[74]. Mas o crime simples subsiste.[75]

Assim podemos considerar necessário este princípio, pois será onde a autonomia e liberdade do indivíduo só seriam retiradas se realmente fosse necessário, ainda que a lei não faça a distinção entre a relevância de 'dados' que o agente precisaria obter para ser preso, caberá assim ao juiz no caso concreto.

5.3 Princípio da Relativização dos Elementos Informáticos

Tem como objetivo identificar o caráter *iuris tantum* dos elementos informáticos, ou seja, o caráter da presunção relativa de veracidade, levando ao operador de direito a ideia de que o conteúdo daquele elemento tanto investigativo ou probatório, pode ser questionado no que tange a sua capacidade de demonstrar um fato. Em contraposição, a doutrina apresenta o conceito de veracidade *iuris et de iure* como sendo aquela que goza de presunção absoluta, no

[72]JESUS; MILAGRE, 2016.
[73]*Ibidem*.
[74]**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.
[75]JESUS; MILAGRE, *op. cit.*, p. 51.

sentido de que sua capacidade de demonstrar um fato é irrefutável ou não admite prova em contrário.[76]

Dessa forma, caso haja a impossibilidade do comprimento do encargo, ou se for mais simples a obtenção da prova ao contrário.

5.4 Princípio da Sigilosidade Reflexa de Dados Armazenados

Este Princípio busca demonstrar que sempre que os fins da ferramenta ou do sistema informáticos forem utilizados além das expectativas razoáveis, não se pode utilizar o comportamento registrado pelo usuário ou os dados por ele criados em prejuízo dele próprio.

Pois, obrigado o titular da ferramenta ou o controlador do sistema a manter sigilo sobre todos os dados ali armazenados sob pena de considerar-se que o usuário fez prova contra si inconscientemente.[77]

Dessa forma, a Lei Marco Civil da *Internet* Brasileira - a Lei n. 12.965/2014 -, bem como a Lei Geral de Proteção de Dados - Lei n. 13.709/18 - as empresas provedoras de serviços e aplicações de internet não podem efetuar a guarda de dados excessivos à finalidade consentida pelo titular e, portanto, a fortiori, a entrega de dados aquém do permitido pela legislação configura violação à Sigilosidade de modo a gerar nulidade da prova obtida.[78] Esta Sigilosidade dos dados é uma hipótese trazida pela CF/88.

---

[76]SYDOW, Spencer Toth. **Da necessária relativização do elemento informático perante o princípio da manipulação**. [2022a]. Disponível em: https://s3.meusitejuridico.com.br/2019/08/7913457e-relativizacao-elemento-informatico-principio-manipulabilidade.pdf. Acesso em: 07 set. 2022. p. 16.

[77]SYDOW, Spencer Toth. **A importância do RHC No 99.735 – SC para o Direito Penal Informático**. [2022b]. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/06/26/importancia-rhc-no-99-735-sc-para-o-direito-penal-informatico/. Acesso em: 08 set. 2022.

[78]SYDOW, *op. cit.*

6 LEIS QUE REGEM OS CRIMES CIBERNÉTICOS

6.1 Lei Geral de Proteção de Dados

A Lei 13.7093 de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), entrou em vigor no dia 18 de setembro de 2020, com aplicação de sanções administrativas apenas a partir de 01 de agosto de 2021, em virtude da aprovação da Lei n. 14.010/20, que prorrogou o prazo inicialmente previsto, por conta da pandemia do Coronavírus (Covid-19) desta forma, toda pessoa natural ou pessoa jurídica de direito público ou privado, que incorra na realização de tratamento de dados pessoais deve estar em conformidade com a LGPD.

Para compreender a relevância que os programas de *compliance*[79] assumem na tutela da proteção dos dados pessoais e no direcionamento dos agentes de tratamento a respeito das condutas necessárias para atender aos preceitos legais, bem como determinar as linhas gerais que devem ser observadas no que se refere à LGPD, afigura-se fundamental determinar o que se entende por *compliance*, suas funções e o conteúdo de tais programas.[80]

A LGPD aprimora o conceito de proteção de dados pessoais, passando a ser um direito fundamental, porém deve ser realizada de maneira eficiente e eficaz, traduzindo-se em uma forma de estreitar o vínculo com o cidadão, que acredita que suas informações estão seguras e sendo utilizadas de maneira apropriada, obedecendo ao princípio constitucional da inviolabilidade à privacidade, previsto na Carta Magna, em seu art. 5º, inciso X[81].[82]

E necessário que as organizações entendam o que e estar em *"compliance"* com a LGPD, exigindo assim, entre outros aspectos, a adequação dos processos organizacionais existentes, demandando, algumas vezes investimentos em consultoria especializada, em capacitação pessoal, ferramenta de segurança no mapeamento de dados [83] (data *mapping*), na

[79]Com origem no verbo inglês **"to comply",** que quer dizer cumprir, obedecer, estar de acordo, define-se **Compliance** como seguir as leis, normas e procedimentos internos das organizações, além de parcerias éticas, seja com o setor público ou privado e seus fornecedores.

[80]TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais.** [*S.l.*]: [*s.n.*], 2019. p. 683.

[81] 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;

[82]SANTOS FILHO, Antônio Leite dos. **Cartilha Lei Geral de Proteção de Dados Pessoais 2021 – LGPD**. Disponível em: https://www.gov.br/dnit/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-lgpd/cartilha_lgpd_2021.pdf. Acesso em: 21 ago. 2022.

[83]Mapeamento de Dados: documento essencial quando da execução do processo de adequação às normas de proteção de dados. O mapeamento deve refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita.

melhoria de procedimentos e nos fluxos internos e externos acerca de dados pessoais, bem como, na implementação de uma cultura organizacional voltada para a segurança da informação e privacidade.

A 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.[84]

A LGPD traz claramente quais são os fundamentos relacionados à proteção de dados pessoais, que servem para embasar toda e qualquer ação que envolva seu tratamento. Sendo eles:[85]Inviolabilidade da intimidade, da honra da imagem, Autodeterminação informativa, Desenvolvimento econômico e tecnológico e inovação; Respeito à privacidade; Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais; Livre iniciativa, livre concorrência e defesa do consumidor; e Liberdade de expressão, de informação, de comunicação, e de opinião**.**

Sendo assim, toda organização deve buscar a conformidade legal, e neste caso, se manter atualizada quanto às legislações, normas e padrões de segurança aplicáveis à privacidade e proteção de dados.

Em caso de desconformidade, há possibilidade de responsabilização para muito além das infrações relacionadas exclusivamente à Lei Geral de Proteção de Dados Pessoais.

Portanto, organizações públicas e privadas, servidores públicos e funcionários devem conhecer suas responsabilidades e atribuições legais inerentes a esse ambiente de alta criticidade ao qual estão inseridos.

Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade pública e o interesse público para a realização de tratamento dos dados [86].

Insta salientar que, conforme o art. 7º da LGPD, a Administração Pública pode tratar dados mediante base legal específica (inciso III), não dependendo de consentimento ou

[84]CONAB. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.conab.gov.br/lei-geral-de-protecao-de-dados-pessoais. Acesso em: 20 ago. 2022.
[85]SANTOS FILHO, 2022.
[86]PINHEIRO, Patrícia Pack. **Proteção de Dados Pessoais:** Comentários à Lei 13.709/2018. [*S.l.*]: [*s.n.*], [20--].

enquadramento em outras hipóteses, exceto se mais específica, como é o caso da tutela à saúde.[87]

O Eventual compartilhamento de informações pessoais de interesse público deve ser expressamente autorizado por lei, com base nos critérios da necessidade, proporcionalidade e adequação, de modo a não tornar o direito fundamental à privacidade inócuo.

6.2 Harmonização entre a LGPD e a Lei de Acesso à Informação

A Lei de Acesso à Informação entrou em vigor em maio de 2012, sendo considerada um marco muito importante para a Administração Pública brasileira, essa lei regulamentou as informações que são manuseadas pelo poder público.

Ambas as leis LGPD e LAI inspiram-se no valor da transparência pública, que permite ao indivíduo, pessoa física, exercer a defesa de seus direitos e garantias fundamentais contra o Estado (negativamente), além de ter controle efetivo sobre atividade pública (positivamente), para contrariar o desequilíbrio de poder em relação ao indivíduo que está presente na relação entre o cidadão e o Estado.[88]

A Lei de Acesso à Informação guarda similitudes e divergências com a Lei Geral de Proteção de Dados Pessoais. Cada qual possui diversos fundamentos e matrizes sobre as quais se estruturam.

No entanto, esta última acrescenta pontos essenciais, não regulados pela primeira. Ainda que seja relevante a garantia da transparência, igualmente importante é a tutela dos dados pessoais – principalmente em um cenário globalizado, em que os dados pessoais se tornaram importantes elementos comerciais.

Faz-se, portanto, que se observe a difícil tarefa do Poder Público em se aplicar a harmonização entre os institutos, de acordo com o caso concreto, sem comprometer os preceitos basilares de ambos, quais sejam o direito à informação e o direito à privacidade.[89]

Dessa forma, a busca por conformidade à Lei Geral de Proteção de Dados Pessoais, como vimos, é sem dúvida um grande desafio para as organizações, em especial para o Poder

[87]COTS, Márcio; OLIVEIRA. Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. [*S.l.*]: [*s.n.*], [20--]. p. 145.
[88]HAJE, Lara. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas.** Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/. Acesso em: 20 ago. 2022.
[89]T. FILHO, 2021.

Público, que via de regra, detém grande volume de dados pessoais sob sua custódia e é inerente a suas atividades o tratamento de dados.

6.3 Lei Carolina Dieckmann – Lei nº 12.737/2

Ao abordar os crimes cibernéticos, comenta-se o nome da Carolina Dieckman, que no dia 03 de dezembro de 2012 foi publicada pelo Diário Oficial da União, ao qual foi sancionada pela ex Presidente da República Dilma Rousseff, a Lei 12.737/12 que veio dispor a tipificação criminal para os crimes cibernéticos, ganhou essa nomenclatura pelo fato da atriz em maio de 2011, ter seu computador invadido por *hackers*, que subtraíram fotos íntimas e as divulgaram na *internet*.

A Lei Carolina Dieckmann e composta de dois artigos que foram incluídos no Código Penal de 1940.[90]

O artigo 154 trata-se de quando o criminoso invade um dispositivo por meio fraudulento, rompendo mecanismos de segurança e praticando delitos, seus parágrafos 1. 2 e 3 nos traz a modalidade de atenuantes quando a invasão resulta prejuízo econômico, ou que o mesmo obtenha informações sigilosas, ou comunicações privadas, sendo a pena aumentada até 2 terços se o conteúdo for comercializado ou transmitido a terceiros.[91]

---

[90]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.
§ 3 o 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 obtidas.
§ 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.

[91]BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502209428/. Acesso em: 24 ago. 2022. p. 24.

Quando o crime for ocorrido contra Presidente da República, governadores e prefeitos, bem como autoridades públicas, a pena é aumentada de 1 terço a 50% nas atenuantes da dosimetria da pena.[92]

Assim, no artigo 154 – B, irá tratar-se do funcionalismo da Ação Penal, que somente é procedida perante representação, tendo a exceção quando o crime for contra administração pública direta ou indireta, independente dos poderes do Estado.[93]

No seu artigo 266 [94] estabelece regulamentação sobre quem pratica o crime impedindo ou dificultando informações de utilidade pública, e de quem usa dos dados para falsificação de documentos.

6.4 Marco Civil da *Internet* - Lei nº 12.695/14

O Marco Civil da *Internet* foi criado através de uma incorporação de vários projetos similares, que ganharam força principalmente pelas descobertas de espionagem do Governo Norte Americano contra o Brasil e outros países.

Assim, no dia 23/04/2014 a Lei n. º 12.695/2014 foi sancionada pela então presidente Dilma Rousseff, o qual estabelece princípios, garantias, deveres e direitos aos usuários da internet.[95]

O grande objetivo da Lei 12.965/2014 é garantir a defesa dos consumidores que usam a *internet* para adquirir produtos ou serviços, pois regula a comercialização das empresas que utilizam da *internet* como meio de comércio, assegurando a livre iniciativa, bem como a livre concorrência. Regendo também os serviços que são prestados pelas multinacionais provedoras de *Internet*. O artigo segundo do Marco Civil da *internet*, foi sancionado para disciplinar o uso de *internet* no Brasil, trazendo como fundamento principal a liberdade de expressão.

---

[92]Ação penal Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for 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. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

[93]BRITO, 2013, p. 25.

[94]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 for cometido por ocasião de calamidade pública. ” (NR)
Falsificação de documento particular.

[95]SENADO NOTÍCIAS. **Sancionada a Lei do Marco Civil da Internet**. Disponível em: https://www12.senado.leg.br/noticias/materias/2014/04/23/sancionada-a-lei-do-marco-civil-da-internet. Acesso em: 25 ago. 2022.

O capítulo I, do referido dispositivo legal, dispõe sobre conceitos, princípios, direitos e deveres para a utilização da *internet* a nível nacional, bem como estipula diretrizes para a atuação do poder público em relação à matéria.[96]

O artigo terceiro [97] veio no viés intencional do artigo segundo, trazendo consigo alguns princípios, como proteção da privacidade, proteção de dados pessoais, preservação de rede, com padrões internacionais, e responsabilização dos agentes em conformidade com a lei.[98]

O artigo quarto[99] teve como objetivo a promoção do direito à acesso de internet para todos, prezando também o acesso à informação ampliando, e fomentando as novas tecnologias, fazendo com que as pessoas aderissem a novos estilos de pesquisa.[100]

[96]JESUS, Damásio Evangelista D.; OLIVEIRA, José Antônio M.; MILAGRE, D. **Marco Civil da Internet**: comentários à Lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 25 ago. 2022.

[97]Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - Proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação E garantia da neutralidade de rede;
V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte

[98]JESUS; OLIVEIRA; MILAGRE, *op. cit*., p. 21.

[99]Art. 4o A disciplina do uso da internet no Brasil tem por objetivo a promoção:
I - Do direito de acesso à internet a todos; 24
II - Do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV - Da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados

[100]JESUS; OLIVEIRA; MILAGRE, *op. cit*., p. 24.

O artigo quinto[101] veio para determinar os efeitos da Lei, estabelecendo fundamentos sobre *internet*, terminal, endereço de protocolo, conexão e registros de aplicações de *internet*.[102]

Já o artigo sexto delimitou que a legislação além de se utilizar de seus fundamentos, princípios e objetivos previstos, pode se fazer uso de costumes e importância dos particulares. Abrangendo o contexto legislativo.[103]

No capítulo II, dispõe sobre direitos e garantias dos usuários, estabelecendo proteção à intimidade e a vida privada dos usuários, além de assegurá-los o direito de informações claras e precisas quanto às políticas de uso dos *sites*, provedores e redes sociais.[104]

O capítulo III estabelece a provisão de conexão e de aplicações de *internet*, onde define inúmeras normas. A neutralidade da rede é uma das diretrizes que foram estabelecidas neste capítulo, sendo que esta é de fundamental importância, pois institui ao responsável pela transmissão, comutação ou roteamento da obrigação de tratar de forma isonômica quaisquer pacote de dados, sem distinção pela sua origem, destino, conteúdo, serviço, terminal ou aplicação.[105]

Por outro lado, o capítulo IV, aborda diretrizes para a atuação dos entes públicos no desenvolvimento da *internet* no Brasil.[106]

Por fim, o capítulo V dispõe sobre disposições finais estabelecendo a liberdade de escolha do usuário na utilização de programa de computador, além de estimular a defesa dos seus interesses e direitos estabelecidos na presente Lei no âmbito administrativo e judicial.[107]

---

[101]Art. 5o Para os efeitos desta Lei, considera-se:
I - Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
II - Terminal: o computador ou qualquer dispositivo que se conecte à internet;
III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
IV - Administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
V - Conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
VI - Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[102]JESUS; OLIVEIRA; MILAGRE, 2014, p. 26.

[103]*Ibidem*, p. 29.

[104]*Ibid*., p. 31.

[105]*Ibid*.

[106]*Ibid*., p. 75.

[107]*Ibid*., p. 81-82.

Dessa forma esses direitos poderão ser exercidos de forma individual ou coletivamente na forma da lei.

6.5 Convenção Europeia sobre os Crimes Cibernéticos – Convenção de Budapeste

A Convenção de Budapeste, foi elaborada no dia 23/11/2001 pelo Conselho da Europa, sendo um órgão internacional e intergovernamental que engloba 45 estados membros, incluindo a União Europeia, foi o primeiro tratado internacional que trouxe legislações competentes para a modalidade dos cibercrimes.

Esta lei entrou em vigor em 01 de julho de 2004, abrangido tanto o Direito Penal como o Direito Processual Penal, definindo as formas de crimes cibernéticos e suas formar de persecução, ou seja, essa convenção trata-se basicamente sobre as violações do direito autoral, fraudes relacionadas com o acesso da *internet* pelo computador, pornografia infantil e violações de segurança de rede.[108]

Como essa convenção teve origem no Conselho Europeu, o Brasil não participou desta forma, não seguimos esse tratado, os EUA foi o único país que não pertence à Europa que ratificou o tratado em 2006.

O primeiro capítulo nos traz terminologias, definindo assim, termos como "sistema de computador" (*computer system*), provedor de serviços, (*servisse provedor*), entre outros, seu objetivo é uniformizar tais definições.

Nos capítulos seguintes estão previstas as medidas a serem tomadas no âmbito das legislações nacionais, estabelecendo leis penais, normas processuais e investigativas, criminalizando também determinadas condutas.

O título I da Convenção determina quais infrações devem ser definidas a nível nacional aos países signatários contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos.[109]

Já o título II, dispõe sobre infrações relacionadas a computadores, tais como a falsidade e burla informática, as quais correspondem respectivamente a introdução, modificação e eliminação de dados informáticos.

---

[108]FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil**. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil. Acesso em: 21 ago. 2022.

[109]JESUS; MILAGRE, 2016.

No título III, institui algumas infrações, porém, em especial a regulamentação da pornografia infantil.

Por outro lado, o Título IV, aborda infrações relacionadas à violação a direito de autor e direitos conexos. [110]

Por fim, no Título V, faz referência às formas de responsabilidade e sanção, abordando temas de ordem processual como, por exemplo, a busca e a apreensão de dados armazenados em sistemas informáticos, além de dispor sobre a obrigação do fornecedor de serviços registrar todas as informações, bem como transmiti-las para as autoridades competentes quando solicitadas.

6.6 Leis que tratam de Crimes Específicos

Projeto de Lei 8.045/2010 trata-se de um projeto de lei do novo Código de Processo Penal.

Este projeto não menciona em nenhum de seus artigos a obrigatoriedade do registro e guarda dos logs de acesso à internet, tampouco trata-se da obrigatoriedade de cadastro dos usuários da rede, este projeto limita-se a prever as medidas cautelares pessoais, como o bloqueio de endereço eletrônico. A justificativa desse projeto foi a adequação do CPP a CF/88, uma vez que o código estava ultrapassado na visão de doutrinadores e juristas.

A Lei nº 9.296/1996 disciplinou a interceptação de comunicação telemática ou informática, o que se aplica aos crimes cometidos no ambiente virtual ou por seu meio.

A interceptação telefônica ocorre mediante autorização de autoridades judiciais, a capacitação de ligações telefônicas de cidadãos, sem que os participantes da conversa tenham conhecimento que estão sendo gravados.

É um recurso muito utilizado pelas autoridades públicas durante as investigações criminais ou instrução processual penal, não podendo ser realizadas livremente, somente nas hipóteses previstas em lei.[111]

[110]NASCIMENTO, 2022, p. 18.
[111]ROCHA, Kassio Henrique Sobral. **Resumo da Lei de Interceptação Telefônica para a PCRJ.** Disponível em: https://www.estrategiaconcursos.com.br/blog/lei-interceptacao-telefonica/. Acesso em: 03 set. 2022.

A CF no ins. XII do art. 5º, busca a proteção da intimidade e vida privada do cidadão contra investigações abusivas [112]. Em seu artigo primeiro temos a disposição de quando poderá ocorrer a interceptação telefônica.[113]

Dessa forma, a lei traz expressamente situações em que não é admitida esse procedimento:[114]

1- Quando não houver indícios razoáveis da autoria ou participação em infração penal;

2- Quando a prova puder ser feita por outros meios disponíveis;

3- Quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Somente ocorrerá a interceptação quando não houver outros meios de conseguir provas, devendo haver indícios razoáveis da autoria ou participação nos crimes sujeitos à reclusão. [115]

Dessa forma o juiz e o único que pode decretar a interceptação, podendo ser a interceptação de ofício, aquela que ocorrer sem nenhuma solicitação, ou também poderá autorizá-la quando for requerido:[116]

1- Pela autoridade policial, na investigação criminal;

2- Pelo representante do Ministério Público, na investigação criminal e na instrução processual penal.

No pedido de interceptação deverá conter a demonstração de que a sua realização é necessária a apuração de infração penal, com a indicação dos meios que serão empregados, tendo o juiz 24h para decidir sobre a solicitação, uma vez que haja o caráter de urgência em sua utilização.

Assim, caso seja deferido este pedido, a autoridade policial conduzirá os procedimentos, dando ciência ao MP, que poderá acompanhar a realização.

---

[112]"Art. 5°, XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. "

[113]"Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[114]ROCHA, *op. cit.*

[115]BRASIL. Supremo Tribunal Federal. **A Interceptação Telefônica como meio de prova**. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-10-08_08-00_A-interceptacao-telefonica-como-meio-de-prova.aspx. Acesso em: 30 ago. 2022.

[116]ROCHA, 2022.

A Lei 14.155/21 entrou em vigor no dia 27 de maio de 2021, com alteração no CP tornando assim mais rigorosa a punição para os crimes de violação de dispositivo informático, furto e estelionato cometidos na internet, ou por algum meio eletrônico.

Uma das alterações foi o aumento da pena de reclusão de quatro para oito anos do crime de furto realizado por meio de aparelhos eletrônicos, e aumenta-se a pena para o crime de invasão de aparelhos de informática para obtenção, modificação e destruição de dados, entre outras medidas.[117]

Essas mudanças aconteceram para a atualização do CP diante das mudanças que ocorrem no mundo, principalmente no meio digital, com a facilitação das transações bancárias e os novos modelos de pagamento, (ex; *pix* e *Whatsapp*), para trazer assim uma responsabilidade penal mais gravosa para esses cibercriminoso, que sempre buscam novas formas de praticar esses atos fraudulentos.

Dessa forma essas modificações buscam minimizar os riscos, e também penalizar mais gravemente esse criminoso visto que anteriormente essas penas eram brandas.

Diante do Furto qualificado a nova legislação nos traz, 'Se o furto for cometido mediante fraude e por meio de dispositivo eletrônico, a pena será de reclusão de quatro a oito anos e multa', sem agravantes genéricas, anteriormente somente se tinha a definição desse crime no caso de furto com a destruição de algum obstáculo, (ex: porta, cadeado); fraude ou concurso entre pessoas.[118]

Para este mesmo crime, se for cometido por servidores fora do país, a pena poderá chegar até doze anos e se praticada contra idoso ou vulnerável poderá chegar até dezesseis anos.

Já diante do Estelionato temos o aumento de pena de reclusão de quatro a oito anos e multa, quando a vítima for enganada e assim fornecer informações por meio de redes sociais, com uma possível majoração da pena quando o crime for realizado por meio de servidor localizado em outro país.[119]

---

[117]JOVELINO, Luiz. **Lei 14155 2021**: Lei que amplia penas para crimes cibernéticos é sancionada. Disponível em: https://blconsultoriadigital.com.br/lei-14155-2021-crimes-ciberneticos/. Acesso em: 30 ago. 2022.

[118]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.

[119]MORAES, Leticia Hemerly de. **Dos crimes cibernéticos:** uma análise do crime de estelionato praticado pela internet. Disponível em: https://www.jornaljurid.com.br/doutrina/penal/dos-crimes-ciberneticos-uma-analise-do-crime-de-estelionato-praticado-pela-internet#:~:text=A%20nova%20reda%C3%A7%C3%A3o%20da%20lei,servidor%20localizado%20em%20outro%20pa%C3%ADs.. Acesso em: 30 set. 2022.

Essa legislação nos trouxe um novo dispositivo para o CPP, definindo a competência para processar e julgar determinadas modalidades de crimes de estelionato, entretanto para os casos de estelionato realizados através de depósito, emissão de cheques sem fundos ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima.[120]

O crime de invasão de aparelhos de informática para obtenção, modificação e destruição de dados, teve sua pena aumentada para reclusão de um a quatro anos. A redação antiga nos trazia o seguinte,[121] já com a nova atualização foi para a seguinte forma.[122]

Observamos assim, que este crime teve um aumento considerável em sua pena, com agravantes nos casos que causar prejuízo a vítima, sendo o principal a invasão que resultou na obtenção de senhas e dados da vítima, anteriormente a lei afirmava que nos casos em que não ocorreu a violação dos mecanismos de segurança não haveria crime, atualmente o ato de invasão e considerado crime mesmo que não ocorra a violação dos mecanismos de segurança ocorrendo também o aumento da pena de 2/3, chegando em até sete anos de prisão.[123]

Por último, mas não menos importante, foi incluído o crime de 'Fraude Eletrônica" [124], acontece quando o agente comete o crime com a utilização de informações fornecidas pela vítima ou por terceiro, incluindo-se o ato de induzir ao erro através das redes sociais, contato telefônicos ou pelo correio eletrônico fraudulento ou meio análogo.

Com isso serão punidos os crimes cometidos diante de sites de compra e venda de produtos, podendo a pena chegar a oito ano, sem contar os agravantes.

---

[120]BRASIL. Superior Tribunal da Justiça. **Lei 14.555/2021 só alterou competência para julgamento de estelionato em casos específicos**. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30052022-Lei-14-5552021-so-alterou-competencia-para-julgamento-de-estelionato-em-casos-especificos.aspx. Acesso em: 30 set. 2022.

[121]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.

[122]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.
(…)
Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
§ 3º (…)
– Reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

[123]JOVELINO, 2021.

[124]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 nº 9.609/1998 dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

Atualmente esta lei passou a ser mais conhecida como a lei de *software*[125], ou seja, e o dispositivo que protege os direitos de quem desenvolve programas de computador no Brasil, servindo como referência no sentido de estipular direitos e deveres em relação ao uso de softwares de modo geral, afetando diretamente as atividades de *startups*[126] e *fintechs*[127]*;*[128]

Devemos dar um destaque especial ao artigo 2º[129] da lei, que compara o programa de computador a uma obra literária, ou seja, para as autoridades brasileiras, há uma equivalência em termos de propriedade intelectual, sendo assim, a lei do software e a garantia de que elementos como registro de programas, direitos autorais, contratos de licença e outros pontos serão respeitadas, também estão previstos as sanções para os que sendo comprovadamente desrespeitarem seus termos.

Tem como objetivo principal, como a própria lei já diz, a proteção da propriedade intelectual de programa de computador, sua comercialização no país. Passou-se a ser considerado um marco visionário, pois o marco civil da internet só foi publicado seis anos depois, sendo que a lei do software antecipou uma década para o tratamento de direitos e deveres.

Aqueles que divulgarem, reproduzirem ou extrair vantagem indevidas de programas de computador desenvolvidos por terceiros, até aqueles que adotam ou compram programas nessas condições responderão de maneira criminal, ou seja, todos que violarem os direitos autorais de *softwares* estarão sujeitas a penas de detenção de até 2 anos.[130]

Esta lei está dividida em seis capítulos, abordando questões ligadas ao contexto comercial deixando de lado a parte técnica. Em seu artigo 2º parágrafo 3º, trata-se da proteção desses direitos independentemente de registro, mas não significa que os desenvolvedores estão

---

[125]Software pode ser um produto ou um serviço, podendo ser patenteado e ter seus direitos de comercialização restritos.

[126]Segundo o dicionário português; Startup significa o ato de começar algo, normalmente relacionado com companhias e empresas que estão no início de suas atividades e que buscam explorar atividades inovadoras no mercado**.**

[127]Fintechs é uma empresa de tecnologia que proporciona soluções para os clientes através de serviços digitais. Dessa forma, todos os processos feitos anteriormente apenas em agências físicas, podem ser feitos no celular ou computador, de onde o usuário estiver.

[128]FREITAS, Cristiano. **Lei de softwares**: 4 pontos que sua empresa precisa se atentar. Disponível em: https://syhus.com.br/2019/09/24/le-de-software/#:~:text=A%20lei%20n%C2%BA%209.609%20de,versa%20sobre%20aspectos%20mais%20autorais. Acesso em: 30 ago. 2022.

[129]"O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei".

[130]FREITAS, 2022.

dispensados de registrar suas criações, estando devidamente disposto nas alíneas I, II e III do artigo 3º[131].

A propriedade intelectual de um programa de computador deve ser registrada no Instituto Nacional da Propriedade Industrial (INPI), órgão do governo, ligado ao Ministério da Economia, que é o responsável por protocolar requisições de marcas e patentes, este registro possui validade de cinquenta anos, contendo a partir de 1º de janeiro do ano seguinte a sua criação (art.2º p. 2º).

O capítulo III, trata-se da garantia dos usuários, afinal um dos objetivos finais do desenvolvedor de programa é destiná-lo a venda, para geração de lucro. Já o capítulo IV, fala sobre os contratos de licença de uso, sua comercialização e transferência de tecnologia, o INPI entra como um órgão garantidor desses direitos e deveres (art. 11º[132]). Os artigos 7º e 8º nos trazem os direitos dos usuários, ou seja, as pessoas que compram estes programas de computador.[133]

A Lei 14.132/21 entrou em vigor no dia 31 de março de 2021, com alteração no CP para a inclusão do artigo 147-A[134], tipificando o crime de *stalking* (perseguição[135]), sendo uma inovação para o ordenamento jurídico tipificando esse tema em específico.

Segundo Carlos Pereira Thompson *apud* Vitor Pereira Pacheco:

> A criminalização da conduta de *stalking* acompanha um movimento que nasceu nos Estados Unidos e se estendeu para a Europa, numa verdadeira onda punitiva ligada aos fatores de expansão do Direito Penal. Nesse jaez, é correto

---

[131]O pedido de registro estabelecido neste artigo deverá conter, pelo menos, as seguintes informações:
I – Os dados referentes ao autor do programa de computador e ao titular, se distinto do autor, sejam pessoas físicas ou jurídicas;
II – A identificação e descrição funcional do programa de computador; e
III – os trechos do programa e outros dados que se considerar suficientes para identificá-lo e caracterizar sua originalidade, ressalvando-se os direitos de terceiros e a responsabilidade do Governo.

[132] Nos casos de transferência de tecnologia de programa de computador, o Instituto Nacional da Propriedade Industrial fará o registro dos respectivos contratos, para que produzam efeitos em relação a terceiros.
Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

[133]FREITAS, 2022.

[134]Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
§ 1º A pena é aumentada de metade se o crime for cometido:
I – Contra criança, adolescente ou idoso;
II – Contra mulher por razões da condição de sexo feminino, nos termos do §2º-A do art. 121 deste Código;
III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
§ 3º Somente se procede mediante representação.

[135]Caracterizado no verbo "perseguir", que significa ir ao encalço de, atormentar, importunar, aborrecer.

> afirmar que o legislador utilizou o direito comparado como fonte de inspiração para a emolduração penal específica da conduta criminosa em comento.[136]

Este crime se encontra inserido no capítulo dos crimes contra a liberdade individual, tendo como objeto jurídico a tranquilidade pessoal, ou seja, antes mesmo de atingir a liberdade individual da vítima, restará primeiramente perturbada a sua tranquilidade, mas isto não afasta a possibilidade de proteção de outros bens jurídicos. Dessa forma, deve haver uma sucessão de atos e comportamentos, sendo que somente um ato isolado não será suficiente para a configuração do crime.[137]

Para que esse crime seja configurado na modalidade majora deve ser motivada pela condição do sexo feminino (§1, inc. II[138]), sendo elas as maiores vítimas dessa perseguição, não há forma culposa, sendo seu elemento subjetivo o dolo, não tendo o dolo específico, sendo assim mesmo que o agente não tenha dolo específico, de gerar essas consequências, o tipo exige sua verificação, demonstrando assim qual a espécie de abalo sofrido pela vítima.[139]

Dessa forma, o tipo penal exige que a perturbação gere ou tenha possibilidade de gerar:

1. Ameaça à integridade física ou psicológica;
2. Restrição da capacidade de locomoção; ou
3. Invasão ou perturbação da liberdade ou privacidade.

É considerado um crime de tipo penal aberto, podendo ser praticado de forma livre, pois pode ser praticado por qualquer meio, podendo ser de forma real (presencial) e seguir locais públicos ou privados, comparecer ao local de trabalho, fazer ronda na frente da casa, já a perseguição remota (a distância), se dá de forma *off-line*, como enviar cartas, flores, oferecer músicas em rádios, entregas e encomendas, ou de forma *on-line*, postagens em redes sociais, mensagens e ligações.

A tentativa é admitida. Frise-se, contudo, que, para os adeptos de que a conduta descrita se apresenta como crime habitual, a tentativa não é admitida, por ser uma característica dessa espécie delitiva.

---

[136] PACHECO, Vitor Pereira. **O crime de perseguição**: breves críticas sobre o stalking no Direito brasileiro. [2021]. Disponível em: https://www.migalhas.com.br/depeso/342950/o-crime-de-perseguicao]. Acesso em: 28 jul. 2022.

[137] GARCEZ, Willian. **Lei 14.132/21**: A tipificação do crime de perseguição (stalking). Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/04/28/lei-14-13221-tipificacao-crime-de-perseguicao-stalking/. Acesso em: 05 set. 2022.

[138] O §1° prevê a modalidade majorada, aumentando-se de metade a pena quando o crime for praticado (b**)** contra mulher por razões da condição de sexo feminino;

[139] GARCEZ, 2022.

Caso essa perseguição culmine violência ou agressão física que resultem em lesões corporais, o agente responderá em concurso formal impróprio (§2), sendo caso de concurso de crimes. O acordo de não persecução penal não é cabível.[140]

O Decreto Lei 7.962/2013 entrou em vigor em 15 de março de 2013, que regulamenta o CDC, dispondo sobre a aquisição de produtos ou serviços *online*.

Este dispositivo trata-se da necessidade de exibir aos visitantes ou clientes, informações claras sobre seus produtos, serviços e fornecedores, prestando um atendimento fácil ao consumidor, e garantindo o direito de arrependimento do cliente, ou seja, traz mais segurança nessa relação.[141]

Sendo assim os *sites online* devem destacar os seguintes aspectos:[142]

- O seu nome empresarial e o número do CNPJ;
- Os seus dados localização e contato, como endereço físico, telefone e *e-mail*;
- As descrições essenciais dos produtos, incluindo os riscos à saúde e à segurança;
- A especificação no preço de quaisquer custos adicionais, como despesas com frete ou seguro;
- As condições globais da oferta, contendo a disponibilidade do produto ou de execução do serviço, meios de pagamento, promoções e formas e prazo de entrega;
- As informações sobre possíveis restrições ao aproveitamento da oferta.

Para os *sites* que ofertam compras coletivas ou categorias semelhantes, deverão além dos deveres citados acima conter, para a compra coletivo tem-se uma regulamentação específica em projeto de lei 1.232/2011, que tem por fim regrar a venda eletrônica por meio de sites estabelecendo critérios para seu funcionamento.[143]

- A quantidade mínima de consumidores para a efetivação do negócio;
- O prazo para utilização da oferta pelo comprador;
- A identificação do fornecedor responsável pelo site e do fornecedor da oferta com nome empresarial, número de CNPJ, endereço físico e eletrônico.

O fornecedor também deverá: [144]

- Confirmar imediatamente o recebimento da aceitação da oferta;

---

[140]*Ibidem*.
[141]SILVA SANTANA & TESTON ADVOGADOS. **Decreto Lei 7.962/2013**; Regulamenta o comercio eletrônico. Disponível em: https://www.sst.adv.br/decreto-7-96213-regulamenta-o-comercio-eletronico/. Acesso em: 05 set. 2022.
[142]VTEX. **Lei do E-commerce – regulamentação pelo Decreto n. 7.962**. Disponível em: https://vtex.com/pt-br/blog/estrategia/lei-do-e-commerce-regulamentacao-pelo-decreto-n-7-962/. Acesso em: 05 set. 2022.
[143]*Ibidem*.
[144]*Ibid*.

- Prestar atendimento eficaz em meio eletrônico a fim de permitir que o consumidor obtenha informações, esclareça dúvidas, apresente reclamações e suspenda ou cancele o negócio (devendo a resposta ser fornecida pela empresa em até cinco dias);
- Confirmar instantaneamente o recebimento da solicitação do consumidor pelo mesmo meio utilizado por ele;
- Disponibilizar ferramentas eficazes ao consumidor para identificação e correção instantânea de erros ocorridos nas fases anteriores à conclusão da compra;
- Utilizar mecanismos capazes de garantir a segurança para o pagamento e para o gerenciamento de dados do consumidor;
- Apresentar um resumo do teor do contrato antes da contratação, com informações imprescindíveis para o consumidor tomar sua decisão, destacando os direitos e deveres de loja e cliente;
- Fornecer o contrato ao consumidor para que ele possa ser conservado e reproduzido logo após a finalização da compra;
- As contratações deverão observar o cumprimento dos termos da oferta, sendo que a entrega dos produtos e a prestação dos serviços respeitarão prazos, qualidade, quantidade e adequação inerente.

Além disso, a lei 7.962/2013 cuida ainda do direito de arrependimento do consumidor, devendo o fornecedor informar os meios para que este dispositivo possa ser exercido, o arrependimento em si implica a rescisão contratual sem prejuízo para o consumidor.

Conforme o art. 49 do CDC, este arrependimento deve ser realizado no prazo de sete dias, quando ocorrer por telefone ou em domicílio.[145]

Dessa forma, este decreto veio para que as relações jurídicas sejam mais seguras, facilitando o acesso às informações sobre os fornecedores e seus produtos e serviços, dentro do comércio eletrônico.

[145]VTEX, 2022.

7 PROVAS, AUTORIA E COMPETÊNCIA

7.1 Dificuldade na Colheita de Provas

Com a criação e inovação dos meios tecnológicos, apareceram na sociedade novas formas de difusão de ameaças, através de novos meios para o cometimento de crimes conhecidos e, também, o surgimento de novas modalidades de crimes antes inexistentes.

Ensejando assim o surgimento de novos lócus da criminalidade, por meio da qual os criminosos se valem da vulnerabilidade dos sistemas e dos próprios usuários dessa rede para cometer inúmeros delitos.

Com o surgimento dessas novas modalidades de cibercrimes, juntamente com o anonimato que ocorre na internet, surgiram assim maiores problemas para os operadores do direito no processo de investigação, punição e repressão desses crimes, uma vez que as normas jurídicas não conseguem acompanhar a velocidade em que esses delitos evoluem.[146]

Com esse grande aumento dos crimes cibernéticos, o Brasil passou a ser um dos principais países da América Latina com atividades criminosas pela internet, onde diversas vezes os sujeitos passivos dos crimes virtuais não comunicam a prática desses delitos aos órgãos e autoridades competentes, por incredulidade da resposta estatal.[147]

Essa sensação de insegurança e impunidade, que leva as vítimas a não denunciarem, vêm do reduzido número de casos solucionados e efetivamente reprimidos.

As dificuldades para a solução desses crimes vão além da polícia, passando pelo Ministério Público e o poder judiciário, até os legisladores e os demais operadores de direito que encontram barreiras que dificultam o exercício do jus puniendi e impulsionam assim a criminalidade.[148]

A primeira dificuldade encontrada no ordenamento jurídico, e a necessidade de comprovação do crime, com provas robustas, de autoria e de materialidade do delito, para que a sanção penal seja aplicada, caso não consiga ser comprovada a materialidade ou a autoria, o

---

[146]NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**: Conteúdo Jurídico. Disponível em https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 28 ago. 2022.

[147]SANCHES, Ademir Gasques; ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 30 ago. 2022.

[148]CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista científica eletrônica do curso de direito**, 13. ed., 2019. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 20 ago. 2022.

juiz deverá absolver o réu, conforme o artigo 386 do Decreto – lei nº 3.689, de 3 de outubro de 1941 do CPP.[149]

Os meios informáticos são dotados de variáveis, motivos pelo qual os cibercriminoso encontram várias formas de praticarem esses delitos, mas sendo iniciada a persecução penal, se faz de imediata a identificação do meio pelo qual tal crime foi praticado, pois conforme o meio pelo qual esse criminoso executou o crime, diferente serão as técnicas utilizadas para a obtenção da autoria e materialidade do delito.

A prova da autoria deve ser o primeiro problema a ser resolvido na investigação, pois o agente criminoso não irá utilizar de sua real identidade para o cometimento do cibercrimes, além também do inicial anonimato, sendo esses os fatores que tornam o endereço de IP, uma das evidências de mais relevo dentro da investigação, pois conseguir esses dados é um processo trabalhoso visto que está rodeado de exigências que devem ser respeitadas, para não contaminar a prova obtida e as provas derivadas dela também.

Em alguns casos será necessário ainda que as provas obtidas sejam submetidas a rigorosa perícia técnica, para que depois possam ingressar no processo sendo capazes de lastrear uma condenação.

Os *logs* e o endereço IP (*internet protocol*) são as evidências de maior relevo a serem perseguidas na investigação dos crimes informáticos, além de serem as provas que irão nortear toda a investigação. Essas informações estarão acompanhadas do registro da data, horário e fuso horário da conexão, além do respectivo número de protocolo de *internet* atribuído àquele acesso.[150]

Já quando se trata dos endereços de IP, estamos nos referindo ao registro criado toda vez que uma conexão é feita. Esses endereços de protocolos de internet podem ser estáticos ou dinâmicos.

---

[149]Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça:
I - Estar provada a inexistência do fato;
II - Não haver prova da existência do fato;
III - Não constituir o fato infração penal;
IV - Estar provado que o réu não concorreu para a infração penal;
V - Não existir prova de ter o réu concorrido para a infração penal;
VI – existirem circunstâncias que excluam o crime ou isentem o réu de pena, ou mesmo se houver fundada dúvida sobre sua existência;
VII – não existir prova suficiente para a condenação.

[150]DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos**: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso em: 25 jun. 2022.

Os IPs estáticos são comumente utilizados por grandes corporações como os órgãos públicos, universidades e empresas de grande porte. Esse tipo de IP não tem variação, ou seja, àquele usuário sempre se dará o mesmo protocolo de internet, independente de quantas conexões à rede forem realizadas por ele.[151]

Aos outros usuários, será atribuído o IP dinâmico, o qual terá uma identificação diferente concedida por seu provedor de acesso toda vez que for estabelecida uma conexão com a *internet*.

De qualquer forma, independentemente do tipo de protocolo de internet atribuído ao usuário, se dinâmico ou estático, nunca nenhum número de IP será atribuído a mais de um usuário na mesma data, horário e fuso horário.[152]

Para conseguir acesso o número de IP deve-se ter uma ordem judicial escrita e fundamentada emitida por autoridade judiciária competente, dirigida aos provedores de acesso à internet, que faça referência a três indicadores: número de IP, a data do acesso à rede e o horário e fuso horário deste acesso, mesmo já tendo obtido o número de IP, a nova decisão judicial deverá conter esses três indicadores, caso não faça referência não é capaz de autorizar a quebra de sigilo dos dados telemáticos.[153]

Iniciando as investigações, quando da busca pela autoria da atividade delitiva, a polícia esbarra em seu primeiro obstáculo, qual seja o artigo 5º [154], incisos X [155] e XII [156] da Constituição Federal Brasileira de 1988, que protege a privacidade e os dados.

Desta forma, respeitando tais direitos constitucionalmente assegurados, o acesso aos dados de logs e protocolos de internet só poderão ser requeridos das empresas responsáveis mediante autorização judicial fundamentada, o que, inevitavelmente, leva a uma demora prejudicial ao êxito das investigações.[157]

Tendo em vista toda essa dificuldade do procedimento para o requerimento das provas, os investigadores ainda têm que lidar com empresas que se recusam a prestar auxílio, temos como exemplo a empresa *WhatsApp*, que se recusou a obedecer a ordem da justiça brasileira

---

[151]SILVA, 2022.
[152]*Ibidem*, p. 25.
[153]*Ibid*., p. 26.
[154]**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:
[155]**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.
[156]**XII** - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996).
[157]SILVA, *op. cit.*, p. 26.

para a prestação de informações sobre seus usuários que estavam sendo investigados em processo criminal, sua recusa gerou uma decisão judicial de bloqueio da rede social em todo o território nacional, por tempo limitado. Tal decisão posteriormente foi tida como inconstitucional em decisão do Supremo Tribunal Federal.[158]

Na primeira audiência realizada no dia 28/08/2014, pela Comissão Parlamentar de Inquérito dos Crimes Cibernético, foi discutida a dificuldade sofrida na investigação e repressão dos cibercrimes, dando início já na fase em que se faz necessário rastrear, identificar e punir esses tais cibercriminoso, pois na mesma velocidade em que os crimes são cometidos seus vestígios podem se perder.[159]

O Delegado Elmer Coelho Vicente, aponta duas grandes dificuldades encontradas pela polícia na hora da investigação: sendo a primeira onde a maioria das empresas responsáveis por *sites* e aplicativos, não aceitam a requisição da polícia pela *internet*, a segunda sendo que após a Lei nº 12.965/14 mais conhecida como, Marco Civil da *Internet* as empresas passaram a exigir a ordem judicial para a concessão de informações.[160]

Esses sites e provedores de acesso à rede são os locais em que as informações sobre a utilização da plataforma são registradas e armazenadas, em sua maioria, essas informações não são armazenadas por um longo período de tempo, ficando claro que a demora para a obtenção desses dados para que se possa prosseguir nas investigações, gera danos que são irreparáveis, como a perda total dessas informações, comprometendo todo o trabalho do agente.[161]

Pode ocorrer também a possibilidade desses dados serem apagados ou modificados pelos próprios agentes, gerando a destruição ou a modificação das provas do crime.

Após toda essa fase dos tramites legais e a possível identificação desse cibercriminoso através dessas informações fornecidas, a investigação se dedicara a busca da materialidade do cibercrimes cometido pelo agente, requerente ao juiz competente a expedição de mandado de busca e apreensão em desfavor dos envolvidos no crime, para que se possa apreender os

---

[158]CONSULTOR JURÍDICO. **STF derruba decisão judicial e libera volta do WhatsApp**. Disponível em: https://www.conjur.com.br/2016-jul-19/stf-derruba-decisao-judicial-libera-voltawhatsapp#:~:text=Por%20identificar%20viola%C3%A7%C3%B5es%20%C3%A0s%20liberdades,feira%20(19%2F7). Acesso em: 26 jun. 2022.

[159]CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet**. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-deinternet/. Acesso em: 26 jul. 2022.

[160]*Ibidem*.

[161]FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** Disponível em: https://flucianofeijao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf. Acesso em: 26 jul. 2020.

equipamentos informáticos (computador, celular, *ipad*, *tablet*), e os demais documentos que possam servir para a elucidação e prova do delito.[162]

Com todo o procedimento para se chegar a apreensão dos objetos necessário a prova do crime, causa uma demora, podendo criar um ambiente propício para a destruição dos equipamentos ou dos dados nele armazenados, desaparecendo com as evidências que se busca.[163]

Algumas vezes será necessária a realização de uma perícia técnica para a produção da prova criminal considerada hábil para uma condenação, mas para que tal perícia seja realizada deve-se o perito dispor do computador ou outro equipamento informático obtido na busca e apreensão.[164]

Continuando a apontar os problemas encontrados pelos investigadores, chegamos ao *cloud computing*[165], ou computador nas nuvens, sendo um serviço disponível pela rede mundial de computadores para o acesso e execução de arquivos e programas realizado exclusivamente pela *internet*, ou seja, os dados utilizados pelo usuário não precisam estar necessariamente em seu aparelho, bastando apenas que esse indivíduo acesse a internet, e entre na "nuvem" onde seus arquivos e dados estarão armazenados.[166]

A "nuvem", ou seja, o computador que hospeda os arquivos, pode estar em qualquer lugar do mundo, assim o usuário que estiver no Brasil, pode acessar remotamente arquivos que são armazenados na "nuvem" em qualquer outro país não importando a distância.[167]

Nesse tipo de acesso, qualquer arquivo e programa utilizado não estará vinculado ao computador do usuário, mas sim em servidores on-line que são criados exclusivamente para servir como hospedeiros, permitindo que os usuários desse serviço tenham acesso às informações ali contidas a qualquer tempo, em qualquer lugar e utilizando de qualquer equipamento conectado à rede.[168]

Esse tipo de serviço possui inúmeros benefícios aos usuários, pela sua praticidade e segurança dos dados armazenados, mas o *cloud computing*, ocupa em lugar de destaque no quesito dificuldades para a elucidação e punição dos cibercrimes, visto que é improvável na

---

[162]SILVA, 2022.
[163]*Ibidem*, p. 29.
[164]*Ibid*.
[165]ROCKCONTENT. **Descubra finalmente o que é o cloud computing e para que serve a computação em nuvem.** Disponível em: https://rockcontent.com/br/blog/cloud-computing/. Acesso em: 28 jul. 2022.
[166]SILVA, *op. cit.*
[167]DURBANO, Vinicius. **Computação em nuvem:** tudo que você precisa saber sobre. Disponível em: https://blog.ecoit.com.br/computacao-em-nuvem/. Acesso em: 28 jul. 2022.
[168]CARLOS, Heder Sabino. **Computação na nuvem (cloud computing).** Disponível em: https://www.metodoconcursos.com.br/2021/02/computacao-na-nuvem-cloud-computing.html. Acesso em: 29 jul. 2022.

maioria das vezes que se consiga apreender um computador localizado em outro país podendo inviabilizar ou tornar impossível que seja obtido a prova da materialidade do delito.[169]

A *internet* liga usuários localizados em diferentes partes do mundo, transcendendo fronteiras, permitindo a comunicação e troca de arquivos sem se preocupar com a distância em que os usuários se encontram um do outro, dessa forma os cibercrimes possibilitam que qualquer ameaça seja globalizada, tornando possível dano às vítimas que se encontram a distâncias inimagináveis dos autores dos crimes, também podendo haver o concurso de agentes localizados em diferentes países, isso tudo se tornou possível através do uso de recursos tecnológicos avançados, que permitem a preparação e execução de tais crimes mesmo a longas distâncias.[170]

Já a respeito da consumação desses crimes temos diversos problemas de competência e conflito de normas, devido à natureza transnacional da *internet*, e consequentemente dos delitos cometidos nela, se faz necessário assim que haja uma cooperação internacional entre os Estados soberanos para melhor interligar os órgãos jurisdicionais e investigativos quanto aos crimes cibernéticos que assolam as nações atualmente.[171]

Dessa forma será abordado mais uma dificuldade encontrada, sendo esta a falta de legislação adequada, para a obtenção das provas, os operadores de direito em geral, com ênfase na fase investigativa, devem respeitar o princípio da legalidade e as normas processuais, ocorrendo assim a falta de normas que possam ser aplicáveis nos crimes virtuais e suas vertentes, sofrendo muitas vezes com a falta de técnica legislativa adequada, dando margens para que haja a interpretações dúbias, dificultando a sua aplicabilidade.[172]

O processo legislativo tenta controlar essa problemática criando normas, leis e tipificando crimes que estão surgindo tentando facilitar a fase investigativa, mas não conseguindo acompanhar a velocidade em que os crimes informáticos se desenvolvem e se aperfeiçoam.[173]

Sua dificuldade se encontra em normas relativas ao procedimento cabível para a apuração desses crimes, levando em conta as peculiaridades do meio pelo qual tais delitos foram

---

[169]FREIRE, André Luiz; KUJAWSKI, Fabio. **Tratamento e classificação de informações em nuvem e a Lei de Acesso à Informação**. Disponível em: https://www.convergenciadigital.com.br/Opiniao/Tratamento-e-classificacao-de-informacoes-em-nuvem-e-a-Lei-de-Acesso-a-Informacao-61250.html. Acesso em: 29 jul. 2022.

[170]SILVA, 2022, p. 30.

[171]SOUZA, Carlos Jeremias Marques. **Os Delitos Informáticos na Internet**. Disponível em: https://repositorio.ufc.br/bitstream/riufc/29334/1/2008_tcc_cjmsousa.pdf. Acesso em: 29 jul. 2022.

[172]DORIGON; SOARES, 2022.

[173]SILVA, *op. cit*., p. 31.

cometidos, não nos enganemos pensando então que essa dificuldade se encontra na falta da criação de tipos penais, pois o objeto material do crime virtual já está tutelado penalmente.

Saindo um pouco da problemática que envolve a internet, mas falando ainda da dificuldade encontrada pelos investigadores, chegamos aos problemas estatais, que se dão pela falta de efetivo nos órgãos investigativos, sendo essa deficiência de investimentos nos órgãos policiais, sendo um dos mais prejudiciais a falta de pessoal que atua nessa área, gerando assim um acúmulo de *notitia criminis*[174], sendo que a demanda não consegue ser cumprida pela quantidade de agentes estatais.[175]

Dessa forma o volume de investigações cresce paralelamente com o número dos crimes praticados virtualmente, com isso o efetivo dos policiais judiciários e dos órgãos de perícia técnica precisam crescer na mesma proporção, para que se consiga maior êxito na repressão e investigação desses crimes.

O problema se torna ainda maior, quando se analisa a falta de capacitação técnica adequada do pessoal desses órgãos, pois as tecnologias de informação e comunicação possuem uma complexidade extrema, fazendo com que os órgãos, tanto legislativos, investigativos e judiciários não estejam preparados e nem capacitados para lidar com essa criminalidade.[176]

Se faz necessário que os investigadores tenham conhecimento adequado para buscar e manusear os dados, pois as evidências são instáveis e podem facilmente serem perdidas, corrompidas, apagadas ou modificadas, exigindo essa capacidade para que se garanta que ocorra a correta coleta dessas evidências.[177]

Mas para que isso aconteça o Poder Público deve investir constantemente na capacitação dos seus agentes que atuam nessa área.

Quando o profissional possui capacitação técnica, seu trabalho sofre com a falta de equipamentos e meios técnicos adequados, inviabilizando as investigações dos crimes virtuais, caracterizando a flagrante falta do Estado, em sentido amplo.[178]

Diante do exposto, se faz necessário a criação de delegacias especializadas no combate de crimes cibernéticos, também de varas em tribunais especializadas nessa área, onde geraria um aperfeiçoamento do Estado para lidar com essa crescente modalidade criminosa, além de

---

[174]Conceitua-se ***notitia criminis***, ou **notícia de um crime**, como o ato pelo qual se leva ao conhecimento da autoridade policial a ocorrência de um fato criminoso. (**CPP, art. 5º**). PETIÇÕES ON LINE. **Tipos de petições**. Disponível em: https://www.peticoesonline.com.br/tipo-de-peticao/notitia-criminis. Acesso em: 29 jul. 2022.
[175]CRUZ; RODRIGUES, 2019.
[176]DORIGON; SOARES, 2022.
[177]SILVA, 2022, p. 32.
[178]*Ibidem*, p. 33.

acompanhar essa sua veloz evolução. No estado de São Paulo no ano de 2020, foi criada a Divisão de Crimes Cibernéticos, para evitar o cometimento desse delito, e no caso dele acontecer terá instrumentos para identificar e prender o criminoso.[179]

Como vimos anteriormente, o problema que ronda os crimes cibernéticos e seus investigadores, tem a ver com a falta de efetivos e especialização desses agentes, a falta de qualificação e a falta de meios adequados para perseguir esses delitos, impulsionando assim o crescimento da criminalidade virtual, mas o fator que gera maior adversidade, e que impulsiona mais ainda o crescimento desses delitos sendo a principal causa da impunidade e o anonimato.

A *internet* se tornou um ambiente altamente atrativo à prática de crimes devido à suas características, como a facilidade do cometimento desses atos; a volatilidade dos dados ali gerados; a possibilidade de perpetrar o ilícito penal em qualquer lugar que se encontre o agente ou a vítima; a sensação de anonimato e a aparente ausência de vigilância, o que impulsionam o cometimento de crimes nessas circunstâncias.[180]

Como já exposto, em regra, a autoridade policial em sua investigação, e com a autorização judicial terá acesso aos logs e endereços de IP, que foram utilizados na conduta criminosa, após conseguindo a localização e identificação do agente que cometeu tal crime, porém a diversas formas de se fraudar esse tipo de evidência, podendo se utilizar de redes *Wi-Fi* abertas ou *Lan Houses*[181] e *Cyber* cafés[182], ou até mesmo *proxies*.[183;184]

A criação dos *proxies* foram criadas visando a proteção dos usuários, sua função inicial era esconder o endereço de IP dos usuários e protegê-los de ameaças na rede ou evitar o furto

---

[179]SÃO PAULO. Governo do Estado. **Polícia Civil e Governo do Estado inauguram Divisão de Crimes Cibernéticos**. Disponível em: https://www.policiacivil.sp.gov.br/portal/faces/pages_home/noticias/noticiasDetalhes?rascunhoNoticia=0&collectionId=3584125652210479 10&contentId=UCM_056415&_afrLoop=77207818476528&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26collectionId%3D3584125652210479 10%26_afrLoop%3D77207818476528%26contentId%3DUCM_056415%26rascunhoNoticia%3D0%26_afrWindowMode%3D0%26_adf.ctrl-state%3D99w8trdog_4. Acesso em: 29 jul. 2022.

[180]CRUZ; RODRIGUES, 2019.

[181]Lan House estabelecimento comercial em que é possível, mediante uma taxa equivalente ao tempo de uso, ter acesso a computadores e, na maioria das vezes, à internet, com o objetivo de pesquisar, jogar, receber e enviar mensagens eletrônicas. Geralmente esse local oferece, ainda, outros serviços, como impressão de material.

[182]Cyber Café (Ciber café, no português) é uma palavra utilizada para se referir a um estabelecimento comercial de ambiente calmo que oferece o serviço de lanchonete e bar, juntamente com computadores para acesso à internet ou outros aparelhos eletrônicos. O local disponibiliza pontos de acesso para notebooks e principalmente a cobertura de internet wireless, rede sem fio para a entrada dos dispositivos próprios dos clientes, que pagam uma taxa pela sua utilização.

[183]Os proxies são servidores que atuam como intermediários, solicitando, para seus clientes, recursos ou serviços de outros servidores. Desta forma, os proxies agem como ponte" entre o usuário do serviço e o conteúdo acessado por este usuário na internet. Uma vez utilizado este recurso, o endereço de internet protocol que constará no banco de dados do site ou do provedor de acesso à rede será o do servidor proxy, e não o do usuário que efetivamente acessou àquela página da internet.

[184]SILVA, 2022, p. 33.

de seus dados, porém essa ferramenta passou a ser utilizada para práticas criminosas, passando a ser criados proxies destinados exclusivamente para os meios ilícitos, visando esconder a real identificação de seus usuários dificultando assim a investigação de crimes praticados por eles, obtendo a impunidade do criminoso.[185]

Essa modalidade foi denominada de *proxy* anônimo, sendo uma ferramenta muito utilizada para evitar que suas atividades praticadas virtualmente deixassem vestígios, ocultando suas informações pessoais que poderiam o identificar, esses servidores garantem que haja o anonimato sobre o computador ou equipamento informático que deu origem ao evento na *internet*, ou sobre quem praticou as condutas lesivas na rede[186].

Este usuário ainda tem a possibilidade de utilizar uma cadeia de *proxies*, onde se houver a falha em algum desse *proxie* os demais iriam trabalhar para que as informações do usuário fiquem ocultas, de forma que não haja falhas no processo de se manter anônimo, assegurando que será impossível rastrear o seu número de IP.[187]

Já as redes *Wi-Fi* abertas, tem sua finalidade de servir um público em geral com esses tipos de conexões, não exigem nenhum cadastro ou identificação de seus usuários normalmente, gerando aos cibercriminoso um ambiente favorável para o cometimento desses crimes, pois sua identificação e localização do criminoso será quase impossível gerando mais chances de impunidade.[188]

Cabe lembrar, ainda, que nos poucos casos em que essas empresas prestadoras desses tipos de serviços exigem o cadastro do cliente para que este possa realizar o acesso, o uso de documentos falsos é um meio muito utilizado para burlar esse precário controle.[189]

Adiante pesquisou-se a forma de obtenção dessas provas digitais.

7.2 Obtenção das Provas Digitais

A prova é um meio imprescindível para a formação da convicção do juiz, a respeito da existência ou não do fato alegado.

[185]SILVA, 2022, p. 34.
[186]DORIGON; SOARES, 2022.
[187]SILVA, *op. cit*., p. 34.
[188]DORIGON; SOARES, *op. cit*..
[189]SILVA, *op. cit*., p. 35.

Nas palavras de Bentham, a prova: “no sentido mais amplo da palavra, entende-se como um fato supostamente verdadeiro que se presume deva servir de motivo de credibilidade sobre a existência de outro fato”.[190]

Nas palavras de Benjamim Silva Rodrigues, a respeito das provas digitais:

> À prova eletrônico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada em repositório eletrônico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrônicas, privadas ou publicamente acessíveis, sob a forma binária ou digital.[191]

No artigo 125º do CPP[192], encontra-se o Princípio de Admissibilidade de todas as provas que a lei não proibir, devendo possuir seu valor probatório, para poder ser admitida pelo julgador, sendo encontrada em um formato distinto.[193]

A prova em seu formato digital dificulta a sua apreensão, pois é constituída por meios técnicos específicos que exigem certos conhecimentos técnicos para aprender e disponibilizar, podemos dizer que se trata de uma prova duradoura pois não extingue com o tempo, sua conservação pode ser armazenada e transmitida por meios de armazenamentos digitais, que utilizamos em nosso dia a dia, sendo computadores, PEN USB[194], disco de armazenamento, entre outros.[195]

Apesar deste formato digital, a prova digital possui capacidade bem ampla, pois pode abranger inúmeros tipos de conteúdo (áudios, vídeos, dados da rede, programas), atribuindo um caráter útil e dinâmico a este tipo de prova, durante o processo e na descoberta da verdade material para sua resolução.

A prova digital passa a ser imprescindível na investigação criminal, esta que é bastante complexa, e apesar de toda a sua utilidade, carrega consigo algumas fragilidades inerente a sua estrutura, primeiramente por ser uma prova incorpórea (digital), codificada, altamente mutável,

---

[190]NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. São Paulo: Grupo GEN, 2021b. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993627/. Acesso em: 26 jun. 2022.

[191]RODRIGUES, Benjamim Silva. **Direito Penal**: Parte Especial: Direito Penal Informático-Digital. Coimbra (Portugal): Coimbra Ed., 2009. p. 39.

[192]Art. 125º : Legalidade da Prova: São admissíveis as provas que não forem proibidas por lei.

[193]BRANCO, Jose Ricardo Marques. **Prova digital os meios de obtenção de prova digital e a restrição de direitos do arguido.** Disponível em: https://estudogeral.sib.uc.pt/retrieve/203656/Disserta%C3%A7%C3%A3o%20-%20Jos%C3%A9%20Ricardo%20Marques%20Branco%20-%20uc2012153587%20-%20pdf.pdf. Acesso em: 01 set. 2022.

[194]Uma Pen-USB trata-se de um “dispositivo de memória constituído por memória flash (EEPROM), capaz de fazer a gravação de dados com uma ligação USB tipo A, permitindo a sua conexão a uma porta USB de um computador ou outro equipamento com uma entrada USB, como um rádio ou televisão”. A velocidade de transmissão e a capacidade de armazenamento variam consoante os dispositivos, in o .

[195]BRANCO, *op. cit.*, p. 21.

que exige conhecimentos técnicos especializados para poder ser investigada, não é qualquer pessoa que consegue aceder a este tipo de dados, ou a outros sistemas informáticos, deve ser alguém que possua técnicas específicas para realizar a investigação muito complexas e sensíveis, que não levem a perda ou alteração da prova.[196]

Possui também um caráter temporário e frágil, pois pode ser modificada ou alterada com bastante facilidade, tornando-se assim um tipo de prova bastante dinâmico, mas instável, o que leva a que se tenha um cuidado maior do investigador ao recolher a prova digital.

Partindo do ponto em que se fala da fragilidade da prova digital, não podemos deixar de falar sobre a área que mais recebe crítica, a identificação do agente que praticou o cibercrimes, pois pode ser extremamente difícil identificar o concreto sujeito que praticou aquele crime, muitas vezes é impossível, não é fácil saber quem produziu o documento, utilizou o computador, o celular, ou outro aparelho informático, pois não se consegue visualizar o agente.[197]

Já o que se diz respeito aos dispositivos em si é diferente, pois sua identificação se dá pelo endereço de IP, a partir deste endereço é possível saber a localização do dispositivo que pratica determinado ato, e pratica o crime informático.

Há muitos autores que defendem que a única opção que realmente se consegue identificar o agente que praticou o crime e este usar uma assinatura digital, este tipo de assinatura informática confere credibilidade ao documento, presumindo que quem o submeteu ou enviou tenha sido a pessoa identificada na assinatura.[198]

Trata-se de uma presunção, pois pode por exemplo, a assinatura digital[199] provir de local onde efetivamente ocorreu a prática do crime, mas este ter sido praticado por outro indivíduo que não o proprietário.[200]

Também é relevante abordar-se sobre como a prova pode ser encontrada, recolhida e como ser feita dentro dos trâmites da Ciência Forense Digital, sendo caracterizada seguindo o pensamento de David Ramalho como "a categoria genérica que abrange, em sentido amplo, as atividades de identificação, recolha e análise de prova digital e que inclui, entre outros ramos,

---

[196]BRANCO, 2022, p. 19-20.

[197]"no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em si evidentes, como placas de veículos ou a aparência física, por exemplo." ARAS, Vladimir *apud* MILITÃO, Renato Lopes. **A propósito da prova digital no processo penal**. [*S.l.]:* [*s.n.*], [20--]. p. 263-264.

[198]MILITÃO, *op. cit.*, p. 264.

[199]Assinatura Digital – Uma assinatura digital é um tipo específico de assinatura eletrônica que cumpre os requisitos legais mais rígidos e fornece o mais alto nível de segurança da identidade de um signatário. O QUE é uma assinatura digital? Disponível em: https://www.adobe.com/pt/sign/digital-signatures.html. Acesso em: 01 set. 2022.

[200]BRANCO, *op. cit*., p. 20.

a Ciência Forense Computacional",[201] não se tem uma opinião dominante sobre qual a metodologia correta adotar no processo de recolhimento de prova digital.[202]

Dessa forma, a regulamentação da prova digital, se encontra circunscrita a três diplomas: o Código de Processo Penal nos seus artigos 187º, 188º e 189º, na Lei nº 32/2008, de 17 de julho, e por último a Lei nº 109/2009, de 15 de setembro, que recebeu o nome de Lei do Cibercrime.

7.3 Da Autoria dos Crimes

Os crimes cibernéticos podem ser praticados por qualquer pessoa, física ou jurídica, mas existem indivíduos específicos que praticam estas infrações.

Esses indivíduos podem ser denominados de *hacker*[203], *cracker*[204], *phreakers*[205], *cardes*[206] e *cyberterrorists*[207] (*cibe* terroristas), dessa forma, vemos que as denominações desses indivíduos vem do idioma inglês, visto que é a linguagem oficial utilizada na *internet*, em diversos serviços e ferramentas oferecidas pela rede, assim, também identifica os sujeitos que praticam esses crimes cibernéticos.[208]

---

[201]RAMALHO, David da Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. [*S.l.*]: Almedina, 2017. p. 108-146.

[202]Neste sentido, David Ramalho faz referência ao modelo de etapas proposto pelo NIST (National Institute of Standards and Technology), que é constituído por quatro etapas na recolha da prova digital, são elas: a recolha, o exame, a análise e o relatório. *Ibidem*, p. 130.

[203]Hacker, em inglês, significa "fuçador". O termo aponta aquele que possui alta habilidade técnica para lidar com sistemas de computação ou comunicações em rede. Na verdade, o hacker procura invadir máquinas de terceiros para satisfazer seu próprio ego, como se fosse para vencer o desafio tido como invencível. Sua intenção não costuma ir além de fuçar determinado sistema. Podemos dizer que a conduta do hacker, se fosse tipificada com a ideia acima, seria um crime de mera conduta, já que não apresenta nenhuma lesão efetiva a um bem jurídico. Na maioria das vezes o hacker invade sistemas informáticos alheios apenas para provar que é capaz de tal proeza. Seria, hipoteticamente, uma "invasão de domicílio moderna".

[204]Cracker, ou pirata digital, é a pessoa especialista em sistemas informatizados, que invade sistemas alheios, sem autorização. Porém, seu objetivo é adulterar programas e dados, furtar informações e valores e praticar atos de destruição deliberada. O cracker destaca-se por ser autor de grandes fraudes eletrônicas, que causam expressivos prejuízos a usuários privados e às instituições públicas.

[205]pheackers, especializados no ramo de telefonia e que atacam os sistemas de telecomunicação (móvel ou fixa): "são aqueles indivíduos especialistas nos famosos 'gatos de telefonia', que realizam ligações clandestinas de telefone, ou mesmo praticam a clonagem de linhas telefônicas, fixas ou móveis.

[206]Cardes é a denominação que se dá aos criminosos que se apropriam do número de cartões de crédito, obtidos através de invasão de listas eletrônicas constantes nos sites de compras efetivadas pela Internet, ou de outros meios ilícitos para realizar toda a espécie de compras. Eles conhecem o número dos cartões de crédito dos usuários da rede, normalmente a partir da instalação de programas espiões, capazes de permitir o acesso a todo tipo de informação digitada no teclado do computador do usuário.

[207]cyberterrorists indica a atividade ilícita daquele que desenvolve bombas lógicas ou vírus com o intuito de "sabotar computadores e provocar a queda do sistema de grandes provedores, impossibilitando o acesso de usuários, gerando grandes prejuízos econômicos".

[208]FIORILLO, Celso Antônio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788547204198/. Acesso em: 10 out. 2022.

O *Hacker* possui uma habilidade técnica para conhecer e alterar todo e qualquer dispositivo eletrônico e programa, na maioria das vezes, eles são jovens estudantes que invadem sistemas informáticos alheios, motivados principalmente pela curiosidade, para satisfazer o próprio ego.[209]

Já os *crackers* são os indivíduos especializados em invadir sistemas alheiros, de forma ilegal e antiética, com o objetivo de causar um dano a vítima, subtraindo informações do computador da mesma, programas e dados.[210]

Um dos grandes aliados na aplicação de golpes virtuais são hoje os computadores alheios ou "máquinas zumbis" ou *botnets.*[211] Tanto os invasores estrangeiros estão recrutando no Brasil máquinas para atacar instituições financeiras em seu País de origem como os invasores brasileiros vêm recrutando máquinas zumbis no exterior para atacar empresas e bancos aqui.[212]

Os *pherakers* são especialistas em telefonia, que exclusivamente visam fraudar sistemas de telecomunicações, utilizando de linhas telefônicas convencionais, ou de aparelhos celulares que são clonados para a realização de ligações clandestinas, facilitando o ataque a sistemas externos, dificultando assim o rastreamento.[213]

Os *cardes* são indivíduos que se apropriam dos números de cartão da vítima, que são subtraídos de *sites* de compras pela *internet*, utilizando de programas de espiões que são instalados no momento do acesso ao site, no computador da vítima. [214;215]

---

[209]NASCIMENTO, 2022.

[210]*Ibidem*.

[211]"O nome se refere a computadores caseiros controlados remotamente por um invasor para cometer crimes, sem que seu dono desconfie. Redes com mais de 100.000 computadores zumbis sob o comando de um único criminoso já foram detectadas nos Estados Unidos e na Europa. É um exército que trabalha de forma sincronizada e pode enviar spams, invadir sites num ataque coletivo ou até hospedar material ilícito ou pornográfico. O computador escravizado também pode entregar os dados pessoais de seu dono, como contas bancárias, senhas ou número de cartão de crédito digitados no teclado. O golpe não é novo, mas cresce de forma perturbadora no Brasil. Uma pesquisa da empresa de segurança digital Symantec, divulgada em outubro, mostra que o País tem praticamente a metade dos computadores zumbis da América Latina, algo em torno de 140.000 máquinas aliciadas. São 3% do total mundial, número inferior ao da China (20%), dos EUA (19%), mas que nos coloca à frente de países como Itália, Índia e Israel. Na prática, em vez de um único computador para aplicar o golpe, o criminoso passa a contar com milhares de ciberlaranjas para executar o trabalho sujo. Isso fez com que usuários domésticos se tornassem um dos pontos mais vulneráveis da segurança na internet hoje. O crescimento das redes zumbis no Brasil está ligado ao número de computadores conectados à internet banda larga – cerca de 4,7 milhões – que são mais úteis aos criminosos pela rapidez na navegação e pelo tempo que ficam conectados." BORTOLOTI, Marcelo. Sua Máquina a serviço do crime. **Revista Veja,** Ed. Abril, n. 44, ano 39, p. 134-135, 8 nov. 2006.

[212]Contra as redes zumbis foi criada em 2005 uma Força Internacional – a International Botnet Task Force, cuja ideia era trazer soluções para esse tipo de ataque e encurtar o tempo de ação da polícia. "Para desmantelar uma botnet é preciso fazer o caminho inverso. Só que essas redes contêm centenas de intermediários, de diferentes lugares do mundo. E para rastrear tudo isso, é necessária uma ordem judicial que pode demorar cerca de dois anos", explica Paulo Quintiliano, na IV Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber), em palestra ocorrida em 26 de setembro de 2007, evento realizado no Guarujá – SP.

[213]NASCIMENTO, *op. cit*., p. 26.

[214]FIORILLO; CONTE, 2016.

[215]NASCIMENTO, 2022, p. 26.

Dessa forma, observa-se que esses *cybers* terroristas desenvolvem vírus de computadores, cada qual da sua forma.

7.4 Tempo, Local do Crime e Competência

A grande dificuldade acerca dos crimes informáticos, se dá na hora de indicar exatamente o momento da prática do ato ilícito, para que se possa ser aplicada a sanção penal.

No meio informático existe uma dissociação temporal, sendo possível programar a execução de um crime no tempo, ou seja, o ato ilícito é programado para ser executado após alguns meses, isso se dá ao fato de que todo computador possui um relógio interno.[216]

Diante dessa situação, o Código Penal adotou a teoria da atividade para poder descrever o momento do crime, sendo que neste momento ocorreu na ação ou omissão, independentemente do momento em que de fato se deu o resultado.[217]

Contudo, no ciberespaço não existe um espaço físico que seja predeterminado ou que seja delimitado, assim para que seja realizada a constatação da prática de um crime informático é necessário detectar a localização da informação, sendo essencial para proporcionar a ideia de território. [218]

O espaço virtual a qual denominamos de ciberespaço nos indica o local onde ocorre todo o fluxo de informações através das redes de comunicações, desta forma, grande parte dos crimes virtuais vão além de fronteiras territoriais, não existe uma legislação processual penal nacional para esta matéria, sendo necessário que seja aplicado alguns princípios do nosso Código Penal Brasileiro, mais precisamente o da territorialidade, extraterritorialidade, nacionalidade, defesa e representação.

O Código Penal trata do lugar do crime, determinando a possibilidade de aplicação ou não da lei penal brasileira, em seu art. 6º: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Dessa forma, qualquer fragmento de conduta que tenha tocado o solo nacional desafia a aplicação da lei penal pátria. Trata-se da adoção da denominada teoria da ubiquidade aplicada pela maioria dos países do mundo e que leva em consideração tanto o momento executivo quanto o consumativo do crime.[219]

---

[216]*Ibidem*.
[217]*Ibid*..
[218]*Ibid*., p. 27.
[219]FIORILLO; CONTE, 2016.

O Princípio da Territorialidade se encontra previsto no art. 5º do Código de Processo Penal, determinando que seja aplicado a lei penal brasileira a todos os crimes executados em território nacional, sem prejuízo das normas, convenções e tratados de Direito Internacional.[220]

Já o Princípio da Extraterritorialidade, nacionalidade, defesa e representação, se encontram previstos no art. 7º do Código Penal, que conduz a extraterritorialidade da lei penal nacional, determinando a aplicação da nossa legislação penal para os crimes praticados fora do nosso território.[221]

Dessa forma, mesmo que o crime tenha ocorrido no exterior, a lei penal brasileira poderá ser aplicada diante das seguintes hipóteses:[222]

1º - Quando o indivíduo for brasileiro;

2º - Quando o bem lesionado for brasileiro, seja este objeto ou pessoa;

3º - Quando o crime for transnacional, e o Brasil comprometido a reprimir tal conduta criminosa, através de tratados ou convenções;

4º - Quando o crime ocorrer no interior de aeronaves ou embarcações brasileiras, mercantis ou de propriedade privada, ainda que em território estrangeiro, caso não tenha sido julgado.

Ressalta-se, que caso seja caracterizado o caso de extraterritorialidade condicionada, devem ser respeitados os requisitos previstos no Art. 7, §§ 2º e 3º do Código Penal Brasileiro.

Com relação ao lugar do crime, o código penal adotou a teoria da ubiquidade, que define o local do crime onde ocorreu a ação ou omissão, em todo ou em parte, bem como onde se produziu o resultado. Portanto, qualquer tipo de Cibercrime que tenha ocorrido em todo ou em parte em nosso território nacional, poderá ser objeto da aplicação da legislação penal brasileira.[223]

Deste modo, ao se considerar alguém, no Estado do Paraná, que invade o computador de outrem, localizado Santa Catarina, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático.

Já nos crimes em que a ação/omissão e o resultado ocorrem em comarcas diferentes, o direito brasileiro adota a Teoria do Resultado, já apresentada acima.[224]

---

[220]FRANÇA, Leandro Ayres. **Lei Penal no espaço**. Disponível em: https://www.cafeefuria.com/ayresfranca/02_Lei_penal_no_espaco_v1.pdf. Acesso em: 10 set. 2022.
[221]QUANDT, Gustavo de Oliveira. **Artigo**. Disponível em: https://www.ibccrim.org.br/noticias/exibir/7323/. Acesso em: 11 set. 2022.
[222]NASCIMENTO, 2022.
[223]TRILHANTE. **Lugar do crime**. Disponível em: https://trilhante.com.br/curso/lei-penal-no-tempo-e-espaco/aula/lugar-do-crime-2. Acesso em: 10 de setembro de 2022.
[224]TRILHANTE, 2022.

Já no que diz respeito a condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deverá ser tratada pela extradição.[225]

De modo esclarecedor, Damásio Evangelista de Jesus[226] entende que, para casos relacionados à internet, deveria ser adotado algo semelhante à teoria da atividade que, como visto, determina como sendo o local do crime aquele em que o agente praticou o delito.

Pensamento contrário é defendido por Valin, que acredita ser a melhor solução considerar-se como local do crime aquele em que está o autor das infrações, pois o referido país teria melhores condições de aplicar eventual pena, sem necessidade de discussão sobre extradição, no máximo se discutiria o cumprimento dos efeitos cívis da condenação no sentido de retirar da rede o material publicado, o que talvez possa gerar a necessidade de um novo processo em país distinto ao da condenação.[227]

Importa dizer ainda que, nos termos do §2° do art. 70 do código de Processo Penal, quando atos executórios tenham ocorrido fora do Brasil, a competência será do local onde a infração se deu ou foi concluída a ação delituosa (resultado). Sobre o assunto o STJ diz que a competência será, de regra, determinada pelo lugar em que se consumar a infração.[228]

Com relação a competência a maioria dos casos é de responsabilidade da Justiça Federal, tendo em vista o predominante sentido transnacional do crime, assim no art. 109 da CF 88, nos traz as hipóteses em que há a competência da JF em processar e julgar a pratica de determinados crimes, principalmente contra a Administração Pública Federal que ultrapassem as fronteiras.

Sendo os crimes de racismo e de pedofilia praticados pelo meio virtual, são expressamente processados e julgados pela JF, por expressão previsão em convenções internacionais de direitos humanos.[229]

Já os crimes contra a honra, praticados por meio virtual, devem ser processados e julgados pela Justiça Estadual.

---

[225]RAMOS, Lucas de Oliveira; OLIVEIRA, Christian Santos; SANTOS, Bruno Ribeiro dos; BEZERRO, Eduardo Buzetti Eustachio. **A competência penal nos cybercrimes**. Disponível em: http://www.unoeste.br/site/enepe/2017/suplementos/area/Socialis/01%20-%20Direito/A%20COMPET%C3%8ANCIA%20PENAL%20NOS%20CYBERCRIMES.pdf. Acesso em: 10 set. 2022.

[226]*Ibidem*, p. 117.

[227]*Ibid*.

[228]*Ibid*.

[229]NASCIMENTO, 2022.

7.5 A Escassa Previsão Legal quanto a Prática de Cibercrimes via *Internet*

As condutas ilícitas praticadas pela internet causam inúmeras dificuldades práticas na hora de punir os infratores, pois mesmo que existam legislações que tipificam as condutas, ainda existem inúmeras impunidades pela prática de condutas ilícitas e antiéticas no âmbito virtual.

A Lei do Marco Civil (lei nº 12.695/2014) trouxe grandes avanços relacionados ao uso da internet, pois institui deveres e direitos aos usuários da *internet*.[230]

Mas com o grande crescimento da criminalidade na informática, ainda é maior do que a prevenção e evolução legislativa quando o regulamento da matéria, assim no brasil aplicamos a legislação penal vigente, pelo meio do enquadramento jurídico, que em grande parte não regulam especificadamente a matéria, como o crime contra a honra e ameaça, além do furto de valores de conta bancaria, preconceito e discriminações, e a pornografia infantil.[231]

Podemos ver então que é necessário a regulamentação especificamente de cada conduta ilícita praticada nos meios virtuais para que seja reduzido o número de lacunas legislativas relacionadas aos crimes virtuais.

[230] *Ibidem*.
[231] *Ibid*., p. 29.

8 COMO EVITAR CAIR NOS CRIMES CIBERNÉTICOS

Dessa forma, podemos observar que os crimes virtuais podem ser praticados por qualquer indivíduo, mais principalmente por especialistas como os craques e *cyber* terroristas, deve-se tomar cuidado para não ser uma vítima desses crimes, tomando precauções para que o dispositivo eletrônico não seja invadido, ou caso isso venha a acontecer, providenciar o resguardo das provas.

É necessário manter o computador protegido com um programa de antivírus sempre atualizado, que irá impedir ou ao menos dificultar a invasão do computador por terceiros, detectando e eliminando qualquer vírus que for localizado, também, é necessário se policiar a respeito dos sites que pretende visitar, devendo analisar primeiramente se é de confiança.[232]

Os crimes que são frequentemente praticados virtualmente são:[233]

> - Roubo de identidade e senha: são utilizadas para efetuar compras online e até mesmo transações financeiras de forma indevida.
> - Falsa identidade: uma pessoa omite/mente sobre suas características para tirar proveito de outro indivíduo.
> - Calúnia ou difamação: sendo a divulgação de informações falsas sobre alguém, que podem por ventura prejudicar a vítima.
> - Pirataria, cópia ou reprodução de livros, músicas, imagens e softwares de empresas sem a devida autorização do proprietário.
> - Discriminação: é toda divulgação de informações com caráter preconceituoso sobre a cor de pele, sexo, orientação sexual, religião e nacionalidade.
> - Pedofilia: é o abuso sexual infantil, que geralmente são possibilitados através de sites ou rede sociais.

No Brasil a Difamação fica como a primeira colocada nos casos de crimes virtuais, segundo o advogado Jair Jaroleto, especialista em Direito Penal e crimes na *internet*, que diz: "Isso porque as pessoas esquecem que escrever nas redes sociais é similar a escrever em um *outdoor*".[234] Vale ressaltar também que estão sendo criadas novas legislações para combater com mais vigor os crimes, o treinamento para capacitação mínima do pessoal que trabalha com investigação desses tipos penais também é de suma importância, a cooperação policial de todas

[232]NASCIMENTO, 2022.

[233]TECMUNDO. **Crime Virtual**: o que é e como se proteger das ameaças. Disponível em: https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm. Acesso em: 31 jul. 2022.

[234]ZVARICK, Leonardo; CASTRO, Mariangela de. **Compartilhar conteúdo sem autorização é crime e dá cadeia**. Disponível em: https://agora.folha.uol.com.br/sao-paulo/2019/06/compartilhar-conteudo-sem-autorizacao-e-crime-e-da-cadeia.shtml. Acesso em 30 jul. 2022.

as instâncias, inclusive a polícia internacional, entre outras soluções que são necessárias para acompanhar o desenvolvimento dos crimes na *internet*.[235]

Já por outro lado, caso alguma pessoa foi vítima de ofensas praticadas na *internet*, é necessário que se preserve todas essas provas, visto que no ambiente virtual as páginas podem ser modificadas ou tiradas do ar a qualquer momento, o que de fato, pode acarretar grandes dificuldades nas investigações para punir o infrator.

Quando o crime informático deixar vestígios que se substanciam em ilícitos materiais, deve ser realizada uma perícia para analisar todas as provas e demonstrar a materialidade e autoria do crime.[236]

A legislação aplicada atualmente é insuficiente para coibir os crimes, além das penas serem brandas, e a investigação é pouca, chegando às vezes em ter a comprovação do delito, mas sem a localização do criminoso.[237]

Desta forma, é necessário tomar todas as providencias possíveis para evitar ser vítima de qualquer crime informático, e caso isso ocorra, deve ser todas as provas preservadas para facilitar as investigações e consequentemente punir os infratores que praticaram o ato ilícito.[238]

O *site* chamado Norton Symantec Corporation, sendo um *site* provedor de antivírus trouxe algumas dicas de como se prevenir: [239]

1. Manter seu computador atualizado com os *patches*[240] e atualizações mais recentes de antivírus;

2. Versões de dispositivos mais recentes podem ser configuradas para fazer download[241] automaticamente dos *softwares*, assim você não precisa se lembrar de verificar a disponibilidade do *software* mais recente;

3. Configuração de aplicativos da *internet*;[242]

---

[235]TORMEN, 2022.
[236]NASCIMENTO, 2022, p. 30.
[237]TORMEN, *op. cit*., p. 31.
[238]NASCIMENTO, *op. cit*.
[239]NORTON SECURITY. **Como reconhecer e se proteger contra o crime cibernético**. [2017]. Disponível em: https://br.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime. Acesso em: 31 jul. 2022.
[240]Patch – Um patch é um arquivo que contém apenas as mudanças feitas pela atualização e, justamente por isso, é sempre muito pequeno se comparado ao arquivo original. Ele é obtido comparando a versão anterior com a nova (com a ajuda de algum programa naturalmente). Ao ser aplicado, o patch modifica o programa, "transformando-o" na versão corrigida. MORINOTO, Carlos. **Definição de Patch**. [2016]. Disponível em: https://www.hardware.com.br/termos/patch. Acesso em: 30 jul. 2022.
[241]Download – significa transferir "baixar". Em um ambiente de rede, receber arquivos de dados de outro computador, provavelmente de um computador maior ou de um computador host.
[242]A configuração de aplicativos da Internet, como o navegador da Web e o programa de e-mail, é uma das áreas que merece mais atenção. Por exemplo, algumas configurações no seu navegador da Web (como o Internet Explorer ou Firefox) determinarão o que acontece quando você acessa sites na Internet. As configurações de segurança mais rigorosas proporcionarão maior controle sobre o que acontece on-line, mas podem também

4. Senhas complexas: sempre realizar a manutenção das senhas;

5. Instalação de *softwares* de segurança em seu dispositivo, e deduz que são necessários vários tipos de softwares de segurança para obter uma segurança *on-line* básica;

6. Proteção das informações pessoais: o que consiste em evitar de compartilhar dados pessoais, como seu nome completo, endereço residencial, telefones, e documentações, para com vantagens de serviços *online;*

7. Verificar os extratos bancários e extratos de cartão de crédito regularmente: sendo um bom exemplo a ação dos criminosos que hackeiam várias contas do banco e retira R$ 0,01 centavo de cada conta, no final dá um montante monstruoso, que os clientes nem vão atrás devido a quantia", fazendo que os bancos deixem passar despercebidos, mas os impactos são enormes de furtos através dos crimes cibernéticos à agências de bancos.

E segundo a dica do *site Norton Security*, reduz drasticamente se for efetuada nos conformes:

> O impacto de um roubo de identidade e crimes on-line pode ser reduzido significativamente se eles forem detectados logo após o roubo dos dados ou quando ocorrer a primeira tentativa de uso das informações. Uma das maneiras mais fáceis de descobrir se alguma coisa está errada é procurando transações incomuns nos extratos mensais fornecidos pelo seu banco ou operadora de cartão de crédito. Além disso, vários bancos e serviços utilizam sistemas de prevenção contra fraudes que chamam a atenção para compras fora do comum (por exemplo, se você mora no Texas e de repente começa a comprar refrigeradores em Budapeste). Para confirmar essas compras fora do comum, eles poderão entrar em contato com você para que você possa confirmá-las pessoalmente. Não ignore essas chamadas. Elas indicam que alguma coisa errada pode estar acontecendo e você deve considerar alguma das atividades mencionadas na seção sobre como reagir, caso se torne uma vítima.[243]

Seguindo todas essas dicas do *site Norton*, o acesso do *cyber* criminoso ao computador ou outros aparelhos eletrônicos desses indivíduos, seria dificultoso, pois o mesmo estaria protegido contra esse indivíduo, mas sua garantia não é de 100%.

causar frustração em algumas pessoas, com um volume exagerado de perguntas do tipo "Isso pode não ser muito seguro, deseja realmente seguir em frente?" ou a incapacidade de fazer o que desejam. A seleção do nível apropriado de segurança e privacidade depende de cada usuário do computador. Muitas vezes, as configurações de privacidade e segurança podem ser definidas adequadamente sem nenhum conhecimento especial. Basta usar o recurso "Ajuda" do seu software ou ler as informações contidas no site do fornecedor. Caso não se sinta à vontade para definir essas configurações sozinho, consulte alguém conhecido em quem você confie para obter assistência ou entre em contato diretamente com o fornecedor. NORTON SECURITY, 2017.

[243] *Ibidem*.

8.1 Quais Procedimentos tomar se sofreu Crime Cibernético

Com a falta de orientação, conhecimento e até mesmo medo, diversas pessoas que sofrem crimes, não denunciam os casos, apesar de ser um assunto comum os crimes virtuais as pessoas parecem não se dar conta do crime acontecendo, e acaba não tomando a providência necessária, assim sendo é de suma importância realizar a denúncia, pois desta forma podemos contribuir para que esses crimes diminuam.

No *site* Direitos Brasil, vemos um passo a passo de como proceder caso sofra um crime cibernético.[244]

O primeiro passo consiste na coleta de informações, ou seja, reunir as informações e dados do crime, a vítima deve salvar tudo que pode auxiliar a provar o crime cometido, desde *e-mails*, *prints*, dados do criminoso, conversas em redes sociais. Sendo assim, nessa etapa é essencial armazenar todos os materiais e arquivos que comprovem o crime.

O segundo passo é o Registro, após coletar todas as informações relacionadas ao crime, a vítima deve dirigir-se a um cartório e registrar esses arquivos em uma ata notarial. Essa ata é um instrumento público que registra os documentos e declara a veracidade deles, ou seja, confirma que os documentos são verdadeiros.

Por último temos a realização do Boletim de Ocorrência (BO), também está relacionada a um registro, que deve ser realizado em delegacias de polícia. A vítima do crime deve dirigir-se a uma delegacia de polícia e registrar um boletim de ocorrência sobre o ocorrido. Algumas cidades no país possuem Delegacias Especializadas em Crimes Cibernéticos, mas esse registro pode ser feito em qualquer delegacia por todo o país. O boletim de ocorrência é um documento fundamental no processo de denunciar um crime virtual, pois permite que seja instaurado um inquérito policial para realizar a apuração do crime, ou seja, a investigação.[245]

Portanto, seguindo esse rito de procedimentos, se a pessoa vier à sofrer com crimes cibernéticos, a primeira hipótese a fazer é coletar as provas, para tentar saber a veracidade e a autoria do fato, deste sim, o segundo passo é a vítima procurar um Cartório de Registros para efetuar uma Carta Notarial, a qual deverá ser autenticada por um agente público, dando assim fé pública no documento, e o terceiro e último passo é procurar uma Delegacia de Polícia para

[244]DIREITOS BRASIL. **Como denunciar um crime virtual passo a passo**. Disponível em: https://direitosbrasil.com/denunciar-um-crime-virtual-passo-passo/#:~:text=O%20primeiro%20passo%20para%20denunciar,em%20redes%20sociais%2C%20entre%20outros. Acesso em: 02 ago. 2022.
[245]*Ibidem*.

efetuar o Boletim de Ocorrência (BO), pedindo a representação ao Ministério Público, para dar prosseguimento a Ação Penal Pública.[246]

Bem como também é fundamental procurar um advogado, se possível especialista em crimes cibernéticos, para que tome as medidas cabíveis para buscar a reparação do delito.

[246]DIREITOS BRASIL, 2022.

9 CONCLUSÃO

Dessa forma, observa-se que a internet é um importante meio de comunicação, tendo um aumento muito grande com o passar dos anos, devido aos inúmeros indivíduos que utilizam essa ferramenta para compartilhamento de informações pessoais ou comerciais.

Sendo assim, da mesma forma que a *internet* proporciona muitos benefícios, também, possibilita a pratica de atos ilícitos que prejudicam de diversas formas os usuários conectados à rede.

Diante desses delitos deve haver uma resposta do Estado, para tentar coibir essa modalidade de crime, sendo a formulação da tipificação penal, com isso temos a criação da Lei 12.735/12, chamada como a Lei Carolina Dieckmann que foi um grande avanço para o Direito Penal, mais possui uma tipificação muito lesada, devendo ser revista de modo a ser mais rigorosa e ampliada.

Mesmo com o avanço que ocorreu na criação da Lei 12.965/14, chamada de Marco Civil da *Internet* que surgiu para regular as translações internacionais, sendo um grande aliado no combate às ações delitivas digitais, o Brasil se encontra em desvantagem com os outros países, sendo considerado um "país de terceiro mundo", nos países elencados como de primeiro mundo, com a existência de pactos, um deles e a Convenção de Budapeste, que trata dos crimes cibernéticos de forma mais branda.

Essa convenção não teve a participação Brasileira, pois foi criada por países da Europa, e o único país da América que foi convidado a participar dessa convenção foi os Estados Unidos da América.

No Brasil, recentemente foi aprovado a Lei n. º 12.695/2014, popularmente conhecida como Marco Civil da *Internet*, que trouxe inúmeros avanços quanto aos direitos e deveres dos usuários e provedores da internet, porém, infelizmente, por si só ainda não é suficiente ao combate aos crimes cibernéticos que crescem de forma extraordinária.

Destaca-se que a maioria desses crimes é praticada por *softwares* criminosos, como: *spyware*, *spammings*, *hoaxes*, *sniffer*, cavalo de troia, *backdoors*, vírus e *Worm*. Esses crimes podem ser praticados por qualquer pessoa, contudo, existem indivíduos específicos que praticam esses atos, sendo eles os: *hackers, craker, pherakers*, *cardes* e *cyberterrorists*.

Comtemplamos a grande dificuldade em se indicar com precisão o tempo e o local do crime, pois, no âmbito virtual não existem espaços físicos predeterminados e não é possível programar a execução do crime no tempo, desta forma, é essencial a identificação da

localização da informação, pois a partir desta constatação proporciona a ideia de território, para que seja aplicada a sanção penal competente.

A principal medida para não se cair nesses crimes cibernéticos e a prevenção, ou seja, caso tenha dúvida na hora de abrir arquivos que sejam suspeitos, não abra os arquivos, ou quando tiver certeza de que um site, ou arquivo estiver vírus, denuncie para que outras pessoas não criam, caso o crime for de cunho pessoal cito injúria, calúnia, exposição de imagens constrangedoras, ou até mesmo crimes sexuais, a única saída é buscar o judiciário para resolver as questões de forma justa.

É necessário assim a regulamentação de leis específicas para o combate ao crime cibernético, bem como deve haver investimentos para a proteção na segurança das informações dos dados dos usuários.

REFERÊNCIAS

ABDALLA, Samuel L.; GUESSE, André. **Informática para Concursos.** São Paulo: Saraiva, 2012. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502180642/. Acesso em: 25 set. 2022.

ALEXANDRE JUNIOR, Júlio Cesar. Cibercrimes: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso em: 25 jun. 2022

ALMEIDA, Jessica de Jesus. **Crimes cibernéticos**. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/download/2013/1217. Acesso em: 22 jun. 2022.

ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes do Direito**. Disponível em: https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/23590106.2017v4n2p191#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime. Acesso em: 27 ago. 2022.

BECCARIA, Cesare. **Dos delitos e das penas**. Tradução: Torrieri Guimarães. 2. ed. São Paulo: Martin Claret, 2008.

BELL. **Índices para catálogo sistemático**: Informática e criminalidade: Direito penal. [1979]. Disponivel em: https://docplayer.com.br/69154805-Isbn-indices-para-catalogo-sistematico-1-informatica-e-criminalidade-direito-penal-004-3.html. Acesso em: 25 jul. 2022. p. 169.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte geral. 19. ed. São Paulo: Saraiva, 2013. v. 1.

BOLQUE, Elisa. **Modus operandi**. Disponível em: https://direito.legal/dicionario-juridico/modus-operandi-significado/. Acesso em: 25 jun. 2022.

BORTOLOTI, Marcelo. Sua Máquina a serviço do crime. **Revista Veja,** Ed. Abril, n. 44, ano 39, p. 134-135, 8 nov. 2006.

BRANCO, Jose Ricardo Marques. **Prova digital os meios de obtenção de prova digital e a restrição de direitos do arguido.** Disponível em: https://estudogeral.sib.uc.pt/retrieve/203656/Disserta%C3%A7%C3%A3o%20-%20Jos%C3%A9%20Ricardo%20Marques%20Branco%20-%20uc2012153587%20-%20pdf.pdf. Acesso em: 01 set. 2022.

BRASIL. Senado Federal. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. Disponivel em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em: 10 ago. 2022.

BRASIL. Superior Tribunal da Justiça. **Lei 14.555/2021 só alterou competência para julgamento de estelionato em casos específicos**. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30052022-Lei-14-5552021-so-alterou-competencia-para-julgamento-de-estelionato-em-casos-especificos.aspx. Acesso em: 30 set. 2022.

BRASIL. Supremo Tribunal Federal. **A Interceptação Telefônica como meio de prova**. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-10-08_08-00_A-interceptacao-telefonica-como-meio-de-prova.aspx. Acesso em: 30 ago. 2022.

BRASIL. Supremo Tribunal Federal. **AgRg no recurso em habeas corpus nº 92.801 - SC (2017/0322640-7).** Relator: Ministro Felix Fischer. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1689703&num_registro=201703226407&data=20180326&formato=PDF. Acesso em: 18 jul. 2022.

BRASIL. Supremo Tribunal Federal. **Conflito de competência nº 133.534 - SP (2014/0094026-9).** Relator: Ministro Reynaldo Soares da Fonseca. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1459186&num_registro=201400940269&data=20151106&formato=PDF. Acesso em: 18 jul. 2022.

BRASIL. Supremo Tribunal Federal. **Conflito de competência nº 145.576 - MA (2016/0055604-1)**. Relator: Ministro Joel Ilan Paciorni. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1503783&num_registro=201600556041&data=20160420&formato=PDF. Acesso em: 18 jul. 2022.

BRASIL. Supremo Tribunal Federal. **Conflito de competência nº 156.284 - PR (2018/0008775-5).** Relator: Ministro Ribeiro Dantas: Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1680838&num_registro=201800087755&data=20180306&formato=PDF. Acesso em: 18 jul. 2022.

BRASIL. Supremo Tribunal Federal. **Recurso em habeas corpus nº 79.848 - PE (2017/0000411-6).** Relator: Ministro Nefi Cordeiro. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1735277&num_registro=201700004116&data=20180903&peticao_numero=-1&formato=PDF. Acesso em: 18 jul. 2022.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502209428/. Acesso em: 24 ago. 2022.

CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet**. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-deinternet/. Acesso em: 26 jul. 2022.

CARLOS, Heder Sabino. **Computação na nuvem (cloud computing).** Disponivel em: https://www.metodoconcursos.com.br/2021/02/computacao-na-nuvem-cloud-computing.html. Acesso em: 29 jul. 2022.

CAVALCANTE, Gercina Alves Moraes. **A relativização do princípio da presunção de inocência frente ao cumprimento antecipado da pena**: análise jurisprudencial. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/22546/1/INACIO%20E%20RENATO%20dep%C3%B3sito.pdf. Acesso em: 08 set. 2022.

CONAB. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.conab.gov.br/lei-geral-de-protecao-de-dados-pessoais. Acesso em: 20 ago. 2022.

CONSULTOR JURÍDICO. **STF derruba decisão judicial e libera volta do WhatsApp**. Disponível em: https://www.conjur.com.br/2016-jul-19/stf-derruba-decisao-judicial-libera-voltawhatsapp#:~:text=Por%20identificar%20viola%C3%A7%C3%B5es%20%C3%A0s%20liberdades,feira %20(19%2F7). Acesso em: 26 jun. 2022.

COSTA, Fernando José da; COSTA JÚNIOR, Paulo José da. **Código penal comentado**. São Paulo: Saraiva, 2011. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502133914/. Acesso em: 24 out. 2022.

COTS, Márcio; OLIVEIRA. Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. [*S.l.*]: [*s.n.*], [20--].

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista científica eletrônica do curso de direito**, 13. ed., 2019. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 20 ago. 2022.

DIANA, Daniela. **História da internet**. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 10 ago. 2022.

DIREITOS BRASIL. **Como denunciar um crime virtual passo a passo**. Disponivel em: https://direitosbrasil.com/denunciar-um-crime-virtual-passo-passo/#:~:text=O%20primeiro%20passo%20para%20denunciar,em%20redes%20sociais%2C%20entre%20outros. Acesso em: 02 ago. 2022.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos**: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso em: 25 jun. 2022.

DURBANO, Vinicius. **Computação em nuvem:** tudo que você precisa saber sobre. Disponível em: https://blog.ecoit.com.br/computacao-em-nuvem/. Acesso em: 28 jul. 2022.

FARIAS, Dermeval. **Direito Penal Parte Geral**: Princípios Penais e Jurisprudência do STF e STJ. Disponível em: file:///C:/Users/MARCIELE%20FERREIRA/Downloads/38021265-principios-penais-e-jurisprudencia-do-stf-e-stj.pdf. Acesso em: 15 jul. 2022.

FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil**. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil. Acesso em: 21 ago. 2022.

FIORILLO, Celso Antônio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788547204198/. Acesso em: 10 out. 2022.

FRANÇA, Leandro Ayres. **Lei Penal no espaço**. Disponível em: https://www.cafeefuria.com/ayresfranca/02_Lei_penal_no_espaco_v1.pdf. Acesso em: 10 set. 2022

FREIRE, Andre Luiz; KUJAWSKI, Fabio. **Tratamento e classificação de informações em nuvem e a Lei de Acesso à Informação**. Disponível em: https://www.convergenciadigital.com.br/Opiniao/Tratamento-e-classificacao-de-informacoes-em-nuvem-e-a-Lei-de-Acesso-a-Informacao-61250.html. Acesso em: 29 jul. 2022.

FREITAS, Cristiano. **Lei de softwares**: 4 pontos que sua empresa precisa se atentar. Disponivel em: https://syhus.com.br/2019/09/24/le-de-software/#:~:text=A%20lei%20n%C2%BA%209.609%20de,versa%20sobre%20aspectos%20mais%20autorais. Acesso em: 30 ago. 2022.

FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** Disponível em: https://flucianofeijao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf. Acesso em: 26 jul. 2020.

GARCEZ, Willian. **Lei 14.132/21**: A tipificação do crime de perseguição (stalking). Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/04/28/lei-14-13221-tipificacao-crime-de-perseguicao-stalking/. Acesso em: 05 set. 2022.

GOMES, Caio. **Princípios do Direito Penal**: resumo e jurisprudência. Disponível em: https://www.direcaoconcursos.com.br/artigos/principios-do-direito-penal-resumo-e-jurisprudencia/. Acesso em 20 ago. 2022.

GOMES, Genevieve Aline Zaffani Grablauskas. **Princípios do Direito Penal Brasileiro**. Disponivel em: https://semanaacademica.org.br/system/files/artigos/principios_do_direito_penal_brasileiro.pdf. Acesso em: 25 jul. 2022.

GREGO, Rogerio. **Curso de Direito Penal**: Parte Geral. 18. ed. Niterói, RJ: Impetus, 2016.

HAJE, Lara. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas.** Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/. Acesso em: 20 ago. 2022.

JESUS, Damásio D.; MILAGRE, José A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 25 set. 2022.

JESUS, Damásio Evangelista D.; OLIVEIRA, José Antônio M.; MILAGRE, D. **Marco Civil da Internet**: comentários à Lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 25 ago. 2022.

JOANONE, Bruno. **Crimes virtuais e a necessidade de uma legislação especifica**. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/49970/crimes-virtuais-e-a-necessidade-de-uma-legislacao-espeficica. Acesso em: 25 jun. 2022.

JOVELINO, Luiz. **Lei 14155 2021**: Lei que amplia penas para crimes cibernéticos é sancionada. Disponível em: https://blconsultoriadigital.com.br/lei-14155-2021-crimes-ciberneticos/. Acesso em: 30 ago. 2022.

LUZ, Josuel Pedroso da. **Princípio da exclusiva proteção de bens jurídicos**: como se proteger do direito penal ou quem vigia o vigia? Disponível em: https://jornaltribuna.com.br/2022/07/principio-da-exclusiva-protecao-de-bens-juridicos-como-se-proteger-do-direito-penal-ou-quem-vigia-o-vigia/. Acesso em: 20 ago. 2022.

MELLO, Daniel. **Home Office foi adotado por 46% das empresas durante a pandemia**. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia#:~:text=O%20trabalho%20em%20casa%20foi,atuam%20em%20todo%20o%20Brasil. Acesso em: 10 ago. 2022.

MESQUITA FILHO, Jose Pires. **Crimes Digitais**. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. Acesso em: 25 jun. 2022. p. 49.

MILITÃO, Renato Lopes. **A propósito da prova digital no processo penal**. [*S.l.]:* [*s.n.*], [20--].

MINTO, Rafael. **Saiba tudo sobre o princípio constitucional da reserva legal**. Disponível em: https://masterjuris.com.br/saiba-tudo-sobre-o-principio-constitucional-da-reserva-legal/. Acesso em: 16 jul. 2022.

MORINOTO, Carlos. **Definição de Patch**. [2016]. Disponivel em: https://www.hardware.com.br/termos/patch. Acesso em: 30 jul. 2022.

MORAES, Leticia Hemerly de. **Dos crimes cibernéticos**: uma análise do crime de estelionato praticado pela internet. Disponível em: https://www.jornaljurid.com.br/doutrina/penal/dos-crimes-ciberneticos-uma-analise-do-crime-de-estelionato-praticado-pela-internet#:~:text=A%20nova%20reda%C3%A7%C3%A3o%20da%20lei,servidor%20localizado%20em%20outro%20pa%C3%ADs.. Acesso em: 30 set. 2022.

NASCIMENTO, Natalia Lucas do. **Crimes Ciberneticos**. Disponivel em: https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf. Acesso em: 19 out. 2022.

NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**: Conteúdo Jurídico. Disponível em https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 28 ago. 2022.

NORTON SECURITY. **Como reconhecer e se proteger contra o crime cibernético**. [2017]. Disponível em: https://br.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime. Acesso em: 31 jul. 2022.

NOVO, Benigno Nunez. **O princípio da presunção de inocência**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-171/o-principio-da-presuncao-da-inocencia/. Acesso em: 16 de agosto de 2022.

NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. São Paulo: Grupo GEN, 2021b. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993627/. Acesso em: 26 jun. 2022.

NUCCI, Guilherme de S. **Princípios Constitucionais Penais e Processuais Penais**. 4. ed. São Paulo: Grupo GEN, 2015. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/978-85-309-6296-8/. Acesso em: 25 set. 2022.

NUCCI, Guilherme de S. **Manual de Direito Penal**. São Paulo: Grupo GEN, 2021a. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993566/. Acesso em: 16 set. 2022.

NUCCI, Guilherme de Souza. **Aplicação da Lei Penal Militar**: princípio de legalidade. Disponivel em: http://genjuridico.com.br/2021/04/14/lei-penal-militar-legalidade/. Acesso em: 25 jul. 2022.

O QUE é uma assinatura digital? Disponível em: https://www.adobe.com/pt/sign/digital-signatures.html. Acesso em: 01 set. 2022.

PACHECO, Vitor Pereira. **O crime de perseguição**: breves críticas sobre o stalking no Direito brasileiro. [2021]. Disponível em: https://www.migalhas.com.br/depeso/342950/o-crime-de-perseguicao]. Acesso em: 28 jul. 2022.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. [2000]. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2014;001018201. Acesso em: 25 jul. 2022.

PARDAL, Rodrigo. **Direito penal**: Principios. Disponível em: file:///C:/Users/MARCIELE%20FERREIRA/Downloads/71683560-principios-e1656501927.pdf. Acesso em: 14 jul. 2022.

PETIÇÕES ON LINE. **Tipos de petições**. Disponível em: https://www.peticoesonline.com.br/tipo-de-peticao/notitia-criminis. Acesso em: 29 jul. 2022.

PINHEIRO, Patrícia Pack. **Proteção de Dados Pessoais:** Comentários à Lei 13.709/2018. [*S.l.*]: [*s.n.*], [20--].

QUANDT, Gustavo de Oliveira. **Artigo**. Disponível em: https://www.ibccrim.org.br/noticias/exibir/7323/. Acesso em: 11 set. 2022.

RAMALHO, David da Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. [*S.l.*]: Almedina, 2017.

RAMOS, Lucas de Oliveira; OLIVEIRA, Christian Santos; SANTOS, Bruno Ribeiro dos; BEZERRO, Eduardo Buzetti Eustachio. **A competência penal nos cybercrimes**. Disponível em: http://www.unoeste.br/site/enepe/2017/suplementos/area/Socialis/01%20-%20Direito/A%20COMPET%C3%8ANCIA%20PENAL%20NOS%20CYBERCRIMES.pdf. Acesso em: 10 set. 2022.

RESUMO de Direito Penal: Princípio da lesividade ou da ofensividade. Disponível em: https://www.questoesestrategicas.com.br/resumos/ver/principio-da-lesividade-ou-da-ofensividade#:~:text=Para%20Claus%20Roxin%20%E2%80%9Cum%20conceito,da%20atividade%20punitiva%20do%20Estado%E2%80%9D. Acesso em: 21 ago. 2022.

RNP. Rede Nacional de Ensino e Pesquisa. **Nossa História**. Disponível em https://www.rnp.br/sobre/nossa-historia. Acesso em: 10 ago. 2022.

ROCHA, Kassio Henrique Sobral. **Resumo da Lei de Interceptação Telefônica para a PCRJ.** Disponível em: https://www.estrategiaconcursos.com.br/blog/lei-interceptacao-telefonica/. Acesso em: 03 set. 2022.

ROCKCONTENT. **Descubra finalmente o que é o cloud computing e para que serve a computação em nuvem.** Disponível em: https://rockcontent.com/br/blog/cloud-computing/. Acesso em: 28 jul. 2022.

RODRIGUES, Benjamim Silva. **Direito Penal**: Parte Especial: Direito Penal Informático-Digital. Coimbra (Portugal): Coimbra Ed., 2009.

SANCHES, Ademir Gasques; ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 30 ago. 2022.

SANTANA, Roque Felipe da Silva**. Crimes Cibernéticos**: Análise Evolutiva da Legislação Penal Brasileira e seus Desafios. Disponível em: http://ri.ucsal.br:8080/jspui/bitstream/prefix/4456/1/TCCROQUESANTANA.pdf. Acesso em: 25 jul. 2022.

SANTORO FILHO, Antonio Carlos. **Princípio da Responsabilidade Penal Subjetiva e Responsabilidade Penal da Pessoa Jurídica**. Disponível em: https://www.sedep.com.br/artigos/responsabilidade-penal-da-pessoa-juridica-e-principio-da-responsabilidade-pessoal/#:~:text=O%20princ%C3%ADpio%20da%20responsabilidade%20pessoal,conduta%20apenas%20em%20virtude%20do. Acesso em: 20 ago. 2022.

SANTOS, Karl Heisenber Ferro. **Crimes Digitais**. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. p. 60. Acesso em: 22 jun. 2022.

SANTOS, Rafael Baltazar Gomes dos. **Princípio da lesividade (ou ofensividade).** Disponivel em: http://www.blogladodireito.com.br/2016/05/principio-da-lesividade-ou-ofensividade.html#.yzyixhbmjpy. Acesso em: 20 ago. 2022.

SANTOS FILHO, Antônio Leite dos. **Cartilha Lei Geral de Proteção de Dados Pessoais 2021 – LGPD**. Disponível em: https://www.gov.br/dnit/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-lgpd/cartilha_lgpd_2021.pdf. Acesso em: 21 ago. 2022.

SÃO PAULO. Governo do Estado. **Polícia Civil e Governo do Estado inauguram Divisão de Crimes Cibernéticos**. Disponivel em: https://www.policiacivil.sp.gov.br/portal/faces/pages_home/noticias/noticiasDetalhes?rascunhoNoticia=0&collectionId=358412565221047910&contentId=UCM_056415&_afrLoop=77207818476528&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26collectionId%3D358412565221047910%26_afrLoop%3D77207818476528%26contentId%3DUCM_056415%26rascunhoNoticia%3D0%26_afrWindowMode%3D0%26_adf.ctrl-state%3D99w8trdog_4. Acesso em: 29 jul. 2022.

SENADO NOTÍCIAS. **Sancionada a Lei do Marco Civil da Internet**. Disponível em: https://www12.senado.leg.br/noticias/materias/2014/04/23/sancionada-a-lei-do-marco-civil-da-internet. Acesso em: 25 ago. 2022.

SILVA, Debora Cristina da. **Cibercriminalidade e a (in)suficiência legislativa pátria para a repressão dos crimes cometidos por meio da internet**. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/218882/TCC%20-%20FINAL.pdf?sequence=1&isAllowed=y. Acesso em: 15 jun. 2022.

SILVA, Douglas. **Princípio da Exclusiva proteção do Bem Jurídico.** Disponível em: https://djus.com.br/principio-da-exclusiva-protecao-do-bem-juridico-dp80/#:~:text=Princ%C3%ADpio%20da%20exclusiva%20prote%C3%A7%C3%A3o%20do%20bem%20jur%C3%ADdico%3A,ser%C3%A1%20protegido%20pelo%20direito%20penal. Acesso em: 20 ago. 2022.

SILVA, Eduardo Soares da; BARAKAT, Najah Jamal Daakour. **Crimes Cibernéticos**, **Cyber Crimes**. [2013]. Disponivel em: http://conpedi.danilolr.info/publicacoes/05sx3fe1/3z060c4n/N501YUJ08DF11b96.pdf. Acesso em: 28 jun. 2022.

SILVA, Rita de Cássia Lopes da. U**ma análise da lei de crimes cibernéticos no ordenamento jurídico brasileiro.** Faculdade da Cidade de Maceió Bacharelado em Direito Pedro Henrique Silva dos Santos. 2003. Disponível em: https://www.passeidireto.com/arquivo/102445430/analise-da-lei-de-crimes-ciberneticos. Acesso em: 25 jul. 2022.

SILVA SANTANA & TESTON ADVOGADOS. **Decreto Lei 7.962/2013**; Regulamenta o comercio eletrônico. Disponível em: https://www.sst.adv.br/decreto-7-96213-regulamenta-o-comercio-eletronico/. Acesso em: 05 set. 2022.

SOUZA, Carlos Jeremias Marques. **Os Delitos Informáticos na Internet**. Disponível em: https://repositorio.ufc.br/bitstream/riufc/29334/1/2008_tcc_cjmsousa.pdf. Acesso em: 29 jul. 2022.

SOUZA, Thiago. **História da Internet**: quem criou e quando surgiu. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 25 jul. 2022.

SYDOW, Spencer Toth. **Da necessária relativização do elemento informático perante o princípio da manipulação**. [2022a]. Disponível em: https://s3.meusitejuridico.com.br/2019/08/7913457e-relativizacao-elemento-informatico-principio-manipulabilidade.pdf. Acesso em: 07 set. 2022.

SYDOW, Spencer Toth. **A importância do RHC No 99.735 – SC para o Direito Penal Informático**. [2022b]. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/06/26/importancia-rhc-no-99-735-sc-para-o-direito-penal-informatico/. Acesso em: 08 set. 2022.

T. FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira**. Almedina (Portugal): Grupo Almedina, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556271705/. Acesso em: 19 out. 2022.

TECMUNDO. **Crime Virtual**: o que é e como se proteger das ameaças. Disponível em: https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm. Acesso em: 31 jul. 2022.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais.** [*S.l.*]: [*s.n.*], 2019.

TORMEN, Chalidan Adonai Callegari. **Crimes Cibernéticos**: (IM)possibilidades de coerção. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4078.pdf. Acesso em: 31 jul. 2022.

TRILHANTE. **Lugar do crime**. Disponível em: https://trilhante.com.br/curso/lei-penal-no-tempo-e-espaco/aula/lugar-do-crime-2. Acesso em: 10 de setembro de 2022.

VALVERDE, Danielle Novaes de Siqueira. Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE**, Recife, v. 15, n. 32, p. 236, jul./dez. 2010.

VELLOZO, Jean Pablo Barbosa. **Crimes Informáticos e Criminalidade Contemporânea.** [2015]. Disponível em: https://www.jurisway.org.br/v2/dhall.asp?id_dh=15756. Acesso em: 20 jun. 2022.

VTEX. **Lei do E-commerce – regulamentação pelo Decreto n. 7.962**. Disponível em: https://vtex.com/pt-br/blog/estrategia/lei-do-e-commerce-regulamentacao-pelo-decreto-n-7-962/. Acesso em: 05 set. 2022.

ZVARICK, Leonardo; CASTRO, Mariangela de. **Compartilhar conteúdo sem autorização é crime e dá cadeia.** Disponível em: https://agora.folha.uol.com.br/sao-

paulo/2019/06/compartilhar-conteudo-sem-autorizacao-e-crime-e-da-cadeia.shtml. Acesso em 30 jul. 2022.