SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

CRIMES CIBERNÉTICOS: UMA ANÁLISE SOBRE CONDUTAS CRIMINOSAS NO AMBIENTE VIRTUAL E O TRATAMENTO CONFERIDO PELO ORDENAMENTO JURÍDICO BRASILEIRO.

[ver artigo online]

Isis Rodrigues Fuhr[1]
Cláudia Waléria Carvalho Mendes Macena[2]

RESUMO

Os sistemas informáticos possuem enorme importância no atual momento social. A maioria das pessoas, físicas ou jurídicas, depende do seu dispositivo informatizado, que pode ser um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa, para resolver do mais complexo ao mais simples problema. Nesses dispositivos são armazenadas inúmeras informações que se violadas podem gerar prejuízos de toda ordem. Desse modo, essas pessoas ficam suscetíveis a se tornarem vítimas de crimes praticados por meio da invasão desses equipamentos. Embora na legislação penal já exista a tipificação de condutas como o estelionato, o furto, tais crimes podem ser praticadas tanto fisicamente ou virtualmente, todavia, existem algumas especificidades que precisam estar expressamente contidas na lei. No Brasil foram editadas as leis 12.735/12 e 12.737/12 (denominada Lei Carolina Dieckmann), as chamadas Leis de Crimes Informáticos, que entraram em vigor no ano de 2013, voltadas ao combate dos crimes virtuais, em face do avanço tecnológico e da democratização às redes sociais e, também, por conta da pressão dos meios de comunicação. O presente artigo tem como objetivo geral analisar o tratamento conferido pela legislação brasileira às condutas criminosas praticadas no ambiente virtual. Para isso, torna-se imperioso a compreensão dos novos formatos e arranjos legais quanto aos crimes virtuais; em primeiro lugar, será feito uma abordagem acerca do Direito Penal e sua conceituação; num segundo momento, serão analisados os crimes cibernéticos; por fim, será analisado o tipo penal criado pela Lei Carolina Dieckmann.

PALAVRAS CHAVES: Crimes cibernéticos, tipificação penal, legislação brasileira.

[1] Graduanda do Curso de Direito do Centro Universitário São Lucas/RO. E-mail: isisfuhr@gmail.com.
[2] Docente do Curso de Direito do Centro Universitário São Lucas. Bacharel em Direito. Especialista em Direito Penal e Processo Penal. E-mail: claudia.mendes@saolucas.edu.br

http://dx.doi.org/10.35265/2236-6717-227-12337

ISSN 2236-6717

CYBER CRIMES: AN ANALYSIS OF CRIMINAL CONDUCT IN THE VIRTUAL ENVIRONMENT AND THE TREATMENT GIVEN BY THE BRAZILIAN LEGAL ORDER

ABSTRACT:

Computer systems have enormous importance in the current social moment. Most people, individuals or corporations, depend on their computerized device, which can be a simple flash drive or cell phone, even a computer with a company's confidential database, to solve the most complex to the simplest problem. In these devices, countless information is stored that, if violated, can generate damage of all kinds. In this way, these people are susceptible to becoming victims of crimes committed through the invasion of such equipment. Although in criminal legislation there is already a typification of conduct such as embezzlement, theft, such crimes can be practiced either physically or virtually, however, there are some specificities that need to be expressly contained in the law. In Brazil, laws 12,735/12 and 12,737/12 (known as the Carolina Dieckmann Law) were enacted, the so-called Computer Crime Laws, which came into force in 2013, aimed at combating virtual crimes, in the face of technological advances and the democratization of social networks and, also, due to the pressure of the media. This article has the general objective of analyzing the treatment given by Brazilian legislation to criminal conduct practiced in the virtual environment. For this, it is imperative to understand the new formats and legal arrangements regarding virtual crimes; first, an approach will be made about Criminal Law and its conceptualization; secondly, cyber crimes will be analyzed; finally, the criminal type created by the Carolina Dieckmann Law will be analyzed.

KEYWORDS: Cyber crimes, criminal classification, Brazilian legislation

1 INTRODUÇÃO

O surgimento de novas tecnologias tem trazido benefícios para a sociedade e facilitado a vida das pessoas, no entanto, as facilidades oferecidas pela tecnologia tem contribuído para o aumento do número de vítimas de condutas ilícitas praticadas por indivíduos que se utilizam dessas vantagens tecnológicas e especialmente da internet para a prática de crimes.

É de se notar, também, a importância que os sistemas informáticos possuem no atual momento social, ressaltando que a maioria das pessoas, físicas ou jurídicas, depende do seu dispositivo informatizado, que pode ser um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa. Assim, nesses dispositivos acabam armazenando informações pessoais, sigilosas, privadas que se violadas podem gerar inúmeros prejuízos.

Desse modo, essas pessoas ficam suscetíveis a se tornarem vítimas de crimes praticados com a violação desses dispositivos. Embora na legislação penal já exista a tipificação de condutas como o estelionato, o furto, tais crimes podem ser praticadas tanto fisicamente ou virtualmente, existem algumas especificidades que precisam estar expressamente contidas na lei. Vale lembrar que as leis penais devem ser taxativas, no sentido de serem claras e precisas para que assim, possam ser compreendidas.

Assim, diante da prática de novas condutas que não estão tipificadas em lei, a ampliação do Direito Penal se torna necessária, a fim de garantir um método correto e eficaz na aplicação das normas penais, visando coibir e prevenir a prática que engloba todo o universo criminoso existente na internet.

O presente artigo tem como objetivo geral analisar o tratamento conferido pela legislação brasileira às condutas criminosas praticadas no ambiente virtual.

Dentre os objetivos específicos do presente trabalho está a conceituação e a caracterização do que seria um crime cibernético. A análise da Lei n. 12.735/12, que tipificou condutas com relação aos sistemas eletrônicos e da Lei Carolina Dieckmann (Lei n. 12.737/12), que inseriu no Código Penal o art. 154 (Invasão de Dispositivo Informático).

O tema tem relevância jurídica, pois conforme já destacado é de suma importância para o direito, dada a necessidade da tipificação dos crimes cibernéticos, entendida como a disponibilidade, confidencialidade e integridade das informações

dos usuários, há tempo já clamava por proteção jurídico-penal, já que a "violência" nesse meio vem evoluindo a longos passos.

Considerando que o presente trabalho é de natureza bibliográfica, o método de abordagem a ser adotado no seu desenvolvimento será o dedutivo, tendo como pressuposto argumentos gerais, para argumentos particulares; quanto ao procedimento será analítico e histórico crítico, a partir da doutrina e da jurisprudência dos tribunais. Quanto à metodologia, será de natureza qualitativa.

Por fim, ressalte-se que a escolha deste tema se deu em razão da necessidade de debates sobre as condutas que envolvem os "Crimes Cibernéticos", sobretudo em razão da grande proporção de que a chamada "era informática" tomou no atual cenário social.

2 A FUNÇÃO DO DIREITO PENAL

O Direito Penal é o setor do ordenamento jurídico que define crimes, comina penas e prevê medidas de segurança aplicáveis aos autores das condutas incriminadas. A definição de crimes se realiza pela descrição das condutas proibidas; a cominação de penas e a previsão de medidas de segurança se realiza pela delimitação de escalas punitivas ou assecuratórias aplicáveis, respectivamente, aos autores imputáveis ou inimputáveis de fatos puníveis (SANTOS, 2014, p. 27).

De tal modo que, nas lições do autor:

> O Código Penal, estatuto legal que define crimes e prevê penas e medidas de segurança, é o centro do programa de política penal do Estado para controle da criminalidade. As penas criminais constituem o instrumento principal da política penal do Estado, agrupadas em três categorias: a) penas privativas de liberdade; b) penas restritivas de direito; c) penas de multa (CP, art. 32). As medidas de segurança constituem instrumento secundário da política penal oficial, agrupadas em duas categorias: medidas de segurança detentivas e medidas de segurança não detentivas (CP, art. 96-99) (SANTOS, 2014, p. 28)

Ensina o autor, que os objetivos declarados do Direito Penal nas sociedades contemporâneas consistem na proteção de bens jurídicos - ou seja, na proteção de valores relevantes para a vida humana individual ou coletiva, sob ameaça de pena. Os bens jurídicos protegidos pelo Direito Penal são selecionados por critérios político-criminais fundados na Constituição Federal, o documento fundamental do moderno Estado Democrático de Direito.

Numa formulação simples, conceitua-se o Direito Penal como o ramo do Direito encarregado de definir as infrações penais e combinar-lhes a respectiva sanção. O Direito Penal é o ramo do Direito que se encarrega de regular os fatos humanos mais perturbadores da vida social, definindo-os quanto à sua extensão e consequências, de modo a assegurar, por meio da aplicação efetiva de suas prescrições, a garantia da vigência da norma e as expectativas normativas (ESTEFAM, 2018, p. 39)

É o conjunto de normas jurídicas voltado à fixação dos limites do poder punitivo do Estado, instituindo infrações penais e as sanções correspondentes, bem como regras atinentes à sua aplicação. Do ponto de vista objetivo, o direito penal é o corpo de normas jurídicas destinado ao combate à criminalidade, garantindo a defesa da sociedade. Por outro lado, do ângulo subjetivo, é definido como o direito de punir do Estado, que surge após o cometimento da infração penal (NUCCI, 2014, p. 48).

Por isso, quando o bem jurídico penal é destacado como tal, surgem tipos penais incriminadores para protegê-los, indicando as condutas proibidas, sob pena de lesão ao referido bem jurídico tutelado.

A Constituição Federal indica vários bens jurídicos, vários dos quais o Direito Penal chamou a si para a conveniente proteção e amparo. Ilustrando, vêm os seguintes bens jurídicos fundamentais: vida, liberdade, igualdade, segurança, propriedade, intimidade, vida privada, honra, trabalho, dentre outros (NUCCI, 2014, p. 50).

Vale ressaltar as seguintes lições:

> O Direito Penal apresenta-se, por um lado, como um conjunto de normas jurídicas que tem por objeto a determinação de infrações de natureza penal e suas sanções correspondentes — penas e medidas de segurança. Por outro lado, apresenta-se como um conjunto de valorações e princípios que orientam a própria aplicação e interpretação das normas penais. Esse conjunto de normas, valorações e princípios, devidamente sistematizados, tem a finalidade de tornar possível a convivência humana, ganhando aplicação prática nos casos ocorrentes, observando rigorosos princípios de justiça. Com esse sentido, recebe também a denominação de Ciência Penal, desempenhando igualmente uma função criadora, liberando-se das amarras do texto legal ou da dita vontade estática do legislador, assumindo seu verdadeiro papel, reconhecidamente valorativo e essencialmente crítico, no contexto da modernidade jurídica. (BITENCOURT, 2012, p. 57)

Segundo o autor, o Direito Penal regula as relações dos indivíduos em sociedade e as relações destes com a mesma sociedade. Como meio de controle

social altamente formalizado, exercido sob o monopólio do Estado, a persecução criminal somente poderá ser legitimada a partir das normas previamente estabelecidas. Por esse motivo os bens protegidos pelo Direito Penal não interessam ao indivíduo, exclusivamente, mas à coletividade como um todo.

3 CRIMES CIBERNÉTICOS

Os crimes cibernéticos, também chamados de crimes digitais, crimes eletrônicos, *cyber* crimes, entre outras nomenclaturas, estão em constante desenvolvimento. Com o avanço da tecnologia os crimes que dela se utilizam tomam novas formas que permitem e facilitam a incidência da criminalidade, surgindo diversos tipos de delitos cibernéticos.

O crime de informática pode ser conceituado “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. (ROQUE, 2007, p.25).

No Brasil, com o intuito de tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares foram editadas as Leis n. 12.735/12 e 12.737/12, as chamadas Leis de Crimes Informáticos, que entraram em vigor em 2013.

De igual modo, foi editada a Lei n. 12.965, conhecida como Marco Civil da Internet, esta com a finalidade de regulamentar o uso da Internet por meio de princípios, garantias, direitos e deveres para os usuários.

Contudo, a edição de leis que visam coibir o mau uso da internet e a prática de crimes utilizando esse ambiente, não são suficientes, do mesmo modo que não são as leis penais de modo geral, que combatem a prática de crimes em ambientes físicos, diante da falta de efetividade da norma.

A internet vem se tornando cada vez mais uma ferramenta necessária e indispensável para os atos da vida comum, ela pode ser utilizada dentre várias tecnologias, como serviços de comunicação: celulares, satélite, redes de informação, com isso se torna ampla as formas da prática do crime cibernético.

As comunidades da internet [...] são compostas e decompostas, ampliadas ou reduzidas em tamanho, pelas múltiplas ações provocadas por decisões e impulsos individuais de conectar-se e desconectar-se [...] É precisamente seu perpétuo estado de transitoriedade, sua inerente natureza temporária, já que para sempre provisória, sua abstenção de exigir comprometimentos de longo prazo ou a lealdade absoluta à

disciplina estrita, que as torna tão atraentes para tantos – dados os ambientes fluídos pelos quais é tão famosa a forma de vida líquido-moderna (BAUMAN, 2013, pp. 118-119).

Apesar de um termo pouco tradicional, os crimes associados a esses ambientes são de amplo conhecimento e cometidos com frequência, tais como roubos, estelionato, chantagem, apropriação indébita, e mesmo outros nem tão comuns, como acesso ilegal a base de dados, interceptação ilegal, obstrução de dados dentre outros. A possibilidade de anonimato e da ausência de regras na rede mundial de computadores é um dos fatores que contribui para o crescimento e facilidades para a prática desses crimes.

Devido à simplicidade e a rapidez com que a internet executa determinada função, o ser humano cada vez mais preferiu as ferramentas virtuais a tal ponto que, hoje, se uma pessoa não possui conta de e-mail ou rede social, é considerada de alguma forma "isolada" socialmente. A respeito disso, Maciel Colli posiciona-se:

> O uso da internet possibilitou a superação da dificuldade ocasionada pela distância territorial e pela limitação comunicativa entre as pessoas em locais distantes. A voz e o papel foram desbancados do ranking instrumental de intercâmbio de mensagens. O texto exibido nas telas de computadores, produtos de linguagem binária interpretada e transmutada pelas plataformas dos computadores, elimina a distância e o tempo.

A internet sendo uma rede de computadores integrada por redes menores que se comunicam entre si assim como os computadores se comunicam através dos seus endereços de IP onde inúmeras informações são trocadas.

> "A internet vem modificando o comportamento humano, incentivando a paixão pelo conhecimento, educação e cultura. Isso, entretanto, não é de graça; vem acompanhado da inseparável e sempre (má) companhia criminosa: os criminosos digitais". (KAMINSKI, 2003, p.28).

Assim os crimes virtuais podem ser definidos como as condutas de acesso não autorizado a sistemas informáticos, ações de destruição nos sistemas informáticos, interceptação de comunicações, alterações de dados entre outros.

A internet, portanto, é um novo caminho para a realização de delitos já praticados no mundo real, sendo necessário que as leis sejam adaptadas para combater os crimes eletrônicos. Essa é a nova missão da Justiça: adaptar os vários dispositivos do Código Penal no combate ao crime digital.

3.1 A legislação penal brasileira

Segundo FARIA (2012), a criação do Código Penal Brasileiro ocorreu em 1940 pelo Decreto-Lei 2.848, nessa época não se pensava em "era da informação" a qual deu início em meados de 1970; sendo assim, seu progresso dar-se-á no início da década de 90, com constante evolução até os dias atuais. Nesse período, o Brasil não possuía leis especificas e os artigos do Código Penal também não se enquadravam aos crimes praticados pela internet, e nenhuma informação que enunciasse a respeito da tipificação de tais crimes.

Para coibir a prática de condutas ilícitas por meio da internet, foram editadas as Leis n. 12.735/12 (Lei Azeredo) e 12.737/12 (Lei Carolina Dieckmann), as chamadas Leis de Crimes Informáticos, que entraram em vigor em 2013 com o intuito de tratar dos crimes cibernéticos, além da Lei n. 12.965/14, denominada como Marco Civil da Internet, com a regulação dos direitos e deveres dos usuários de internet no Brasil.

A promulgação da lei que regula o "Marco Civil da Internet" no Brasil atende à obrigação do Estado em disciplinar o direito comunicativo na era digital, em especial na rede mundial de computadores, sem o que haveria violação de direitos humanos (por omissão) por parte do poder público (MAZUOLLI, 2019, p. 468).

3.2 A Lei Eduardo Azeredo – Lei n. 12.735/12

A Lei n. 12.735/2012 altera o Código Penal, o Código Penal Militar e a Lei de combate ao racismo para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.

Ademais, a mencionada estabelece a obrigatoriedade de interrupção imediata de mensagens com conteúdo racista, além de retirá-las de qualquer meio de comunicação.

O texto legal também determina que os órgãos da polícia judiciária estruturem setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Conforme já destacado, a lei sancionada traz somente duas mudanças. A primeira, determina a criação em cada estado de setores especializados no combate às ações delituosas em rede de computadores, dispositivos de comunicação ou sistemas informatizados, conforme estipula o artigo 4º:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado[3].

A segunda, o artigo 5º da referida lei acrescentou no artigo 20 da lei 7.716/89 (Lei de Combate ao Racismo) o inciso II do §3º estipulando que:

> Art. 20, §3º, II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

O texto original da norma envolvia questões polêmicas, como a tipificação de compartilhamento de arquivos e a obrigatoriedade dos provedores de guardar e fiscalizar o registro das atividades de usuários. Entretanto esses pontos foram vetados.

3.3 O Marco Civil da Internet – Lei 12.965/2014

A referida lei visa regulamentar o uso da internet por meio de princípios, garantias, direitos e deveres para os usuários.

É importante frisar, que o Marco Civil da Internet fomenta no Brasil os direitos comunicativos à medida que considera a internet como ferramenta essencial para a liberdade da expressão e o exercício da cidadania, bem como para a promoção da cultura e o desenvolvimento tecnológico. Tal demonstra que o acesso à internet tem ligação direta com o tema dos direitos humanos, eis que auxilia na concretização do direito à liberdade de expressão e no exercício da cidadania (MAZUOLLI, 2019, p. 472).

O Marco Civil da internet foi desenhado a partir de três fundamentos essenciais os quais norteiam a relação das empresas prestadoras de serviços de internet com os seus clientes. São eles: a neutralidade da rede, a privacidade e a fiscalização.

O princípio da neutralidade foi utilizado por *Tim Wu* (2011), a quem seria atribuído a criação do termo, o qual tem por significado que a rede mundial de

[3]BRASIL. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Data de acesso: 11.03.2021.

computadores seja pública, no sentido de tratar todo conteúdo, sites e plataformas digitais de forma igualitária[4].

O princípio da privacidade nada mais é do que a garantia de inviolabilidade das comunicações dos usuários. Nesse sentido, a Lei do Marco Civil atribui o dever de sigilo de suas informações ao provedor do recurso de internet.

A fiscalização trata-se de uma responsabilidade da empresa provedora do serviço cujo prazo mínimo da obrigação é de um ano. Caso necessário, as autoridades podem exigir de um provedor alguns dados cadastrais que qualifiquem os seus usuários, como nome completo, estado civil, profissão, filiação, endereço.

As mudanças introduzidas pela Lei n. 12.965/2014 impactaram diretamente os procedimentos de transferência de informações fornecidas pelos usuários, assim como, a sua segurança enquanto estão sob a tutela da empresa.

A partir da entrada em vigor do Marco Civil da Internet mais do que estarem cientes sobre o tratamento conferido pelas companhias aos seus dados pessoais, o consentimento expresso dos consumidores é uma medida obrigatória.

Cabe ressaltar que, a lei entrou em vigor, nos termos do art. 32, sessenta dias após a publicação (publicação no Diário Oficial, 23 de abril de 2014).

Nesse sentido, com relação as novas mudanças, conforme as lições de Cassanti (2014, p. 94), “com as novas regras, as empresas que atuam no comércio eletrônico terão que dispor em suas páginas informações sobre produtos, fornecedores, serviços e aperfeiçoamento do atendimento ao consumidor”.

3.4 A Lei Carolina Dieckmann – Lei n. 12.737/12 e a nova tipificação penal do art. 154 – A do Código Penal Brasileiro

O século XXI está experimentando um avanço tecnológico inacreditável. Situações que, em um passado não muito distante, eram retratadas em filmes e desenhos infantis como sendo hipóteses futuristas, hoje estão presentes em nosso dia a dia. As conversas on-line, com visualização das imagens dos interlocutores, seja através de computadores, ou mesmo de *smartphones*, que pareciam incríveis no início

4 CONSULTOR JURÍDICO. **Neutralidade da Rede e Proteção do Consumidor no Contexto Pandêmico** Disponível em https://www.conjur.com.br/2021-jun-16/garantias-consumo-neutralidade-rede-protecao-consumidor-contexto-pandemico#_edn2. Data de acesso: 15.03.2022.

da segunda metade do século XX, atualmente fazem parte da nossa realidade (GRECO, 2017, p. 849).

Essas mudanças tecnológicas fizeram com que diversas informações fossem armazenadas nesses equipamentos, todavia, no ordenamento jurídico brasileiro não havia uma lei específica para tratar acerca de possíveis violações das informações e das imagens contidas nesses dispositivos.

Apesar de a sociedade estar cada vez mais inserida no mundo da informática, percebe-se que o Direito (em especial, o Direito Penal) não acompanha, como deveria, a evolução que movimenta o setor cibernético (CUNHA, 2016, p. 243).

O episódio envolvendo a atriz Carolina Dieckmann que teve seu computador invadido e seus arquivos pessoais subtraídos, com a exposição de suas fotos íntimas na rede mundial de computadores gerou comoção e indignação na sociedade. Tal fato fez com que fosse editada a Lei n. 12.737, de 30 de novembro de 2012, que tipificou como crime a invasão de dispositivo informático.

O objeto jurídico do crime é a privacidade individual e/ou profissional, resguardada (armazenada) em dispositivo informático, desdobramento lógico do direito fundamental assegurado no art. 5°, X, CF/88: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação".

Destaque-se os ensinamentos trazidos por Sarlet (2018, p. 471) acerca do direito à privacidade:

> o direito à privacidade possui uma dupla dimensão: objetiva e subjetiva, o qual opera na condição de direito subjetivo, em primeira linha como direito de defesa, portanto, como direito à não intervenção estatal e de terceiros no respectivo âmbito de proteção do direito e, como expressão também da liberdade pessoal, como direito a não ser impedido de levar sua vida privada conforme seu projeto existencial pessoal e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal e que não interferem em direitos de terceiros, envolvendo a autodeterminação do indivíduo. Por sua vez, da perspectiva de sua dimensão objetiva decorre, além da assim chamada eficácia irradiante e interpretação da legislação civil (notadamente no campo dos direitos de personalidade), em sintonia com os parâmetros normativos dos direitos fundamentais, um dever de proteção estatal, no sentido tanto da proteção da privacidade na esfera das relações privadas, ou seja, contra intervenções de terceiros, quanto no que diz com a garantia das condições constitutivas da fruição da vida privada.

O direito à privacidade consiste na faculdade de se optar por estar só e não ser perturbado em sua vida particular, formando uma esfera de autonomia e exclusão dos demais e evitando que, sem o consentimento do titular ou por um interesse público, nela se intrometam terceiros. Assim, o direito à privacidade é um direito fundamental que permite que seu titular impeça que determinados aspectos de sua vida sejam submetidos, contra a sua vontade, à publicidade e a outras turbações feitas por terceiros (RAMOS, 2020, p. 481).

Conforme a jurisprudência do Superior Tribunal de Justiça:

> EMENTA RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. DETERMINAÇÃO DE QUEBRA DO SIGILO DO REGISTRO DE ACESSO À INTERNET. FORNECIMENTO DE IPS. DETERMINAÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO. 1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "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". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital 2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de aparelhos utilizados por usuários que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio. 4. A

determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma. 5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso sub examine. Deveras, o procedimento de que trata o art. 2º da Lei n. 9.296/1996, cujas rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplica a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados. 6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios. 7. Os arts. 22 e 23 do Marco Civil da Internet, em complemento ao art. 10, parágrafo único, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie - se houvesse tal obrigatoriedade legal - plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos

> crimes investigados. 8. Logo, a quebra do sigilo de dados armazenados, assim entendida a requisição mediante ordem judicial de registros de conexão e acesso à internet, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado. 9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau. (Relator Ministro Rogério Schietti Cruz. Recurso Ordinário em Mandado de Segurança. 2019/0119654-6. DJE. 04/09/2020)

Desse modo, o crime de invasão de dispositivo informático consubstancia-se no ato de invadir dispositivo informático alheio, mediante violação de mecanismo de segurança, com o propósito de obter, adulterar ou destruir dados ou informações ou de instalar vulnerabilidades.

Em regra, o crime é de menor potencial ofensivo, salvo na sua forma qualificada (§ 3°), quando majorado pela divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas (§ 4°).

A norma foi publicada no Diário Oficial em 3 de dezembro do mesmo ano, com vacatio legis de 120 dias. Como se cuida de novatio legis incriminadora, não se aplica a fatos ocorridos antes de sua entrada em vigor. O legislador inseriu o tipo penal entre os crimes contra a inviolabilidade dos segredos, revelando parte do bem jurídico protegido. Tutelam-se, além deste, a intimidade e a segurança informática (ESTEFAM, 2020, p. 410)[5]

Esta lei visa tipificar os delitos informáticos tratando das invasões a dispositivos informáticos, da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou desinformação de utilidade pública e da

[5] Vale registrar, por oportuno, que o ordenamento jurídico brasileiro conta com duas importantes leis, que não possuem caráter penal, a respeito de princípios, garantias, direitos e deveres do uso da internet (Lei n. 12.965/2014 — Marco Civil da Internet) e da proteção de dados pessoais por meio da internet (Lei n. 13.709/2018 — Lei de Proteção de Dados Pessoais).

falsificação de documento particular e cartão. E, além disso, tipifica condutas que não eram até então tratadas como infração penal.

A referida Lei introduziu no ordenamento jurídico três tipificações penais no Código Penal:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Ensina o professor Guilherme Nucci (2020, p. 984)

> O principal dos novos artigos preceitua que “a infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei 2.848, de 7 de dezembro de 1940 (Código Penal), obedeceráàs seguintes regras: I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial” (art. 190-A)

Nesse sentido, o verbo nuclear do tipo penal é invadir, no sentido de violar, acessar ou penetrar. Segundo a doutrina, quanto ao dispositivo informático seria todo aquele aparelho capaz de receber ou transmitir os dados, tratá-los, os resultados, a exemplo do que ocorre com os computadores, *smartphones*, *tabletes* etc. Exige o art. 154-A que esse dispositivo informático seja *alheio*, isto é, não pertença ao agente que o utiliza (GRECO, 2019, p.450)

Esse dispositivo informático alheio poder estar ou não conectado à rede de computadores, ou seja, a um conjunto de dois ou mais computadores autônomos e outros dispositivos, interligados entre si com a finalidade de compartilhar informações e equipamentos, como, por exemplo, os dados, impressoras, mensagens etc. (GRECO, 2019, p. 450)

Sendo assim, diz respeito, portanto, a estruturas físicas (equipamentos) e lógicas (programas, protocolos) que possibilitam que dois ou mais computadores possam compartilhar suas informações entre si. Segundo Greco (2019, p. 450) o sujeito ativo do crime pode ser qualquer pessoa; quanto ao sujeito passivo, seria o proprietário, na condição de pessoa física ou pessoa jurídica do dispositivo informático invadido. Ainda, pode ser qualquer outra pessoa que nele tenha arquivado dados ou informações.

Em se tratando de um crime formal, o delito tipificado no caput, do dispositivo não exige resultado naturalístico, qual seja, a efetiva obtenção, adulteração ou destruição dos dados ou informações contidas no equipamento.

Vale ressaltar as lições do professor Rogério Greco (2017, p. 856)

> Esse dispositivo informático alheio pode estar ou não conectado à rede de computadores, ou seja, a um conjunto de dois ou mais computadores autônomos e outros dispositivos, interligados entre si com a finalidade de compartilhar informações e equipamentos, a exemplo dos dados, impressoras, mensagens etc. Diz respeito, portanto, a estruturas físicas (equipamentos) e lógicas (programas, protocolos) que possibilitam que dois ou mais computadores possam compartilhar suas informações entre si. A internet, por ser considerada um amplo sistema de comunicação, conecta inúmeras redes de computadores. As quatro redes mais conhecidas, classificadas quanto ao tamanho, são: 1. LAN (Local Area Network) – redes locais, privadas, em que os computadores ficam localizados dentro de um mesmo espaço, como, por exemplo, uma residência, uma sala comercial, um prédio etc.; 2. MAN (MetropolitanArea Network) – redes metropolitanas, em que os computadores estão ligados remotamente, a distâncias pequenas, podendo se localizar na mesma cidade ou entre duas cidades próximas; 3. WAN (WideArea Network) – são redes extensas, ligadas, normalmente, entre diferentes estados, países ou

> continentes, a exemplo do que ocorre com o sistema bancário internacional; 4. PAN (PersonalArea Network) – são redes pessoais, presentes em regiões delimitadas, próximas umas das outras.

O delito da nova modalidade se consuma no momento em que o agente consegue, efetivamente, invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Dessa forma, ensina o autor, que presentes os demais elementos exigidos pelo tipo penal, poderá ocorrer a infração penal em comento, com a invasão de um dispositivo informático alheio, como ocorre com um computador, que pode não estar ligado a qualquer rede e ser acessado via internet.

Assim, por exemplo, se alguém, percebendo que seu vizinho esqueceu o computador que havia levado para uma festa em que ambos participavam, invadir o equipamento, mediante violação indevida de mecanismo de segurança, com a finalidade de destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, poderá ser responsabilizado pelo tipo penal previsto pelo caput do art. 154-A do Código Penal.

Assim, não é a simples invasão, mediante a violação indevida de mecanismo de segurança, que importa na prática da infração penal tipificada no caput do art. 154-A do diploma repressivo, mas sim aquela que possui uma finalidade especial, ou seja, aquilo que denominamos especial fim de agir, que consiste na obtenção, adulteração ou destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo. Obter tem o significado de adquirir, alcançar o que desejava conseguir; adulterar diz respeito a alterar, estragar, modificar o conteúdo, corromper; destruir quer dizer aniquilar, fazer desaparecer, arruinar (GRECO, 2017, p. 859).

Para que ocorra a infração penal prevista e, portanto, enquadre na tipicidade delitiva, o tipo penal exige, ainda, que a conduta seja levada a efeito mediante violação indevida de mecanismo de segurança. Entende-se por mecanismos de segurança todos os meios que visem a garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de *login* e senhas que visem a identificar e autenticar o usuário, impedindo que terceiros não autorizados tenham acesso às informações nele contidas.

Ensina Guilherme Nucci (2014, p. 579)

> Invadir (violar, transgredir) é um verbo de conteúdo normativo, significando algo ilícito, pois representa a entrada à força em lugar alheio. O objeto da conduta é o dispositivo informático (qualquer mecanismo apto a concentrar informação por meio de computador ou equipamento similar). São dispositivos informáticos: computador de mesa, notebook, laptop, *ultrabook, tablet, ipad, smartphone* etc. Não se exige, para a configuração do crime, conexão com rede, inclusive internet. No entanto, o tipo penal indica a necessidade do dispositivo informático possuir algum mecanismo de segurança, sob pena de ser considerado desprotegido penalmente. Outra forma de praticar o delito é instalar (preparar para funcionar) vulnerabilidade (mecanismo apto a gerar abertura ou flanco em qualquer sistema) no dispositivo informático, com a intenção de obter vantagem ilícita.

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 de violação de dispositivo informático. Trata-se da punição à preparação do crime principal. Este tipo penal não possui sujeito passivo definido, pois a ação é genericamente preparatória. Por isso, ocupa este espaço a sociedade, em seu interesse de preservar a intimidade e a vida privada dos indivíduos em geral.

Destaque-se que a nova legislação inseriu o §1º e §2º ao art. 266 prevendo como crime a conduta de interromper ou perturbar serviço telefônico, telegráfico, informático, telemático ou de informação de utilidade pública. Inseriu o parágrafo único ao art. 298 estabelecendo que configure também o crime de falsidade de documento particular a conduta de falsificar ou alterar cartão de crédito ou de débito.

A ação penal, em regra, é condicionada à representação da vítima, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, hipóteses em que a ação será pública incondicionada. (CUNHA, 2016, p. 248). Citamos a jurisprudência:

> **Ementa:** HABEAS CORPUS. CÓDIGO PENAL. CRIMES CONTRA O PATRIMÔNIO. ART. 154-A, § 1º. INVASÃO DE DISPOSITIVO INFORMÁTICO. ART. 155 § 4º, INCISO I. FURTO QUALIFICADO. ROMPIMENTO DE OBSTÁCULO. Subtração de duas máquinas policorte, uma politriz, uma lixadeira e um jogo de cachimbo, um televisor 40", uma caixa acústica e alguns documentos e cartões, uma TV 65", um micro-ondas e uma TV 32". Relato das vítimas apontam que o paciente é autor do fato, aliado a confissão em Delegacia de Polícia, todavia o delito foi cometido sem violência ou grave ameaça, além disso ele é tecnicamente primário. Liminar deferida no plantão. Parecer pela concessão da ordem. LIMINAR RATIFICADA. ORDEM CONCEDIDA. UNÂNIME.(Habeas Corpus Criminal, Nº 70084860022, Quinta Câmara Criminal, Tribunal de Justiça do RS, Relator: Ivan Leomar Bruxel, Julgado em: 25-02-2021)

No caso em tela, não restou configurada a hipótese de delito por invasão de dispositivo informático, visto que embora os objetos furtados, tais como, televisão, cartões de banco, especialmente, esse que poderia ter havido a violação indevida de mecanismo de segurança alheio, acabou não ocorrendo, tendo sido apenas furtado o cartão bancário, sem que houvesse a tentativa de uso do cartão.

4 CONSIDERAÇÕES FINAIS

A evolução da tecnologia tem propiciado inúmeros benefícios para a sociedade, todavia, essa modernidade também apresenta aspectos negativos. As facilidades e benefícios oferecidos pela tecnologia têm contribuído para o aumento do número de vítimas de condutas ilícitas praticadas por indivíduos que se utilizam dessas vantagens tecnológicas e especialmente da internet para a prática de crimes.

Como forma de prevenção, é necessário conscientizar os usuários dos riscos eminentes que existem nas redes e como podem agir caso sejam lesados e, para que os usuários tenham segurança no uso da internet, é preciso criar normas específicas para serem aplicadas de forma correta e efetiva, deixando de lado a sensação de impunidade existente.

Diante disso, o ordenamento jurídico precisa se adaptar de forma célere, alinhando-se conforme a tecnologia e a sociedade avançam.

O presente artigo objetivou analisar o tratamento conferido pela legislação brasileira às condutas criminosas praticadas no ambiente virtual.

A entrada em vigor da contemporânea Lei n. 12.737/12 representou significativa mudança no nosso ordenamento jurídico, haja vista tratar de crimes cada vez mais constantes na hodierna sociedade, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

De igual modo, o Marco Civil da Internet foi editado buscando regulamentar o uso da internet por meio de princípios, garantias, direitos e deveres para os usuários.

Todavia, é perceptível que embora a legislação brasileira busque estabelecer princípios para o bom uso da internet, bem como combater os crimes virtuais, a legislação precisa acompanhar a evolução tecnológica para que de fato sejam efetivas naquilo a que se propõem.

5 REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral**, 1. – 17. ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011. – São Paulo: Saraiva 2012

BAUMAN, Zygmunt.**Danos Colaterais: desigualdades sociais numa era global.** Tradução: Carlos Alberto Medeiros – Rio de Janeiro: Zahar, 2013.

BRASIL. Código Penal e dá outras providências. **Decreto-Lei 2.848, de 7 de dezembro de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Data de acesso: 11.03.2021.

BRASIL. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Data de acesso: 11.03.2021.

BRASIL. **Lei 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

BRASIL. **Lei 12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Data de acesso: 11.03.2022.

CASSANTI, Moisés de Oliveira. **Crimes virtuais: vitimais reais.** Rio de Janeiro: BRASPORT, 2014.

COLLI, Maciel. **Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos.** Curitiba: Juruá Editora, 2010.

CONSULTOR JURÍDICO. **Neutralidade da Rede e Proteção do Consumidor no Contexto Pandêmico** Disponível em https://www.conjur.com.br/2021-jun-16/garantias-consumo-neutralidade-rede-protecao-consumidor-contexto-pandemico#_edn2. Data de acesso: 15.03.2022.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especi**al. (arts. 121 ao 361) I Rogério Sanches Cunha- 8. ed. rev., ampl. e atual. JusPODIVM, 2016.

ESTEFAM, André. **Direito penal: parte geral** (art. 1º a 120). – 7. ed. – São Paulo: Saraiva Educação, 2018.

FARIA, Matheus Afonso de. **O Problema da tipificação dos crimes informáticos.** Rio Grande: Revista âmbito Jurídico, 2012.

FERREIRA, IvetteSenise. **Direito & Internet: Aspectos Jurídicos Relevantes.** 2 ed. São Paulo: QuartierLatin, 2005.

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

___. **Curso de Direito Penal: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. – 14. ed. Niterói, RJ: Impetus, 2017.

JEOVÁ. Antônio Santos. **Dano Moral Indenizável**. 5. ed. Salvador/BA: Juspodivm, 2015.

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

KAMINSKI, Omar. **Internet Legal: O direito na tecnologia da informação**. 1ed. Curitiba: Juruá, 2003.

MAZUOLLI, Valério de Oliveira. **Curso de direitos humanos**. 6. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2019.

NUCCI, Guilherme de Souza. **Manual de direito penal**. – 10. ed. rev., atual. eampl. – Rio de Janeiro: Forense, 2014.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. – 7. ed. – São Paulo : Saraiva Educação, 2020

ROQUE, Sérgio Marcos. **Criminalidade informática*:* crimes e criminosos do computador.** 1 ed. São Paulo: ADPESP Cultural, 2007.

SANTOS, Antônio Jeová. **Dano Moral na Internet**. 1º Ed. São Paulo: Método, 2001.

SANTOS Juarez Cirino dos. **Direito penal: parte geral I**. - 6. ed., ampl. e atual. - Curitiba, PR: ICPC Cursos e Edições, 2014.

TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. Disponível em https://www.tjrs.jus.br/novo/buscassolr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Data de acesso: 08.05.2022.

SUPERIOR TRIBUNAL DE JUSTIÇA. Disponível em https://processo.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=INVASAO+DE+DISPOSITIVO+INFORMATICO&pesquisaAmigavel=+%3Cb%3EINVASAO+DE+DISPOSITIVO+INFORMATICO%3C%2Fb%3E&b=ACOR&p=true&l=25&i=2&operador=e&tipo_visualizacao=RESUMO&tp=T. Data de acesso: 08.05.2022.

O TEMPO. Disponível em https://www.otempo.com.br/economia/crimes-ciberneticos-atingem-62-milhoes-no-brasil-em-2017-1.1572879. Data de acesso: 30.01.2022