**FACULDADE DE INHUMAS**
**CENTRO DE EDUCAÇÃO SUPERIOR DE INHUMAS**

**CURSO DE DIREITO**

**STEFFANNY ASSUNÇÃO SOUZA OLEGARIO**

# AUMENTO DA CRIMINALIDADE VIRTUAL E A PERSPECTIVA DA LEGISLAÇÃO BRASILEIRA

**INHUMAS-GO**
**2021**

**STEFFANNY ASSUNÇÃO SOUZA OLEGARIO**

# AUMENTO DA CRIMINALIDADE VIRTUAL E A PERSPECTIVA DA LEGISLAÇÃO BRASILEIRA

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.

**Professor (a) orientador (a):** Fernando Emídio dos Santos.

**INHUMAS-GO**

**2021**

**STEFFANNY ASSUNÇÃO SOUZA OLEGARIO**

# AUMENTO DA CRIMINALIDADE VIRTUAL E A PERSPECTIVA DA LEGISLAÇÃO BRASILEIRA

**AVALIAÇÃO DE DESEMPENHO DO(S) ALUNO(S)**

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.

Inhumas, 16 de dezembro de 2021.

**BANCA EXAMINADORA**

_____

Prof. Fernando Emídio dos Santos – FacMais
(orientador(a) e presidente)

_____

Profª. Julyana Macedo Rego– FacMais
(Membro)

**Dados Internacionais de Catalogação na Publicação (CIP)**

**BIBLIOTECA FACMAIS**

O45a

OLEGARIO, Steffanny Assunção Souza
AUMENTO DA CRIMINALIDADE VIRTUAL E A PERSPECTIVA DA LEGISLAÇÃO BRASILEIRA/ Steffanny Assunção Souza Olegario. – Inhumas: FacMais, 2021.

44 f.: il.

Orientador (a): Fernando Emídio dos Santos

Monografia (Graduação em Direito) - Centro de Educação Superior de Inhumas - FacMais, 2021.
Inclui bibliografia.

1. Crimes; 2. Legislação; 3. Investigação. I. Título.

CDU: 34

Dedico esta monografia aos meus familiares e amigos que estiveram presentes durante estes cinco anos.

## AGRADECIMENTOS

A princípio agradeço a Deus, que foi minha base, meu alicerce, minha fonte de força, coragem e determinação. Meu amparo nas horas difíceis para dar continuidade ao meu sonho.

Em seguida, agradeço aos meus familiares, em especial aos meus pais, Lucimar e Elismar e a minha irmã Karla, que sempre me apoiaram. Posteriormente aos meus avós maternos, Ana e Deraldo, que são minha base, que acreditaram no meu potencial, me motivaram a dar continuidade aos meus estudos e nunca desistir.

Agradeço ao meu orientador(a), Fernando Emídio, pelos ensinamentos, pela paciência, pelas críticas construtivas e aprendizado. Um grande mestre, me orgulho de ter lhe escolhido como meu orientador. Levarei seus ensinamentos.

Agradeço aos meus professores(as) que tive a honra de ser acadêmica e aprender coisas extraordinárias. Em especial ao eterno mestre Baloi, meu espelho, que fez eu amar o Direito Penal.

Por fim, agradeço aos meus colegas de curso, em especial aos meus amigos queridos  Luccas, Andrew, Lara e Iasmim, que me apoiaram e me incentivaram a nunca desistir do meu curso, durante estes cinco anos.

Epígrafe: Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade (NUNES, 2016, p.18).

## LISTA DE ABREVIATURAS E SIGLAS

**LGPD -** LEI GERAL DE PROTEÇÃO DE DADOS

## RESUMO

O presente trabalho abordará os crimes cibernéticos, os direitos dos usuários e as perspectivas da legislação brasileira, e traz à tona a legislação que recebeu várias críticas e ficou conhecida como Lei Carolina Dieckmann, Lei 12.737/2012. Com o aumento de usuários, a criminalidade cresceu, acompanhando o avanço da tecnologia e fazendo, por consequência, novas vítimas, que são, muitas das vezes, leigas de informações, sem preparo para lidar com os perigos virtuais. Ademais, a pesquisa apresenta uma breve análise que vivenciamos com a mudança na pandemia, adequação a novas modalidades de trabalho, os riscos a que estamos sujeitos no dia a dia, bem como a falta de provas, a ausência de autoria e as poucas Delegacias Especializadas para investigar crimes cibernéticos.



**Palavras-chaves**: Crimes. Legislação. Investigação.

## ABSTRACT

This work will address cybercrime, users' rights and perspectives of Brazilian legislation, and brings to light the legislation that received several criticisms and became known as Carolina Dieckmann Law, Law 12,737/2012. With the increase in users, crime has grown, following the advance of technology and, consequently, making new victims, who are often information laymen, unprepared to deal with virtual dangers. Furthermore, the research presents a brief analysis of what we experience with the change in the pandemic, adaptation to new work modalities, the risks we are subject to on a daily basis, as well as the lack of evidence, the absence of authorship and the few Specialized Police Stations to investigate cyber crimes.



**Keywords:** Crimes. Legislation. Investigation.

**SUMÁRIO**

# INTRODUÇÃO

O avanço tecnológico ao longo dos anos concebeu às pessoas o acesso fácil às plataformas virtuais, o que facilitou a busca por informações, além de tornar possível se relacionar com outras pessoas em lugares distintos.

Por consequência disso, a prática constante de crimes virtuais cresceu. A maioria dos autores são os chamados “ciber criminosos” ou “hackers”, que invadem o sistema de informação através de um computador, aparelho celular ou e-mail de pessoas físicas ou jurídicas. Eles invadem com a finalidade de obter para si ou para outrem vantagens ilícitas, aplicando golpes em terceiros, além de adulterar, destruir ou compartilhar os dados pessoais. Para este tipo de ato criminoso dá-se o nome de “crime cibernético”, que são quaisquer tipo de infração, omissão ou abusos cometidos via internet, usando quaisquer meios eletrônicos.

A violação da honra humana é presente na vida fora da internet. Mas com o crescente acesso de usuários na esfera digital, ficou mais constante os ataques, e muitas das vezes o direito à privacidade é ferido, o que se torna cada vez mais imperceptível, pois algumas pessoas não reconhecem quando sua honra, direitos e/ou dados pessoais são violados em sites ou plataformas digitais.

Neste contexto, foi necessário a criação de uma nova Lei que atendesse a necessidade do ambiente virtual e da internet atualmente. Tal Lei ficou conhecida nacionalmente como Lei Carolina Dieckmann, Lei Federal nº 12.737/2012.

A norma previu a tipificação de delitos informáticos, porém, destaca-se, como um dos principais pontos desta norma, a inclusão do artigo 154-A no Código Penal. Em suma, a atriz supracitada teve suas fotos íntimas divulgadas sem seu consentimento, após sofrer uma tentativa de extorsão, que resultou em sua honra prejudicada.

Nos dias atuais é indiscutível que a legislação não está conseguindo acompanhar o avanço da tecnologia, e consequentemente os delitos na esfera virtual crescem. Se a legislação não consegue acompanhar a criminalidade virtual no cotidiano, surge um grande empecilho para o desenvolvimento de soluções que evitem crimes cibernéticos.

No âmbito virtual, os crimes que eram frequentes na vida fora da internet passaram a ser presentes no mundo virtual. Alguns crimes mais frequentes são o crime de extorsão, estelionato e os crimes contra a honra (calúnia, injúria e

difamação). A maioria desses crimes são cometidos em redes sociais, perfil falso ou, no caso do estelionato, uma compra, um boleto fraudulento.

Neste ínterim, o avanço tecnológico trouxe diversas vantagens, como a acessibilidade, que facilitou a comunicação entre os indivíduos. O cenário atual de pandemia da COVID-19 fez com que as pessoas se adaptassem a mudanças no dia a dia para proteger-se e proteger os próximos do vírus. Com isso, muitas empresas tiveram que trabalhar em formato “home office”, como é conhecido no Brasil. Além disso, durante o período pandêmico, as pessoas estavam saindo somente em casos de urgência ou grande necessidade. Como ficaram isolados, o acesso às redes sociais, compras onlines e outros afazeres aumentaram e, consequentemente, a criminalidade também.

Os crimes cibernéticos começaram a ser mais recorrentes, fazendo novas vítimas, algumas leigas sobre o assunto, sobre penas adequadas ou até aonde buscar por amparo, onde procurar, o local exato para notificar o delito, para, assim, abrir uma investigação sobre o fato.

Muitas das vezes o anonimato que reina por trás da criminalidade, a ausência de vestígios e provas, são motivos que levam os usuários a desistirem de dar segmento, com o intuito de buscar a autoria do crime. Necessita-se de mais Delegacias especializadas para investigar casos concretos de crimes cibernéticos e amparar as vítimas ou impedir vítimas futuras.

Portanto, o presente estudo é de suma importância para a sociedade compreender o que é crime cibernético. Quando há ou se é impune a legislação em face de crimes virtuais, além dos perigos ao utilizar meios eletrônicos, bem como a existência de Delegacias especializadas.

## 1.CRIMES CIBERNÉTICOS

Crime cibernético ou crime virtual, como o nome já diz, é uma conduta ilícita cometida no âmbito virtual, através de dispositivos eletrônicos, podendo ter como suposto autor um anônimo ou até mesmo hacker e cracker.

Os crimes cibernéticos se enquadram nos mesmos elementos dos tipos penais, por serem uma conduta típica, antijurídica, culpável ou podendo ser dolosa.

Desta forma, por outra perspectiva, conceituamos crime cibernético de acordo com a escrita de Feliciano (2000, p.13) que tange:

> Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que tem por objeto material ou meio de execução o objeto tecnológico informático.

Atualmente, o acesso à internet vem crescendo bravamente e, com isso, surgem novidades, meios tecnológicos, aplicativos, sites e plataformas que facilitam o dia a dia dos indivíduos que usam os meios informáticos, tanto para estudo, trabalho e até mesmo para se relacionarem.

Porém, na internet existe um lado obscuro que poucas pessoas conseguem enxergar, como criminosos que estão a todo momento fazendo novas vítimas. Eles invadem dispositivos eletrônicos (smartphones, tablets ou computadores), aplicando golpes, como estelionato, clonagem, podendo também criar uma conta fake e proferir ameaças, injúrias, bullying e calúnias.

O objetivo de alguns infratores é adquirir, falsificar ou abolir dados, fotos ou arquivos sem o consentimento da vítima, com a finalidade de obter vantagens ilícitas. E muitas das vezes, algumas pessoas são leigas de informações e não percebem que estão sendo vítimas de um crime virtual, cuja penalidade sucede fora de um dispositivo eletrônico.

O doutrinador Rossini define crimes virtuais:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004, p. 110).

Já o doutrinador Pinheiro os classificam como:

> [...] sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, religioso, difusão de pornografia infantil, terrorismo entre outros (PINHEIRO, 2010, p. 46).

Em decorrência dos fatos, surgiu a Lei 12.737/12, que ficou conhecida como Lei Carolina Dieckmann, que visa suprimir os ataques de cibercriminosos, para os quais ainda não existia uma legislação específica de punição..

A referida Lei sucede após o Marco Civil da Internet, intitulado como Lei nº: 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos municípios em relação a matéria, como previsto no Art. 1º da Lei.

Podemos destacar também a Lei 13.709/2018, nomeada de LGPD, Lei Geral de Proteção de Dados, que legisla a proteção de dados pessoais dos indivíduos em qualquer meio que envolva o tratamento de dados pessoais, tanto de pessoas físicas como de pessoas jurídicas, abordando princípios, direitos e garantias no meio digital.

As referidas leis são de suma importância, pois protegem os direitos e garantias dos usuários. Cada uma delas tem sua excepcional função, e nota-se que o ordenamento jurídico trabalha arduamente para não deixar as pessoas desamparadas, já que existem leis para tentar combater a criminalidade no âmbito virtual.

Em contrapartida a justiça é falha, e muitas das vezes os criminosos ficam impunes. A Polícia Civil, que é umas das responsáveis por investigar crimes também na esfera virtual, tem um pouco de dificuldade nas investigações, por falta de provas concretas para constituir os autos.

Por fim, a internet é uma rede que cresce cada vez mais, e com isso as informações também. E a cada passa que a tecnologia evolui, vem trazendo com ela informações e mecanismo de defesas, para tentar minimizar fraudes.

Muitas vezes os mecanismos de defesa ou algumas informações que seriam úteis para os usuários, acaba sendo imperceptível aos seus olhos, pois a criminalidade cresce cada vez mais e poucos usuários conseguem perceber o perigo atrás do mundo digital, ajuntado com a dificuldade de identificar os autores, o que causa a sensação de existir uma justiça falha.

## 1.1 CLASSIFICAÇÃO

Os crimes cibernéticos, como vimos, são crimes praticados através de um meio eletrônico, e o mecanismo que os infratores utilizam para cometer os delitos é a internet. Os delitos podem ser classificados como sendo crimes próprios ou crimes impróprios.

Neste contexto, quando a ação inviabiliza o bem jurídico de um sujeito, acessando os dados armazenados em algum sistema de informática, e tendo como intuito adulterar, destruir, ou inserir dados falsos no dispositivo, caracteriza-se crime próprio.

Destaca-se aqui a conceituação de acordo com Damásio Evangelista de Jesus (apud CARNEIRO, 2012, s/p):

> Crimes eletrônicos puros ou próprios são aqueles que são praticados por computador e se realizam ou se consomem 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.

Neste ínterim, o crime virtual próprio é cometido em um meio eletrônico, tanto a ação quanto o resultado. Assim o delito é efetivado, e dessa forma a infração penal seja distinta das que estão expressa no Código Penal Brasileiro.

Podemos destacar como um crime próprio o Art§1º do art. 154-A do CPB, que abrange sobre a produção e divulgação de programas de computadores destrutivos. Outro exemplo que se enquadra como crime próprio seria a interceptação telefônica, desfiando a ligação de forma ilegal, capturando os dados pessoais e informações para terceiros.

Além disso, temos o crime impróprio, que é a conduta ilícita praticada através de um computador, isto é, uma máquina que tenha acesso à rede de internet. Desta forma, atinge um bem jurídico já tutelado, um crime tipificado no ordenamento jurídico.

Como explica o jurista Damásio E. de Jesus (apud CARNEIRO, 2012, s/p):

> Já os crimes eletrônicos 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.

No crime impróprio, o agente utiliza-se de um computador para aplicar golpes afetando um bem jurídico já tutelado no nosso ordenamento e que não tenha ligação

ao mundo informático, haja vista que o referido crime não infringe arquivos ou dados pessoais dos usuários, conforme o Art.154-A do Código Penal Brasileiro.

Uma identificação de crime impróprio seria, por exemplo, o encaminhamento de um e-mail, ou uma simples publicação via rede social. Dessa forma, o agente não precisa de um computador, ele apenas utiliza-se de um meio para aplicar golpes, já previstos na legislação, porém usando um meio, que no caso, é a internet.

É de suma importância a classificação dos crimes virtuais para distinguir os crimes e, assim, aprofundar-se neles. Mas, com o avanço da tecnologia e da rapidez fica difícil adequar as redes de computadores e internet.

Cabe ressaltar que existe uma dificuldade em punir tais ações cometidas no âmbito virtual, pela ineficácia de legislação, visto que o ordenamento jurídico preza pela lei expressa, não punindo crimes que não estejam previstos no Código Penal.

Há certas condutas ilícitas em que o agente comete crimes já previstos no ordenamento, utilizando-se de meros conhecimentos informáticos para cometer infrações penais. Um possível impedimento para esses tipos de ações seria uma tipificação que englobasse todos os atos infracionais cometidos no ciberespaço.

## 1.2 OS DIREITOS DOS USUÁRIOS

O acesso à internet cresceu ao decorrer do tempo, trazendo uma comodidade aos usuários, uma facilidade em realizar afazeres sem sair da zona de conforto, a comunicação com outras pessoas também ficou de fácil acesso. As notícias que antes eram apenas transmitidas via televisão, hoje em dia podem ser acessadas em sites jornalísticos. Ao realizar compras em sites ou criar e-mails, todos os dados cadastrais e pessoais dos usuários ficam à mercê dos infratores.

O acesso à internet nos proporciona muitas vantagens, algumas citadas acima, mas, traz também suas desvantagens e riscos diários. A criminalidade acompanha as inovações tecnológicas, motivo pelo qual os crimes aumentaram.

Observa-se como exemplo uma matéria do canal R7, no Estado de São Paulo, Rio de Janeiro e Minas Gerais no ano de 2019 e 2020:

> Em 2020, houve um aumento de 265% nos crimes praticados no ambiente virtual no Estado de São Paulo. No Rio de Janeiro, durante o período de isolamento, os casos de golpe na internet tiveram um aumento de 11,8% do total de crimes, segundo o ISP (Instituto de Segurança Pública). Em Minas Gerais, o número de crimes virtuais teve uma alta de 50% em 2020, segundo informações da polícia civil.

> [...] No total, em São Paulo, foram 1.492 crimes praticados no ambiente virtual em 2019, contra 5.441 casos em 2020. Dentre estes, o crime de estelionato subiu de 621 ocorrências em 2019 para 3.215 em 2020.

Nota-se que a criminalidade antes era grande, mas com o início da pandemia (COVID-19) em meados de 2019 e 2020, o acesso à internet cresce e junto dela cresce a criminalidade. Este contexto será mais aprofundado no decorrer dessa pesquisa.

O Direito trabalha duramente para acompanhar e criar leis para punir os infratores, pois, pessoas físicas e jurídicas têm direito à privacidade e ter uma certa segurança ao compartilhar seus dados pessoais na internet, em sites, e-mails, etc.

Os crimes digitais tiveram uma importância maior após a criação da Lei 12.737/2012, conhecida mundialmente como Lei Carolina Dieckmann. A legislação tenta ser eficaz, mas existe uma gravidade em punir os infratores.

Por isso, quando se cria uma legislação para combater certo delito, aparecem outros crimes para serem combatidos, ficando cada vez mais difícil acompanhar. O crime cibernético cresce cada dia mais, o que exige novas legislações que adéquem às novas tecnologias e não virem problema social.

Os debates surgiram, a busca constante pela aplicação penal também. Sendo assim, no ordenamento jurídico foi acrescentada a Lei Federal de nº: 12.737/12, conhecida como Carolina Dieckmann, publicada no ano de 2012. Sua criação possibilitou algumas alterações no Código Penal Brasileiro, sendo adicionado os Artigos 154-A (que trata da “invasão de dispositivo informático”) e 154-B, que aborda a conceitualização de crimes cibernéticos e suas demais características.

Assim, presente os Artigos:

> 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.
>
> Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

É notório que no artigo estão presentes duas finalidades, sendo a primeira o ato de invadir o dispositivo informático violando o mecanismo de segurança, com o objetivo de adulterar, introduzir ou destruir dados pessoais ou arquivos de informações. Já a segunda é a ação de invadir o dispositivo informático alheio, instalando um acervo impróprio, com o intuito de obter vantagens indevidas.

Neste contexto, conforme Nunes (2016, p.18):

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade.

Contudo, a Constituição Federal traz em seus artigos normas que protegem a liberdade de expressão, direito da personalidade e o direito à privacidade, que vem ampliando conceitos, porque, muitas das vezes, os delitos no mundo virtual afetam a honra de um indivíduo e a sua imagem.

Um dos casos mais comuns que se enquadram na tipificação de crimes cibernéticos é a falsidade ideológica, na qual o sujeito ativo cria uma conta “fake”, com fins de se apropriar dos dados pessoais da vítima para obter lucros ilícitos.

Em contrapartida, um dos casos que mais crescem é o estelionato, este que um indivíduo não identificado tenta obter para si vantagem ilícita em face de uma pessoa, pedindo valor em dinheiro, ou até mesmo clonando sua conta de "whatsapp" e mandando mensagens para os contatos solicitando depósito em determinada quantia.

Assim, explica Ferreira (apud Carneiro, 2012, s/p) sobre condutas criminosas em sistemas de informática que existem:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Sem dúvidas, a internet é uma rede vasta, onde circulam informações verdadeiras e ao mesmo tempo mentiroso. E provavelmente a sociedade e algumas empresas não sabem a dimensão sobre a prática criminosa na internet, e nem conhece riscos e possíveis prejuízos futuros, apenas por entregar dados cadastrais na internet, para trabalhos, para efetuar compras, etc.

Em suma, destacamos outra Lei que foi criada para proteger e garantir direitos fundamentais dos indivíduos, além de assegurar os dados pessoais fornecidos a empresas públicas e privadas no momento do cadastro. A referida é conhecida pelas siglas LGPD - Lei de Proteção de Dados Pessoais, sob nº: 13.709/2018.

Conforme Peck e Patrícia Pinheiro (2018, p.15):

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolve o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

É fruto de um amplo debate com a sociedade, empresas e órgãos públicos com o intuito de proteger os dados dos clientes. Uma sanção expressa na referida Lei é uma simples advertência que se aplica uma multa de até 2% do valor do faturamento da empresa caso os dados de algum cliente seja violado.

Enfim, a empresa é responsabilizada pelos danos causados. Todas as empresas que coletam dados dos seus clientes devem se adequar às normas da lei LGPD, protegendo seus dados pessoais.

Cabe frisar que a Constituição Federal de 1988 é de suma importância para os brasileiros. Nela estão previstos direitos fundamentais e garantias que asseguram a dignidade da pessoa humana, protegendo o indivíduo de qualquer ato que se caracteriza como crimes ou abusos que está sujeito durante o dia-a-dia.

Aqui se destaca um dos principais artigos da Carta Magna, Art. 5º da CF/88, Inciso X, que aborda o tema em questão:

> Art.5º- Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

A violação da honra humana é presente na vida fora da internet. Mas, com o crescente acesso de usuários na esfera digital, ficou mais constante os ataques, e muitas das vezes o direito à privacidade é ferido, sendo cada vez mais imperceptível,

pois algumas pessoas não sabem quando sua honra, direitos e dados pessoais são violados em sites ou plataformas digitais..

Diante disso, José Serpa (1987) efetua uma explicação mais complexa sobre o conceito de privacidade:

> Um modo específico de vivência pessoal, isolada, numa esfera reservada, consoante escolha espontânea do interessado, primacialmente dentro do grupo familiar efetivo, ou com maior insulamento, mas sempre sem uma notória forma de participação de terceiros, seja pelo resguardo contra a ingerência ou molestamento malevo alheio, seja pela utilização da faculdade que se lhe é atribuída para razoável exclusão do conhecimento público, de dados, ações, ideias e emoções que lhe são peculiares (SERPA, 1987, p.55).

A vida privada, a honra, a imagem e a moral são exemplos de privacidade que são direitos fundamentais do ser humano, ora invioláveis. O direito de privacidade deve ser tratado de forma delicada, pois envolve questões, como informações pessoais, trabalho, família, arquivos confidenciais, cabendo exclusivamente ao indivíduo decidir para quem, onde e o que fazer com as informações pessoais. Somente ele tem o direito de transferir, alterar ou apagar os dados pessoais, no manuseio de sua rede social que é de uso privado.

## 1.3 CRIMES CIBERNÉTICOS NA ESFERA DA LEGISLAÇÃO BRASILEIRA

Em 31 de outubro de 2012, segundo Vargas e Ricci (2013), “o Senado aprovou uma Lei que tipifica os crimes virtuais, inserindo penalidade em relação ao acesso virtual e divulgação não autorizada de informações pertencentes a outras pessoas contidas em meio eletrônico”.Em virtude disso, foi sancionada a Lei 12.737, que ficou conhecida como Lei Carolina Dieckmann, publicada em 30 de novembro de 2012.

Tal lei foi criada com o intuito de punir indivíduo que acessa meios eletrônicos com o intuito de obter ou adulterar dados pessoais e/ou financeiros de pessoas físicas ou jurídicas, sem o consentimento dos usuários.

A maioria desses indivíduos opera através de um meio eletrônico não identificado, agindo intencionalmente, compartilhando vírus de computador e malwares (um programa malicioso programado para causar dano ao computador), com o intuito de capturar senhas e/ou arquivos pessoais, causando prejuízos alheios.

Identificar o autor de um crime cibernético é muito difícil e necessita de provas concretas e de uma boa investigação, por vez que necessita da: “identificação dos

sujeitos uma vez que a produção de provas que evidenciem a configuração do crime e a adequação dessa modalidade de crime praticado em âmbito virtual com os crimes em espécie já previsto em lei é precária" (Carneiro, 2014).

A respeito dessas dificuldades em descobrir os infratores, houve a necessidade de criar leis que se adequassem à realidade, com o intuito de amenizar a criminalidade no âmbito virtual.

David Rechulski (ROVER, 2012) considera a Lei positiva afirmando que "para a caracterização do crime de invasão, é preciso que o sistema computacional esteja protegido por um mecanismo de proteção, pois a lei fala em 'violação indevida de mecanismos de segurança'. Assim, se não houver tal barreira, como um firewall ou senhas de proteção, não haverá, sob o prisma tecnicamente penal, indevida violação".

Por conseguinte, o ordenamento tem que priorizar o meio ou a forma que o delito foi praticado. O crime é cometido no meio virtual, existindo uma debilidade do usuário reagir e se defender de um ataque, em vista a crimes praticados no cotidiano.

É notório que se um computador não tiver um firewall, isto é, um programa de uma rede de computador que protege invasões futuras desconhecidas, protegendo o computador como se fosse uma muralha, ele estará muito mais propenso a ser invadido por criminosos.

Sustentando a tese, Blum (2012) diz:

> É evidente que a lei restringe a tipicidade da invasão aos casos em que há violação indevida de mecanismo de segurança, sendo assim, os dispositivos informáticos não dotados de ferramentas de proteção estariam excluídos da aplicação legal. Mas em se tratando de expressões como mecanismos de segurança e dispositivos informáticos como, por exemplo: hardwares e softwares não foram definidos na lei, restando dúvidas sobre o completo enquadramento de certos casos.

Nos dias atuais é indiscutível que a legislação não está conseguindo acompanhar o avanço da tecnologia, e consequentemente os delitos na esfera virtual crescem. Se a legislação não consegue acompanhar a criminalidade virtual no cotidiano, surge um grande empecilho para o desenvolvimento de soluções para evitar os crimes cibernéticos.

Nas palavras de Crespo: "a evolução tecnológica da sociedade supõe uma evolução tecnológica dos ilícitos, tanto nos meios quanto nos objetos".

A maioria dos crimes praticados virtualmente estão tipificados no Código Penal Brasileiro. A internet foi apenas um meio que os infratores utilizam para aproveitar que

houve um avanço tecnológico e que cresceu o acesso dos indivíduos para cometer crimes já existentes na legislação.

Neste ínterim, existe uma incógnita se há necessidade em implementar uma legislação para punir crimes cometidos na esfera virtual, visto que tais crimes têm sua lei expressa. Por outro lado, a Lei Carolina Dieckmann logrou êxito no crime de invasão, que se tornou evidente após o fato ocorrido com a referida atriz.

A tecnologia enfrentou barreiras buscando melhorias para os usuários, dando um certo conforto e agilidade para os mesmos. Entretanto, a legislação também enfrentou obstáculos para adequar-se à tecnologia. No passado não tinha a necessidade de criar uma legislação, visto que para algumas pessoas seria uma invasão de privacidade.

Com o tempo, a criminalidade foi aumentando, tanto na vida real quanto na digital. Com o avanço da tecnologia, os infratores também aperfeiçoaram a forma de cometer delitos, e houve a necessidade de criar leis, com o intuito de minimizar a criminalidade, visto que a Legislação é o espelho da sociedade, é uma segurança que os indivíduos têm para se resguardar de ações futuras que venham a atingir sua honra e imagem.

Em termos sociológicos foi fator determinante a aprovação da Lei 12.737/2012, a ocorrência de escândalos reiterados de vazamento de fotos íntimas que passaram a afetar um número cada vez maior de pessoas, fazendo com que houvesse uma pressão social sobre o legislativo para que houvesse o endurecimento das penas envoltas a este tipo de delito (BARBOSA et al, 2014).

No capítulo a seguir, abordaremos a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, envolvendo a atriz.

## 2. LEI 12.737/12 (CAROLINA DIECKMANN)

A Lei Federal nº: 12.737/2012, promulgada em 02 de Dezembro 2012, foi nomeada como Lei Carolina Dieckmann, após um episódio envolvendo a referida atriz. A Lei em questão surgiu para realizar alterações no Código Penal Brasileiro, tipificando os delitos e crimes cometidos no âmbito virtual. Adveio do Decreto Lei 2.793/2015.

A protagonista, a atriz Carolina Dieckmann, foi vítima de uma invasão no seu dispositivo, seguida de extorsão. Após ter suas fotos e vídeos íntimos compartilhados na rede e recusando-se a pagar a propina.

Vejamos o texto legal.

> LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei: Art. 1o Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: "Invasão de dispositivo informático Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4o Na hipótese do § 3o , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." "Ação penal Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos." Art. 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 Art. 266. ..... 60 § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR) "Falsificação de documento particular Art. 298. ..... Falsificação de cartão Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR) Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial. Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República. DILMA ROUSSEFF José Eduardo Cardozo (BRASIL, 2012, F).

A Lei foi sancionada em 30 de novembro de 2012 acrescentando os Artigos 154-A e 158-B do Código Penal Brasileiro, tipificando as condutas delituosas

praticadas no âmbito virtual, muito comum na sociedade brasileira e estrangeira, protegendo a liberdade individual dos usuários.

A tipificação foi essencial, pois, o ordenamento jurídico antes da lei ser sancionada não tinha uma sanção branda punitiva para delitos virtuais. Mas, mesmo com a legislação existem lacunas a serem respondidas, pois, o Artigo 154-A pune os criminosos que infringirem sistemas de informações com senhas.

Conforme explica em seu artigo, BERTOLDI, PAIXÃO, STEPHENS NETO, Júlio (2020, np.00):

> Passamos agora por uma segurança fantasiosa, pois a lei está aí para julgar os responsáveis por crimes da internet, porém é muito falha, talvez até acobertando os criminosos, uma vez que deixa brechas para que os mesmos se safem sem problemas e por mais que sejam pegos não garante que sejam punidos, caso a vítima não possua algum dispositivo de segurança os mesmos não cometeram crime, pois não se pode invadir o que está aberto.

As invasões aos dispositivos podem ser em computadores, smartphones, notebooks, celulares, tablets, etc… Estes podem estar conectados ou não a uma rede de internet, que às vezes não possui proteção, caso venha a ser invadida.

Para se enquadrar na legislação, o criminoso deve ter a intenção de adulterar, oferecer, produzir ou destruir dados informáticos. Devem em conjunto encaixar-se em rolls taxativos das condutas delituosas, obtendo um resultado danoso, não autorizado pelo responsável do dispositivo.

Em suma, caso os dados obtidos pelo cibercriminoso sejam divulgados na rede de internet com o intuito de adquirir vantagens ilícitas com os mesmos, a punição é a pena pode ser aumentada de 1(um) a 2(dois) terços. Caso seja praticado em face de pessoas com “cargos de potência máximos” a pena é aumentada de 1/3(um terço) ou até a metade.

Nos termos do § 5º, do art. 154-A do Código Penal, § 5º (BRASIL,1940)

> 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;
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Entretanto, a ação é penal pública condicionada, isto é, a vítima precisa oferecer a denúncia e deseja representar criminalmente em desfavor dos criminosos.

Caso seja cometido contra a Administração Pública, Estado ou União, o próprio Ministério Público pode oferecer denúncia e representar.

Nessa linha, para evitar supostas invasões, existem mecanismos de seguranças que podem ser instalados nos aparelhos informáticos, como forma de proteger invasões de cibercriminosos. A criação da Lei é de extrema importância para o combate dos crimes cibernéticos.

Assim, descreve Pedro Beretta (2014, np. 00):

> [...] demonstrou, mesmo que de forma equivocada, a preocupação do Estado em tutelar diversas mudanças trazidas pela tecnologia da informação, sendo de grande importância o reconhecimento de medidas para proteger os aspectos de liberdade individual do cidadão e também eventuais prejuízos de ordem material originários de uma “nova prática ilícita”.

A referida Lei surgiu com o intuito de proteger os usuários dos perigos a que eles estão sujeitos no dia a dia. Com a nova modalidade de crimes virtuais a solta na internet, que crescem a cada passo que a tecnologia avança, os crimes cibernéticos adaptam-se às mudanças.

Todavia, no ordenamento jurídico existia uma fragilidade de leis, para tratar o assunto mais a fundo. Com isso, os crimes cibernéticos cresciam, porque as pessoas não davam importância. E muitas das vezes, algumas por serem leigas sobre o tema não sabiam sobre seus direitos e as penas cabíveis para os crimes virtuais.

Assim, complementando Tânia Maria Cardoso Silva Amâncio (2013, p.28):

> A fragilidade das leis brasileiras foi um dos fatores que mais contribuíram para que surgissem novos crimes, especialmente nos últimos vinte anos, no ambiente virtual. É certo que muitas condutas podiam ser abrangidas por disposições já existentes na Constituição Federal, no Código Civil, no Código Penal, no Estatuto da Criança e do Adolescente, mas a criação de leis específicas para este tipo de criminalidade se tornou cada vez mais impositiva. […]. Nesse sentido, merece destaque a Lei Carolina Dieckmann, que pode ainda se apresentar limitada, porém se revelou um grande salto na proteção às vítimas de crimes perpetrados na internet.

A criação da Lei foi de extrema importância para as pessoas, passando uma sensação de segurança para os usuários navegarem na internet. Nota-se que a Lei não protege somente o dono do meio virtual, pois em um caso de invasão envolve terceiros, e com isso todos serão vítimas.

Percebe-se que a criação da Lei se reflete no contexto social do dia a dia dos indivíduos, tendo em vista o problema envolvendo a atriz global, Carolina Dieckmann, ao ter seu meio eletrônico invadido por hacker, impulsionando a criação da mesma.

Para Reale (2000, s/p):

> O Direito não é apenas a norma ou a letra da lei, pois é muito mais do que a mera vontade do Estado ou do povo, é o reflexo de um ambiente cultural de determinado lugar e época, em que os três aspectos – fático, axiológico e normativo – se entrelaçam e se influenciam mutuamente numa relação dialética na estrutura histórica.

As Leis são espelho de certos delitos cometidos perante a sociedade, com o intuito de combater atos ilicitamente praticados na população. O Estado tenta de todas as formas criar leis que se enquadram no padrão da sociedade, verificando os problemas sociais que a população anda enfrentando na vida, também no trabalho, na hora do lazer, etc.

A seguir abordaremos alguns crimes que são praticados na internet, que tem suas tipificações no Código Penal, e que vem crescendo no âmbito virtual com aumento de usuários a cada passo que a tecnologia avança.

## 2.1 CRIME DE EXTORSÃO INCORPORADO NOS CRIMES CIBERNÉTICOS

No crime de extorsão, o agente constrange a vítima mediante violência ou grave ameaça, com o intuito de obter vantagens ilícitas. O crime de extorsão encontra-se tipificado no art. 158 do Código Penal, “Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: Pena - reclusão, de quatro a dez anos, e multa”.

Na visão de Cléber Masson (2018, p.447):

> A extorsão é crime pluriofensivo. A lei penal tutela o patrimônio, principalmente, pois o delito está previsto entre os crimes contra o patrimônio, mas não se olvida da integridade física e da liberdade individual, uma vez que para executá-lo o sujeito se vale de grave ameaça ou violência à pessoa. É preciso destacar que o patrimônio, como bem jurídico protegido pelo art. 158 do Código Penal, há de ser compreendido em sentido mais amplo do que a propriedade e a posse, ao contrário do que se dá no furto e no roubo, pois o tipo penal fala em “indevida vantagem econômica". Destarte, qualquer que seja a vantagem patrimonial obtida ou procurada pelo agente, em detrimento da vítima, estará caracterizado um dos requisitos da extorsão. De fato, é patrimônio, no contexto do crime em apreço, todo bem ou interesse cujo sacrifício representa, para o seu titular, um mal maior do que o prejuízo patrimonial correspondente à vantagem exigida pelo extorsionário. São exemplos de tais bens ou interesses a honra, a tranquilidade pessoal ou familiar, o crédito comercial etc. Contrariamente ao sustentado pela maioria da doutrina, não consideramos correto classificar a extorsão como crime complexo. Como se sabe, crime complexo é o que resulta da fusão de dois ou mais crimes (exemplos: roubo, latrocínio, extorsão mediante sequestro

> etc.). E, no terreno do delito tipificado pelo art. 158 do Código Penal, não se verifica tal fenômeno. Com efeito, a extorsão nada mais é do que uma espécie do g nero “constrangimento ilegal” C , art. 146: é o constrangimento ilegal qualificado pelo fim de indébita locupletação e que, por isso mesmo, é trasladado para a órbita dos crimes contra o patrimônio. n cleo do tipo é “constranger”, exatamente como no constrangimento ilegal, e no restante da descrição da conduta criminosa não se verifica a presença de nenhum outro comportamento que, por si só, constitua crime autônomo. Trata-se, portanto, de um constrangimento ilegal com finalidade específica. E nada mais.

Neste contexto, o crime de extorsão preza pela proteção do patrimônio da vítima, mas também pela inviolabilidade dos usuários que tiveram sua honra violada. Para exemplificar como este delito é praticado na esfera virtual, por sua vez, o agente cria perfis “fakes” usando fotos de menores de idade, muita das vezes, meninas, com um padrão de beleza que chama a atenção dos usuários, para aplicar golpes em homens entre 30 a 60 anos, inocentes e leigos de informações.

Em seguida, o perfil “fake”, usando a foto da suposta jovem indefesa, ganha os homens na conversa até conseguirem fazer com que eles encaminhem fotos sensuais, em troca ela fala que encaminhará também fotos sensuais, que são imagens tiradas em sites inapropriáveis.

Após trocas de conteúdos, entra em contato com a vítima, através da rede social ou de aplicativo de "whatsapp", um suposto genitor da menor, ou Advogado, ou até mesmo Delegado. Este profere ameaças em face da vítima, alegando que ele pode ser preso pelo crime de pedofelia, por compartilhar fotos íntimas com uma menor de idade, e para que isso não ocorra ele deverá pagar uma certa quantia em dinheiro que os criminosos estipulam.

Cabe frisar que a maioria dos homens que são vítimas de extorsão na internet depositam o valor pedido, às vezes por serem casados não contou para a esposa, ou até mesmo por “carregar a culpa” por terem praticado um crime ao encaminhar fotos impróprias para a suposta menor, que no caso são criminosos aplicando golpes em pessoas indefesas e sem informações a respeito desse tipo de delito virtual.

Um exemplo de crime de extorsão na esfera cibernética foi o caso envolvendo a atriz, Carolina Dieckmann, no ano de 2012. Carolina foi vítima do crime de extorsão, em virtude disso foi criada a Lei 12.737/12 que ficou conhecida pelo nome da atriz, em decorrência do episódio ocorrido com ela.

A atriz teve suas fotos e vídeos íntimos vazados, após supostamente hackers invadirem seu sistema informático, e eles ordenaram a mesma realizar pagamento de

determinada quantia para não ter suas fotos e vídeos vazados. Recusou-se e os arquivos tornaram-se públicos.

O crime de extorsão cada vez mais se torna frequente no âmbito virtual, fazendo vítimas e causando prejuízos alheios. O anonimato reina, e muitas das vezes as pessoas não sabem com quem realmente conversam nas redes sociais, e em sites de relacionamentos. As pessoas precisam ter mais cuidado ao compartilhar fotos para desconhecidos, pois, eventuais futuras fotos podem se tornar um meio para a prática do crime de extorsão.

O crime de extorsão diferencia os crimes de furto e roubo, isto porque nos referidos crimes o autor precisa estar presente para apropriar-se de coisa alheia, sendo com grave ameaça, como no roubo, ou sendo sem grave ameaça, como no furto. Mas, no crime de extorsão, o autor pode invadir um dispositivo e apropriar-se de arquivos íntimos, ameaçando a vítima virtualmente ou presencialmente para não divulgar os materiais.

Em suma, podemos destacar que outro crime muito praticado no meio virtual é o crime de estelionato, que não é praticado com grave ameaça, e sim obtendo vantagens ilícitas em prejuízo alheio, e que abrangeremos no capítulo a seguir.

## 2.2 CRIME DE ESTELIONATO NA ESFERA CIBERNÉTICA

Diferentemente do crime de furto e roubo, o estelionato é um crime que o agente age de forma fraudulenta, uma conduta no meio digital, induzindo a vítima ao erro que aparentemente é imperceptível de tão bem planejado. Julio Fabbrini Mirabete (2008, p. 287) entende que:

> Existe o crime, portanto, quando o agente emprega qualquer meio fraudulento, induzindo alguém em erro ou mantendo-o nessa situação e conseguindo, assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia.

O principal foco do estelionato é o patrimônio, o agente não age de forma violenta, o objetivo é enganar, aplicar golpes e outros meios fraudulentos, com o intuito de enganar e, assim, conseguir obter o patrimônio de alguém.

Há casos que os criminosos adulteram boletos bancários, clonam anúncios de vendas de veículos e reposta com um valor inferior e com isso faz uma intermediação de venda, envolvendo terceiros que pagam por um bem material que não terá posse.

O crime de estelionato está tipificado no Art.171 Caput do Código Penal Brasileiro, que diz:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de quatro a oito anos, e multa.

No crime de estelionato, o agente entra na mente da vítima, convencendo-a a cometer um erro, agindo de má-fé, criando uma confiança, para conseguir o que deseja. A ação é muito bem planejada, tanto que a vítima confia, não percebendo que está caindo em um golpe.

A prática do estelionato virtual cresce conforme a tecnologia avança. As formas e os meios de cometer o delito ficam fáceis e aperfeiçoam a cada modalidade e com as inovações criadas no mercado virtual.

Nesse contexto, um exemplo de estelionato cometido no âmbito virtual foi o golpe do boleto fraudado, através do aplicativo de whatsapp ou em sites não confiáveis. Muitas das vezes as pessoas acessam o site de uma determinada loja para emitir o boleto, e no referido site possui um número que dá acesso ao whatsapp, e através deste solicitando o documento.

Ao emitir a segunda via do boleto, esta sai adulterada e no instante que a vítima efetua o pagamento da fatura ele não é debitado na loja e sim numa conta de terceiros. Às vezes vem até mesmo escrito o nome do beneficiário, que no caso é um estelionatário que “hackeia” o site ou clona o número da loja, aplicando golpes. E tomado pela sensação de segurança e confiança o cliente sequer confere e paga.

Em suma, é muito difícil identificar um estelionatário, eles têm uma inteligência em criar situações para causar prejuízo a terceiros, que às vezes não deixam provas. E muitas das vezes as Delegacias não são especializadas em investigar esses tipos de crime mais a fundo, deixando em vão, criando uma sensação de impunidade e fazendo com que a vítima desista de ir a diante.

## 2.3 CRIMES CONTRA A HONRA NO MUNDO VIRTUAL

O crime contra a honra acontece quando atinge a honra subjetiva e objetiva de um indivíduo, denegrindo a imagem e honra, infringindo os elementos físicos, intelectuais e morais, oriundos do princípio da dignidade da pessoa humana, um direito inviolável como descrito na Constituição Federal.

O Código Penal Brasileiro no seu Capítulo V, Título I da Parte Especial dispõe dos crimes contra a honra. São eles: calúnia, difamação e injúria.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa [...]
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa [...]
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. [...]

Os crimes contra a honra são também praticados presencialmente, mas na maioria dos casos acontecem na esfera virtual, através de redes sociais, aplicativos de whatsapp, contas fakes, denegrindo a imagem do indivíduo, com comentários maldosos e de baixo calão.

A honra objetiva diz respeito a imagem do indivíduo perante a sociedade, sua reputação, o que as pessoas pensam sobre si. Já a honra subjetiva aborda a face de si próprio, a imagem que tem de si mesmo.

Rogério Greco (2012) fala:

> A chamada honra objetiva diz respeito ao conceito que o sujeito acredita que goza no seu meio social. [...] Já a honra subjetiva cuida do conceito que a pessoa tem de si mesma, dos valores que ela se auto atribui. [...] Honra subjetiva e honra objetiva são conceitos que se interligam, gerando, na verdade, um conceito único. [...] Não podemos considerá-las de forma estanque, completamente compartimentadas (GRECO, 2012, p. 400).

Os crimes contra a honra - calúnia, difamação e injúria - são de ação penal privada, crimes de menor potencial ofensivo, necessitando de um advogado para realizar a queixa-crime e assim iniciar o procedimento na esfera judicial.

Os crimes contra a honra na esfera virtual podem ser praticados através de rede social, aplicativos de "whatsapp", denegrindo a honra, moral e a imagem das pessoas, com xingamentos ofensivos, como no crime de injúria, difamando a pessoa ou difamando a pessoa para terceiros, caluniando o indivíduo acusando-o por algo que não fez, como, por exemplo, acusar a pessoa de ladra, de ter praticado certo delito.

Os crimes contra a honra na internet podem ser praticados por familiares, amigos ou até pessoas não identificadas, prejudicando a vítima de forma direta ou indireta. Muitas das vezes tem autoria identificada, quando é pessoas próximas, mas tem caso que não é possível identificar o autor, como no fato de criar perfil falsos nas redes sociais, denegrindo a imagem da vítima e trazendo um prejuízo para sua honra.

Para realizar a queixa-crime dos delitos deve-se comparecer em uma Delegacia de Polícia, abrir um procedimento que é chamado de T.C.O (Termo Circunstanciado de Ocorrência), utilizado para crimes de menor potencial ofensivo. Para tanto, a vítima precisa saber a localidade do autor, ter provas e testemunhas, e tem o prazo de 6 meses para realizar representação criminalmente.

Neste ínterim, necessita-se de leis mais rígidas para crimes cibernéticos. Os danos crescem junto ao avanço tecnológico e com o número maior de usuários navegando na internet.

> A maioria dos crimes cometidos na rede ocorre também no mundo real. A internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital referem à territorialidade e a investigação probatória, bem como a necessidade de tipificação penal em algumas modalidades que, em razão de peculiaridades, merecem ter um tipo penal próprio (PINHEIRO, 2010. p. 296).

A legislação deve se adaptar às modificações no meio social e virtual, com o intuito de combater a criminalidade e resolver conflitos na sociedade. É de suma importância zelar e proteger a honra de um indivíduo, e o dever do Estado é garantir direito e garantias fundamentais.

## 2.4.PANDEMIA E OS CRIMES CIBERNÉTICOS

O avanço tecnológico trouxe diversas vantagens, acessibilidade, facilitando a comunicação entre os indivíduos. Vivemos no último ano uma pandemia, a COVID-19, conhecida como coronavírus, isto é, um vírus transmissível que paralisou o mundo.

Em decorrência da pandemia e para proteção social, o mundo precisou adaptar-se ao isolamento social, para a não perpetuação do vírus. Com isso, houve

uma série de mudanças, uma delas foi a adaptação do “home office ”, primeiramente para pessoas de risco.

Com o isolamento social, os meios de comunicação cresceram, e as redes sociais foram um dos meios para a interação da sociedade. Posteriormente, houve um crescente aumento de crimes cibernéticos, pessoas de má índole se beneficiando em prejuízo alheio em ato fraudulento. Um dos crimes de maior repercussão foi o estelionato, junto a extorsão, golpes de whatsapp, clonagem, e outros.

Muitos se perguntam o porquê do aumento dos crimes. Na perspectiva de Larissa Pinho de Alencar Lima (2020):

> ARTIGO ANUÁRIO PESQUISA E EXTENSÃO UNOESC SÃO MIGUEL DO OESTE – 2021 “Pela teoria econômica do crime, a ponderação realizada pelo criminoso passa pela (in)certeza da punição, a severidade e a celeridade da aplicação da pena, a probabilidade do reduzido tempo de prisão e até mesmo a possibilidade de prescrição”.

Neste contexto, podemos dizer também que a crise econômica e a falta de desemprego podem levar pessoas a buscar ganho material no mundo do crime, um meio que ganha dinheiro fácil, e um caminho sem volta para muitos criminosos: a morte ou a prisão.

Cabe frisar que na pandemia os casos de roubo e furtos diminuíram, pois a população, em sua maioria, estava em seus domicílios, saindo apenas em caso de extrema necessidade, como ir na farmácia, supermercado ou hospital, mas sempre prezando pelo distanciamento social, uso de máscara e higienização das mãos com uso de álcool em gel.

Por esse motivo, os criminosos tiveram que se adaptar ao meio que vivenciamos para praticar atos ilícitos. Como podemos ver nas palavras de Martins (2020, p. 02):

> Criminosos percebendo o uso massivo da rede mundial de computadores por grande parte da população mundial procuraram, rapidamente, adaptar-se à nova realidade para cometer fraudes eletrônicas, aproveitando-se do estado de medo e ansiedade que a pandemia e a necessidade de isolamento causam às pessoas.

As pessoas acreditaram que com o isolamento elas estariam protegidas da criminalidade, mas não. Somos vulneráveis e estamos sujeitos a risco tanto no cotidiano real quanto no mundo virtual. A maioria das pessoas tem a internet como

ferramenta de trabalho, estudo e demais necessidades, precisam ficar atentas que podem se tornarem vítimas de um crime virtual a qualquer minuto de distração, acessando uma página que não esteja protegida, clicando em links impróprios, realizando uma compra que o site tenha sido clonado. Com isso, deve-se desdobrar os cuidados, são pequenas coisas que fazem a diferença.

Cabe frisar que durante a pandemia surgiu várias Fakes news, notícias falsas sobre a calamidade do Brasil e do Mundo. E muitas das vezes as pessoas acreditavam, causando pânico na população.

Para Raul Galhardi(2019),com base em estudos de pesquisas, o Brasil é o país que mais acredita em notícias falsas e o que mais se preocupa com a veracidade de informações na internet.

> O Brasil vive um paradoxo. Pesquisas recentes revelaram que nós somos a sociedade que mais acredita em notícias falsas, ao mesmo tempo em que somos o país que afirma se preocupar mais com o que é falso e verdadeiro dentre as informações que circulam na internet. De acordo com estudo realizado em 2018 pelo instituto Ipsos, intitulado “Fake news, filter bubbles, post-truth and trust”, 62% dos entrevistados no Brasil admitiram ter acreditado em notícias falsas até descobrirem que não eram verdade, valor muito acima da média mundial de 48% (GALHARDI, 2019).

As notícias falsas causam um sentimento de impotência nas pessoas, de tristeza. Já basta estarmos vivendo em um cenário de calamidade, com a COVID-19, e ainda estarmos sujeitos a essa situação de fakes news e desinformação.

## 3. PROBLEMÁTICA

De acordo com o avanço tecnológico, o direito deve se adequar junto a sociedade que está em constante evolução. Ou seja, o mundo e a tecnologia estão cada vez mais aperfeiçoados e a população deve se adaptar às novas tecnologias, com isso, a legislação tem o dever de criar leis que assegurem direitos e garantias individuais para as pessoas.

De acordo com Patrícia Peck (2009, p.22)

> Ter uma janela aberta para o mundo exige muito mais que apenas a seleção do público-alvo. Exige a criação de uma logística jurídica que reflita a diversidade cultural dos consumidores/clientes virtuais. No aspecto de atendimento ao consumidor, por exemplo, parte das empresas inseridas na rede recorrem à terceirização, contratando contact centers especializados para atender a demanda de usuários de diferentes culturas e países. No aspecto jurídico, é preciso que os profissionais de Direito também estejam preparados para criar essa logística, sabendo que a todo o momento terão de lidar com diferentes normas, culturas e legislações.

A maioria das pessoas passa mais tempo em frente a um computador, seja trabalhando, estudando, pesquisando ou socializando com outras pessoas em lugares

distantes. Dessa forma, existe o lado bom como citado, e o lado ruim é que a sociedade está sujeita a riscos.

Neste diapasão, discorre que:

> A tecnologia digital é uma realidade, e justamente por isso estamos diante da criação de lacunas objetivas, as quais o direito tem dever de estudar, entender e, se necessário, preencher. Com a crescente popularização da grande rede, evidenciamos a criação de novos conceitos sobre valores tradicionais, tais como a liberdade, a privacidade e o surgimento de “crimes” digitais (CORRÊA, 2010, p. 21).

Os crimes cibernéticos começaram a surgir, fazendo novas vítimas, algumas leigas sobre o assunto, sobre as penas adequadas ou até aonde buscar por amparo, onde procurar, o local exato para notificar o delito, para que assim seja possível abrir uma investigação sobre o fato.

Muitas das vezes o anonimato que reina por trás da criminalidade, a ausência de vestígios e provas, são motivos que levam os usuários a desistirem de buscar a autoria do crime e dar segmento.

Sobre isso, argumenta Corrêa (2010, p.91).

> (...) Talvez o pequeno número de casos submetidos à polícia e a nossos tribunais faça com que a habilidade técnica para “fechar o cerco” a tais “crimes” deixe a desejar. Isso é preocupante, pois, como demonstrado anteriormente, a tendência é o aumento qualitativo e quantitativo de tais ilícitos.

Muitas das vezes faltam materialidade, provas concretas ou até mesmo delegacias especializadas para tratar mais a fundo o delito. Outra coisa que dificulta a investigação da Polícia é que os principais autores dos crimes virtuais são hackers ou crackers, especialistas em condutas criminosas no âmbito virtual.

Assim, explica Marcelo Xavier de Freitas Crespo (2011, p.95)

> Hacker" é o nome genérico dado aos chamados “piratas” de computador. Essa expressão surgiu nos laboratórios de computação do MIT (Massachusetts Institute of Technology), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com o computador. Apesar da fama de “criminosos virtuais”, nem todo hacker deseja o prejuízo alheio. Há aqueles que se dizem “hackers do bem”, pois invadem os computadores e deixam mensagens informando a vítima do risco existente, aconselhando-a a providenciar uma proteção mais efetiva. Outros passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear as invasões.

Ao contrário dos hackers, os crackers são invasores com um conhecimento elevado, capazes de invadir uma rede, quebrar um sistema de segurança virtual,

adquirir arquivos sigilosos, com fins de utilizar o que adquiriu para praticar condutas ilícitas.

Por outro lado, os criminosos que praticam certos crimes virtuais são pessoas que já estão presas e têm acesso ilegalmente a um aparelho celular e com isso tem livre acesso para cometer delitos, como, por exemplo, uma ligação telefônica, um estelionato, trotes muito bem calculados.

Muitas das vezes, os presidiários criam contas bancárias virtuais utilizando dados de terceiros, assim que a quantia é debitada a conta é cancelada, para não deixar vestígios.

Por isso, muitas das vezes fica na mente a questão do crime “ser perfeito”, considerando que a vítima não tem capacidade de procurar uma unidade especializada e realizar a denúncia, ou até mesmo por falta de provas ou documentos, pois os autores raramente deixam rastros, e por serem crimes muito bem planejados e por serem pessoas que já estão presas, as vítimas desanimam, ficando a sensação de impunidade.

Porém, existem meios para analisar e investigar o crime, como explica Wendt e Jorge (2012, p. 52/53):

> Análise das informações narradas pela vítima com intuito de preservar o material comprobatório do delito e sua proteção virtual;
> Orientações a vítima com o intuito de preservar o material comprobatório do delito e sua proteção virtual;
> Coleta inicial de prova em ambiente virtual;
> Formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a consequente instauração do feito;
> Investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre os prováveis autores, origens de e-mails, registro e hospedagem de domínios;
> Formalização de relatórios com certidões das provas coletadas e apuração preliminar;
> Representação perante o Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão e acessos. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdos;
> Análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdos.

As autoridades no âmbito das investigações buscam encontrar vestígios deixados durante a prática criminosa do meliante. Sendo que durante o procedimento, a procura inicial é sobre o ID da máquina invasora, visto que não existem 2 desfrutadores de um único IP.

Dessa forma, existem delegacias especializadas em cibercrimes, chamadas de “DELEGACIAS ESPECIALIZADAS EM CRIMES CIBERNÉTICOS”, que investigam minuciosamente o delito com o intuito de obter provas, para chegar nos supostos autores, visto que muita das vezes são anônimos, ou até mesmos presidiários.

Em suma, as Delegacias especializadas em crimes cibernéticos fazem uso de rede social para compartilharem operações e casos de vítimas que caíram em golpes virtuais. A divulgação acontece para que as demais pessoas vejam que a internet tem seu lado bom e ruim, e saibam dos riscos que estão sujeitos, e ainda que devem redobrar os cuidados, tentarem se proteger e olhar com mais austícia ao seu redor.

Por fim, as redes sociais são um meio de comunicação encontrado nos dias atuais, visto que com a evolução das tecnologias milhares de pessoas acessam os meios digitais para se comunicarem e compartilhar informações. O jornal que é transmitido pela televisão nacionalmente é muito importante, porém tem atingido cada dia mais um público menor, pois, a maioria das pessoas estão conectadas nas redes sociais e estão deixando de acompanhar as notícias via televisão, preferindo ficar alienados as redes sociais.

Dessa forma, a Polícia Civil e as Delegacias encontraram nelas um meio para compartilhar com a sociedade certos cuidados, exemplos e casos de vítimas, já que encontram um público grande de usuários navegando, principalmente durante a pandemia que o mundo se voltou para os meios de comunicação.

Mas em contrapartida, os meios utilizados para orientar os usuários não fez com que os crimes cibernéticos diminuíssem, pois as maiorias dos usuários não dão muita importância, ou até mesmo não seguem os cuidados recomendados. E quando se tornam vítimas de um crime virtual, não realizam denúncias sobre o caso, pela falta de coragem, a sensação de uma legislação, pela dificuldade de encontrar o autor e a falta de Delegacias especializadas em algumas cidades. São coisas que desanimam algumas pessoas a realizar a denúncia.

Com isso, segundo Pinheiro:

> “O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que, dessa forma, não passa às autoridades informações relevantes e precisas; b) a falta de recursos em geral das autoridades policiais.” (PINHEIRO, 2010, p. 227).

A falta de legislação encoraja os criminosos a praticar mais crimes virtuais que crescem com o avanço da tecnologia. A falta de informações dos usuários, os meios

de proteção que são importantes não são usados corretamente, abrindo portas para os crimes cibernéticos.

## CONSIDERAÇÕES FINAIS

Esse trabalho buscou mostrar como os crimes cresceram e evoluíram no meio virtual, ficando conhecidos como crimes cibernéticos. Cresceram a cada passo que a tecnologia avançou, trazendo um problema social que resultou na criação de leis para combater e solucionar os problemas da população.

O meio virtual tornou-se cada vez mais procurado pelas pessoas, servindo para trabalhar, estudar, busca de informações e praticidade. Com as novas maneiras de comunicação ficou mais fácil realizar compras virtuais, nacionais e internacionais, ampliando o campo da publicidade e entre outros fatores.

Com tantas vantagens que a internet nos proporciona, vem junto as desvantagens, o medo, o risco que estamos sujeitos. Os delitos virtuais estão tornando-se mais comuns, pela fragilidade das pessoas e pela inaplicabilidade correta da legislação.

O ordenamento jurídico é rico em leis, mas é insuficiente, não são aplicadas corretamente as penalidades nos casos de crimes virtuais. A ausência de Delegacias Especializadas em certas cidades, municípios, próprias para investigar casos cibernéticos é muito importante, pois, são policiais civis especializados naquela área, mas não têm sedes para todas as cidades.

Nota-se que os crimes vêm crescendo com o tempo, e durante certo tempo houve uma necessidade em criar leis, que protegessem os direitos dos usuários, rezando pela sua privacidade, sua honra, pois é um direito nosso.

Com isso, houve a criação de leis, como a Lei 12.737/12, o Marco Civil e a Lei Geral de Proteção de Dados, que recebem muitas críticas, pois na grande maioria dos casos os criminosos ainda ficam impunes. A aplicação das leis deveria ser mais severa, às vezes fica à mercê da justiça, soltando os criminosos para continuarem fazendo vítimas, ou até mesmo dentro da prisão eles têm acesso a aparelhos celulares que entram ilegais, e com isso usam para aplicar golpes, o monitoramento, redobramento de coisas que fazem a diferença.

O ordenamento não precisa de novas leis, existem muitas leis para proteger os direitos e garantias dos indivíduos, mas são aplicadas incorretamente. Outra coisa que melhoraria seria a abertura de mais Delegacias Especializadas que atuassem somente para amparar e investigar casos específicos de crimes cibernéticos.

No último ano vivenciamos uma pandemia, que mudou radicalmente o mundo. Precisamos nos adaptar a uma série de coisas para nos proteger e proteger o próximo. Com isso, várias empresas e pessoas tiveram que se adaptar ao trabalho home office. E mesmo com meios de proteção que impedem invasão de privacidade, muitas pessoas são vítimas dos crimes cibernéticos, sendo a invasão feita por um dispositivo informático, ou pelas redes sociais, numa compra com boleto fraudulento.

A maioria da sociedade não sabe sobre a existência dos crimes cibernéticos e nem que são vítimas. Isso ocorre pela falta de informação, pela falta de Delegacias Especializadas, para dar um suporte para as pessoas, e orientar do perigo que o meio virtual traz se não navegarmos com segurança e muito cuidado.

É de suma importância que os profissionais responsáveis pela investigação tenham mais suporte técnico, e que fossem criadas mais Delegacias Especializadas em investigar crimes virtuais, para investigar, localizar os infratores e puni-los pelo crime.

A tecnologia avançou, mas os meios de segurança e as leis ficaram impunes, fazendo com que os criminosos cometam mais delitos, pois sabem que a legislação é insuficiente, sabem que casos presos saem da cadeia e logo voltam a cometer mais crimes.

Conclui-se que existe a necessidade de uma legislação mais rígida, pois mesmo criando e tendo legislações formatadas, não é o suficiente para combater a

criminalidade no meio virtual, m decorrência das leis não serem aplicadas corretamente, junto a falta materialidade para qualificar o crime e, com isso, chegar a identificar a autoria.

Além disso, o que dificulta todo o processo é a falta de Delegacias Especializadas, para dar mais enfoque às investigações específicas de crimes cibernéticos. Elas também seriam de suma importância para orientar os usuários sobre a existência da criminalidade no âmbito virtual, orientando sobre o lado obscuro da internet, com o intuito de diminuir a criminalidade e mostrar que existem leis para os crimes, e que os usuários possuem direitos.

## REFERÊNCIAS


Anais do 10o **Congresso Internacional de Ciências Criminais** - PUCRS:Direito Penal (Vol. 3).

BERTOLDI, Maria Eugênia PAIXÃO, Celso Eduardo STEPHENS NETO, Julio AMÂNCIO, Tania Maria Cardoso. **O impacto da informática na sociedade e o direito no Brasil.** São Paulo: Revista Jurídica Consulex,2013

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico.** 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdadea-publicidade-e-o-direito-eletronico> Acesso em: 10 nov. 2020.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico,** Rio Grande, XV, n.99, abr. 2012.Disponível em:http://www.ambitojuridico.com.br/site/index.php/?n_link=r**evista_artigos_leitura &artigo_id=11529&revista_caderno=17**. Acesso em: 22 nov. 2014.

MASSON, CLEBER, **Direito Penal**, 2018, p.447.

**CRIMES DIGITAIS**,caderno de pós-graduação em, Direito, BRASILIA, 2020. https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021

Revista **Consultor Jurídico**, 20 de maio de 2020-https://www.conjur.com.br/2020-mai-20/larissa-pinho-crime-escolhido-base-analise-economica.

CORRÊA JÚNIOR RICHARLES SILVA(2020).

DILMA ROUSSEFF José Eduardo Cardozo (BRASIL, 2012, F)

FABRETTI, Humberto Barrionuevo; SMANIO,Gianpaolo Poggio. **Direito Penal-**parte geral (p.204)

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade:** parte I, Lineamentos e Definições. Boletim do Instituto Pedro Pimentel, São Paulo, v 13, n 2, 2000.

GRECO, Rogério. **Curso de direito Penal: Parte Especial: Volume 2.9** ed. Rio de Janeiro:Impetus,2012.

JESUS, Damásio de Estefam André. **Direito Pena**l,vol.1, parte geral 37ªedição. p. 39 e 40.

REALE, Miguel. **Teoria Tridimensional do Direito**. 5ª ed., Editora Saraiva, São Paulo, 2003.

PASCHOAL,Janaina Conceição: 2. edição 2015**.Direito Penal:** parte geral. p.28 e 29.

PECK, Patrícia Pinheiro. **Proteção de dados pessoais**. 2. ed. 2018.

PINHEIRO, Patrícia Peck. **Direito Digital. 4 ed. rev.,atual e ampl**. São Paulo: Saraiva, 2010.

Revista **Consultor Jurídico**, 10 de maio de 2014, 10h15.

**ROSSINI**, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, **2004**.p.110.

**SERPA, Jose de sta. Maria, Direitos da personalidade e a sistemática civil geral i**mprenta: São Paulo, Julex, 1987.p.55.

**Tadeu Rover (repórter da entrevista).**
https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=21D63FF916CA68DFD94D3FD8A2A1E724.proposicoesWebExterno1?codteor=1723447&filename=Avulso+-PL+1127/2019.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos, Ameaças e Procedimentos de investigação. Rio de Janeiro: Brasport, 2013. P.52/53.

http://www.repositoriodigital.univag.com.br/2016.