UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE HUMANIDADES
DEPARTAMENTO DE DIREITO

RUBENS JOSÉ MORAIS

A PROTEÇÃO DOS DIREITOS DA PERSONALIDADE ATRAVÉS DA LEI 12.737/2012

FORTALEZA
2019

RUBENS JOSÉ MORAIS

A PROTEÇÃO DOS DIREITOS DA PERSONALIDADE ATRAVÉS DA LEI 12.737/2012

Monografia, apresentada ao Curso de Direito da Universidade Federal de Ceará como requisito para obtenção do título de bacharel em Direito.

Orientador: Prof. Dr. Felipe Lima Gomes

Fortaleza - CE
2019

Dados Internacionais de Catalogação na Publicação Universidade Federal do Ceará

Biblioteca Universitária

Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M826p Morais, Rubens José.

A proteção do direito da personalidade através da lei 12.737/2012 / Rubens José Morais. – 2019. 67 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2019.

Orientação: Prof. Dr. Felipe Lima Gomes.

1. Personalidade. 2. Internet. 3. Privacidade. I. Título.

CDD 340

RUBENS JOSÉ MORAIS

A PROTEÇÃO DO DIREITO DA PERSONALIDADE ATRAVÉS DA LEI 12.737/2012

Monografia, apresentada ao Curso de Direito da Universidade Federal de Ceará como requisito para obtenção do título de bacharel em Direito.

Aprovada em 17 de Junho de 2019

Banca Examinadora:

_____

Prof. Felipe Lima Gomes (Orientador)
Universidade Federal do Ceará (UFC)

_____

Thiago do Vale Cavalcante
Universidade Federal do Ceará (UFC)

_____

Antônio de Holanda Cavalcante Segundo
Universidade Federal do Ceará (UFC)

Fortaleza - CE

2019

Dedico essa monografia a minha família que sempre me apoiou por todo o percurso da minha vida.

AGRADECIMENTOS

Agradeço ao bom Deus, pela minha vida, a vida dos meus pais, familiares e amigos.

A Universidade Federal do Ceará por ter me dado à oportunidade de realizar este curso.

Agradeço a este meu orientador, professor Felipe Lima Gomes, pela paciência, dedicação e ensinamentos que possibilitaram que eu realizasse este trabalho.

Agradeço aos meus pais, pelo amor, carinho, paciência e seus ensinamentos.

“Uma maneira de preservar sua própria imagem é não deixar que o mundo invada sua casa. Foi um modo que encontrei de preservar ao máximo meus valores.”

(Ayrton Senna)

SUMÁRIO

Resumo

A presente monografia vem analisar a efetividade da lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann na proteção dos direitos da personalidade. O avanço da sociedade da informação e das tecnologias da informação leva a uma reflexão acerca da importância dos direitos da personalidade e como eles estão sendo ameaçados.

A pesquisa para a produção desse trabalho foi focada em livros, para obter uma base teórica na doutrina dos jurisconsultos acerca das diferentes nuances do tema, e na internet, a fim de obter dados e informações atuais que remetem a realidade e gravidade do tema.

Ao final é perceptível que a lei ainda tem muito o que ser aprimorada, pois os defeitos que possui a tornam pouco efetiva. Apesar disso, sua importância se dá por ser uma lei que codifica um crime antes pouco perseguido pela Justiça.

Palavras-chave: Personalidade, Internet, Privacidade.

Resume

This monograph analyzes the effectiveness of Law No. 12,737 / 2012, popularly known as the Carolina Dieckmann Law in the protection of personality rights. The advancement of the information society and information technology leads to a reflection on the importance of personality rights and how they are being threatened.

The research for the production of this work was focused on books, to obtain a theoretical basis in the doctrine of jurisconsults about the different nuances of the theme, and on the internet, in order to obtain current data and information that refer to the reality and gravity of the theme.

In the end it is noticeable that the law still has much to be improved, because the defects that it owns make it ineffective. Despite this, its importance is given by being a law that codifies a crime previously little persecuted by Justice.

Key-words: Personality, Internet, Privacy.

Introdução

Nos últimos anos, a rede mundial de computadores, também denominada internet, se consolidou como parte essencial na vida dos seres humanos, estando presentes em quase todos os aspectos de sua vida como trabalho, relacionamentos, lembranças, entretenimento, entre outros. Da mesma forma que os facilitou, ao mesmo tempo, criou e pôs em xeque paradigmas sociais que desafiam o *status quo*.

Um dos direitos mais suscetíveis a essa mudança de paradigma são os Direitos da Personalidade, pois na internet, especialmente através das redes sociais, como Facebook, Twitter, LinkedIn, Blogger, YouTube, Skype, Instagram, Snapchat, as pessoas são expostas e se expõem, conversam entre si, divulgam informações e dados umas para as outras, não só para fins de comunicação, mas também para a obtenção de serviços. Enfim, elas têm, *a priori*, por vontade própria, a si mesmas expostas; dessa forma a sociedade pode percebê-las através de sua exposição nas mídias sociais e criar um juízo dela.

A lei 12.737/2012, popularmente denominada lei Carolina Dieckmann, traz consigo uma grande rede de conexões tanto com diferentes ramos do direito como com o mundo da informática, levantando assim sua real relevância para a sociedade. São os direitos da personalidade os que mais são resguardados pela lei e, portanto, os que devem receber maior atenção, valendo ressaltar que esse é o conjunto de direitos mais salutares ao ser humano.

Portanto esse trabalho vai observar como a lei se interconecta esses diferentes ramos do direito, analisar como o mundo da informática se relaciona com o mundo do direito e verificar se a lei de fato é efetiva no que se propõe a cumprir e se ela de fato protege os direitos da personalidade.

Capítulo 1 – Os Direitos da Personalidade

Os direitos da personalidade são um conjunto de direitos inerentes à sua personalidade, entendida esta como as características que a distinguem como ser humano, ao mesmo tempo em que integra a sociedade e o gênero humano. São características inerentes ao indivíduo, que se intuem facilmente, que até dispensariam menção, dada sua inarredabilidade da condição humana, e que configuram pressuposto da própria existência da pessoa, mas que nem sempre são fáceis de explicar (MONTEIRO, 2012, p.102).

A legislação brasileira abarca os direitos da personalidade em diferentes códigos, na Constituição Federal, esses direitos são expressamente defendidos e pormenorizados em diferentes elementos para ampliar sua defesa; no Código Civil, esses direitos são protegidos na perspectiva da integridade física, o corpo humano do individuo, e moral, a constituição psíquica do indivíduo; e no Código Penal os direitos da personalidade são bens jurídicos dignos de proteção, caso sejam infringidos o infrator deve ser punido.

1.1 - Esfera Constitucional

A Carta magna defende o Direito da Personalidade como reconhecimento a individualidade da pessoa, isto é, mesmo em vivendo sociedade, em meio a tantas pessoas, é um ser único dotado de sua própria vontade, desejo e ideal que a singulariza perante a coletividade. A Constituição de 1988 reconhece que a pessoa é detém direitos inerentes à sua personalidade, entendida esta como as características que a distinguem como ser humano, ao mesmo tempo em que integra a sociedade e o gênero humano. Tais características não inerentes ao indivíduo, que se intuem facilmente, que até dispensam menção, visto que são inseparáveis da condição humana, e que nem sempre são fáceis de explicar (MONTEIRO, 2012, p.102).

A personalidade não constitui um direito em si, mas ao contrário, ela é objeto de direito, pois é o primeiro bem que a pessoa tem ao nascer, ser quem ela é, isso é algo que possuirá por toda sua vida, e usará para conviver com outros membros da sociedade, até o dia de seu falecimento. Vale apontar que por serem tão intrínsecos, tão íntimos ao ser humano que nenhum ordenamento jurídico pode deixar de reconhecer a importância desses direitos.

O ser humano necessita de uma reclusão periódica à vida privada, pois isso constitui uma necessidade de todo homem, para a sua própria saúde mental. Pois, sem

privacidade não há condições propícias para o livre desenvolvimento da personalidade, pois estar submetido ao constante crivo da observação de outros dificulta o enfrentamento de novos desafios. A exposição constante dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muitas oportunidades para o indivíduo fazer uma avaliação de si mesmo, traçar perspectivas e cogitar metas (MENDES e BRANCO, 2017).

Não existem direitos e garantias irrefutáveis ou irredutíveis, pois a sociedade em si não o é. É uma sociedade fluida, que muda, que se transforma, que está sempre mudando de paradigmas. Ela cria e abole convenções sociais, como os direitos das mulheres, dos negros e dos homossexuais, que outrora foram tidos como cidadãos de segunda classe agora têm plenos direitos. O Poder Judiciário brasileiro reconhece tal fragilidade nos direitos, como aponta o Supremo Tribunal Federal, nas palavras do excelentíssimo ministro Celso de Melo no mandado de segurança N. 23.452-RJ/1999: “Os direitos e garantias individuais não têm caráter absoluto. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas – e considerado o substrato ético que as informa – permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros”.

1.1.1 Personalidade, segundo a constituição

No art. 5°, X da Magna Carta está escrito: “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”.

Por intimidade se entende como tudo aquilo de mais íntimo da pessoa, o que não quer que seja revelado nem para a família nem para os amigos, como sua vida amorosa, sua

opção sexual, seus segredos mais recônditos e suas convicções mais profundas; os quais, por vezes, são revelados a estes de forma que também mantenham segredo dessas informações.

A vida privada, por sua vez, não é o mesmo que intimidade, já que não é tão reservada para a própria pessoa. Ela inclui a vida da pessoa em família, seu relacionamento com seus amigos e colegas de trabalho, enfim pode ser compreendida como a relação entre a pessoa e os membros da sociedade (TAVARES, 2013, p. 541). Por exemplo, o relacionamento entre os pais e os filhos em seu lar é, *a priori*, relativo somente a eles, não podendo ninguém, sequer o Estado, interferir nessa relação; porém caso haja denúncias de abusos ou quaisquer atos criminosos, essa privacidade pode ser infringida. Enfim, pode-se apreender que intimidade é uma "espécie" do "gênero" vida privada, onde o primeiro é conferido ao indivíduo em si e o segundo ao indivíduo e quem o cerca.

Esses dois conceitos são reflexo do direito de estar só (*right to be let alone*). Conceito criado nos EUA nos fins do século XIX por Samuel D. Warren e Louis D. Brandeis que afirma se deve salvaguardar a privacidade do ser humano, pois ela é parte vital da vida do ser humano e os ordenamentos jurídicos não podem ignorá-los.

A esse conceitos está ligada a honra, que é o conjunto de qualidades relativas a reputação e ao bom nome de alguém, em outras palavras, é como alguém é visto por outro, a partir das normas sociais vigentes, sendo denominada pela doutrina honra objetiva. Pode-se dizer que a honra também pode ser definida como o sentimento de autorrespeito, o valor que a pessoa carrega pela boa fama e admiração social, inclusive pela afinidade que a pessoa tem com a sociedade na qual está inserido (HUNGRIA, 1945, p.33).

A doutrina percebeu que a imagem foi protegida de três formas pela Magna Carta. A primeira é a imagem social, constante no art. 5º, V, que caracteriza a imagem da pessoa, seja física ou jurídica, em sua vida em sociedade; a segunda é a imagem-retrato, referida no art. 5º, X, que é referente à imagem física da pessoa, rosto, olhos, nariz, braços, pernas, isto é, o corpo da pessoa em si; e a terceira é imagem autoral, estabelecida no art. 5º, XXVIII, que alude à imagem do autor em obras coletivas, resguardando sua individualidade autoral, porém só se concretiza se ele tiver participação efetiva na obra (BULOS, 2012, p.572).

Para as pessoas públicas e os locais públicos, porém existem exceções para o exercício do Direito da Personalidade. No caso das pessoas públicas, ou seja, quem é de notório conhecimento público como atores, modelos, deputados, senadores, cantores, prefeitos, artistas, entre outras ocupações que chamam atenção, eles optaram por viver de uma forma que sempre o público em geral quer saber o que fazem e há uma indústria midiática por

trás que vive em função dessa curiosidade; porém apesar dessa redução do Direito da Personalidade para essas pessoas elas não estão desamparadas e se há a quebra do limite do quão se pode imiscuir, isto é, a ofensa descabida e desonrosa à pessoa, então haverá punição na forma da lei.

A convivência da pessoa em sociedade implica na utilização de espaços públicos, neles ela ainda preserva seu direito à vida privada, mesmo diante de câmeras de vigilância. Isso implica que a pessoa não pode ser vítima de bisbilhotice alheia ou ser exposta em flagrantes indiscretos, logo tanto o Poder Público como a iniciativa privada não podem ofender ao direito da pessoa de transitar pelos espaços públicos sem ter sua vida privada imiscuída, porventura se cria uma ressalva que é a autorização da pessoa, isto é, ela permitir ser filmada (TAVARES, 2013, p. 541).

1.1.2 - O Sigilo das Comunicações

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

Os meios de comunicação são o modus da informação circular, isso inclui desde uma simples fofoca entre vizinhos até a vasta internet. A circulação de informação de um ser humano para outro é vital à sua sobrevivência e convívio social, entretanto existem informações que podem ser por demais embaraçosas, se vindas a público, podem comprometer a honra da pessoa.

A vedação se refere a qualquer forma de penetração no conteúdo, em outras palavras, abrir o invólucro da correspondência, realizar interceptação telefônica sem consentimento da Justiça, entre outros (BASTOS e MARTINS, 1989, p.72). Por inviolabilidade da comunicação de dados, a Carta Magna se refere às informações transmitidas por qualquer modalidade que não seja a telefônica, portanto a internet.

Entretanto, a inviolabilidade do sigilo das comunicações pode ser mitigada, observando o art. 1º da Lei 9.296/96 que afirma: "A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça" e seu parágrafo único aponta para sistemas de

informática e telemática. Também o art. 6º, XVIII, *a*) da Lei Complementar nº 75, que aponta as atribuições do Ministério Público, diz que cabe ao ele representar "ao órgão judicial competente para quebra de sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, para fins de investigação criminal ou instrução processual penal, bem como manifestar-se sobre representação a ele dirigida para os mesmos fins". Enfim, pode-se afirmar que a quebra do sigilo das comunicações pode ocorrer perante autorização do Poder Judiciário.

1.1.2.1 Dados bancários

O sigilo das comunicações de dados compreendem todas as informações confidencias sobre pessoas físicas e jurídicas, presentes nos bancos; nas instituições financeiras, creditícias e fazendárias; nos fichários pastas, arquivos e cadastros dos órgãos dos Poderes Públicos e dos organismos privados (BULOS, 2012). Pode ser entendido por consistir na obrigação imposta aos bancos e a seus funcionários de discrição a respeito de negócios presentes e passados de pessoas com que lidaram abrangendo dados sobre a abertura e fechamento de contas e a sua movimentação (MENDES e BRANCO, 2012).

O STF se põe a favor do sigilo aos dados bancários e nele impõe um limite, como aponta o MS 2.172 de relatoria do ministro Nelson Hungria do ano de 1969: "É certo que, atualmente, é pacífico em doutrina e em jurisprudência, que os banqueiros são "confidentes necessários" e como tais obrigados a sigilo sobre tudo quanto saem a respeito de seus clientes, em relação contratual que com esses mantem, mas tal obrigação não pode ser invocada quando se trata de prestar esclarecimentos exigidos pela justiça".

A quebra do sigilo bancário ocorre por requisição da Justiça como ilustra o STJ na voz do relator do REsp 124.272-0/RO, ministro Hélio Mosimann: "A ordem jurídica autoriza a quebra do sigilo bancário, em situações excepcionais. Implicando, entretanto, na restrição do direito à privacidade do cidadão, garantida pelo princípio constitucional, é imprescidível demonstrar a necessidade das informações solicitadas, com o estrito cumprimento das condições legais autorizadoras"

1.1.2.2 Dados Fiscais

Um dos órgãos públicos que mais possuem dados da pessoa é a Fazenda Pública,

pois é ela que guarda dados do CPF e do CNPJ, dados tributários de todas as pessoas, tanto físicas como jurídicas, dados de importação e exportação, dados dos produtos que circulam pelo país, enfim informações que devem ser protegidas.

Para isso o CTN determina em seu art. 198: "Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades". Portanto, através desse artigo, é defeso a disseminação de informações sob resguardo da Fazenda Pública.

1.1.3 – Acesso a Informação

O art. 5°, XIV diz: "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional". Pode-se verificar aqui o reguardo ao direito fundamental à informação, que é o direito de qualquer pessoa tem de saber o que está acontecendo ao seu redor.

Esse inciso pode ser conectado ao inciso XXXIII do mesmo artigo o qual obriga os Órgãos Públicos a tornar de conhecimento da pessoa informações de interesse particular ou geral, sob exceção daquelas que condizem a Segurança Nacional e também ao inciso IX que assegura a liberdade de imprensa.

O direito à informação é de vital importância para o ser humano. Saber o que ocorre ao seu redor o faz pensar em como isso vai afetar sua vida cotidiana e o propicia a se adaptar às mudanças do mundo; também é percebendo o que há no mundo que alguém é capaz de verdadeiramente formar sua opinião, assim participar do processo democrático.

Entende-se como sigilo da fonte é o direito da pessoa de não se revelar como a fonte de uma matéria jornalística, isto é, nem a lei nem o Poder Público sequer entes particulares podem obrigar o jornalista a revelar quem é sua fonte (CELSO e MARTINS, 1989, p. 81).

Existe, porém, uma frequente colisão entre esse direito fundamental e os direitos da personalidade, quer dizer, para se resguardar a intimidade e a vida privada da pessoa se limita o acesso às informações dessa pessoa. Ambos os direitos são fundamentais, portanto inexiste hierarquia entre eles e ambos merecem salvaguarda constitucional, daí se deve buscar a solução no caso concreto onde se pode ponderar a melhor solução observando as

peculiaridades de cada caso (FARIAS e ROSENVALD, 2016, p. 185).

1.1.4 - Os Atos Jurídicos

Há o inciso LX do art. 5° que pondera: “a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem” também o art. 93 IX que prescreve: “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”. Esses incisos são direta manifestação do princípio da Publicidade que afirma que todos os atos processuais devem ser de total ciência pública; isso tem o condão de dar à pessoa tanto maior acesso à Justiça como garantir a ela que a Justiça está sendo aplicada de forma correta; também se verifica a manifestação de outro princípio: o da motivação dos atos judiciais, que atesta que o juiz deve mostrar às partes e aos demais interessados como se convenceu para chegar a sentença. Porém, sob o fenômeno informatização dos atos processuais se reforça um dilema: o choque com os direitos da personalidade. Aparentemente há uma colisão entre o princípio e o direito ditos, pois quanto maior a publicidade dos atos mais exposta a pessoa fica, podendo revelar ao público segredos e intimidades que não seriam convenientes, assim podendo danificar não só a honra e a imagem das pessoas envolvidas no processo como também a de terceiros. Por um lado está o dever do poder público de informar suas ações ao povo e do outro está a proteção à Personalidade dos envolvidos no processo.

Há, porventura, um remédio para essa situação: o segredo de justiça. Ela é um instrumento que limita o acesso às informações do processo apenas às partes e a seus patronos, assim salvaguardando sua intimidade e evitando que se vá a público fatos que possam ocasionar embaraço ou ridicularização pública. Também se estende o segredo de justiça para terceiros não interessados, como testemunhas e peritos.

Assim se manifesta o STF: RMS 23036, Relator(a): Min. MAURÍCIO CORRÊA, Relator(a) p/ Acórdão: Min. NELSON JOBIM, Segunda Turma, julgado em 28/03/2006, DJ 25-08-2006 PP-00067 EMENT VOL-02244-02 PP-00246 RTJ VOL-00199-01 PP-00225 LEXSTF v. 28, n. 333, 2006, p. 159-195: “A publicidade e o direito à informação não podem ser restringidos com base em atos de natureza discricionária, salvo quando justificados, em

casos excepcionais, para a defesa da honra, da imagem e da intimidade de terceiros ou quando a medida for essencial para a proteção do interesse público.

1.1.5 - Os Danos

A Constituição Federal constituiu três formas de dano: o material, o moral e à imagem, estando explícitos no seu art. 5, V e X. Sendo concebido que a reparação monetária é o mínimo que o ofensor pode fazer para reparar a desfeita contra o ofendido, que pode ser, por vezes, irreparável.

O dano material é o estrago no patrimônio do ofendido a nível econômico, isto é, estragos à sua moradia, seu material de trabalho, seu veículo de transporte, enfim aos bens materiais de forma geral.

O dano moral é detectado pela mágoa profunda ou constrangimento de toda espécie, que deprecia o ser humano, gerando-lhe lesões extrapatrimoniais. Pouco importando o tamanho do malevolência. Havendo nexo de causalidade entre a ofensa perpetrada e o sentimento ferido está caracterizado o dano moral (BULOS, 2011).

O dano à imagem é qualquer forma de atentado, feita por qualquer pessoa, contra a expressão sensível da personalidade, ou seja, se constitui dano à imagem quando há exposição não autorizada da imagem da pessoa de forma que comprometa seu convívio social dela.

Há também um quarto tipo de dano, o dano estético que é caraterizado como a lesão *permanente* a beleza do ser humano comprometendo a harmonia das suas formas externas, enfeiando-lhe e causando-lhe humilhação, vergonha, desgosto, mal-estar e tristeza (BULOS, 2011) vale apontar ainda a súmula 387 do STJ que diz: “É lícita a cumulação das indenizações de dano estético e dano moral”; portanto se percebe uma individualização do dano estético.

1.2 - Esfera Civil

O artigo 11 do Código Civil atesta que os direitos da personalidade são intransmissíveis e irrenunciáveis, portanto indisponíveis. Porém é concebido que se pode relativizar esse direito, isto é, afastar seus efeitos de forma temporária desde que isso não tenha efeito perene ou completo e seja preservada sua constituição humana (FARIAS e

ROSENVALD, 2016, p. 180) isso também é corroborado pela própria redação do art. 11 que afirma “com exceção dos casos previstos em lei [...]” portanto dá autonomia à pessoa fazer o que bem entender com seus direitos (*idem*, p.181) .

Por exemplo, em programas de *reality shows* a pessoa cede seu direito à imagem durante um determinado período de tempo ou numa doação de órgãos. Vale apontar ainda que se configurando ameaça de lesão ou mesmo lesão a esses direitos, por exemplo, em casos de uso de imagem indevida em publicidade, divulgação de informações íntimas, apresentação de obras artísticas, entre outros, é possível exigir reparação de danos, observado que os atos devem ter ocorrido sem prévia autorização do possuidor os direitos (BITTTAR, 1994, p. 231)

1.2.1 - O Nome

O nome da pessoa é um direito, não podendo esse nome ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.

O nome é o pilar central da personalidade, pois é o elemento identificador primordial do ser humano, o seu primeiro elemento de distinção para com outros seres humanos, sua marca individual na sociedade (FARIAS e ROSENVALD, 2016, p. 287). Ele é formado pelo prenome, o termo individualizador, e pelo sobrenome, o termo identificador da família.

1.2.2 O Corpo

À pessoa é garantida a livre disposição do corpo durante ou após a vida, sendo facultada a revogação de sua decisão. Porém a pessoa não pode se submeter a procedimento médico-cirúrgico que lhe venha a pôr em risco sua vida ou lhe diminua a integridade física, daí advém a natureza indisponível do direito ao próprio corpo, porém existem situações onde o Direito á Vida se sobrepõe, por exemplo, a amputação de um membro gangrenado ou preso a destroços. Nesse âmbito, incluem-se as cirurgias plásticas, os transplantes de órgãos e as cirurgias de redefinição sexual.

O corpo humano é essencial no exercício de seus direitos, pois é nele que a pessoa existe e através dele que toma qualquer ação de sua vida. Quaisquer danos ao corpo que impeça ou dificulte a pessoa de usufruí-lo, pode tornar viável a cobrança de perdas e danos ou

até punições na esfera penal, como é possível depreender do art. 12 do Código Civil: “Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.” e também no capítulo II do Código Penal..

1.2.3 A Imagem

Segundo o art. 20 do Código Civil, imagem da pessoa é inviolável, salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a sua utilização poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

No Direito Civil, a representação física da pessoa: olhos, orelhas, boca, mãos, busto, entre outras características fisionômicas são alguns dos elementos que identificam a pessoa na sociedade. Desde que tais características possam ser identificáveis através de fotografias, vídeos, desenhos, filmes, teatro, entre outras formas de exibição pública, a imagem da pessoa está inviolável e a somente sendo perpassado sob autorização da pessoa (BITTAR, 1994, p. 262).

Associa-se o direito à imagem da pessoa também a sua voz e seus escritos já que, todo modo de comunicação verbal e sonora, constitui expressão de emoções e de pensamentos da pessoa e isso a identifica no meio social, sendo importante apontar a proteção constitucional a esses elementos (CF, art. 5º, XXVIII, *a*, 2ª parte), portanto a voz e as produções escritas constituem um dos direitos da personalidade (DINIZ, 2014).

Também se pode aludir às escutas telefônicas, onde a voz da pessoa pode ser usada como prova num processo judicial, mas isso só pode ser feito se houver autorização judicial como se pode afirmar ao observar a Constituição Federal no art. 5º, LVI que diz que são inadmissíveis, no processo, as provas obtidas por meios ilícitos em conjunto com o art. 10 da Lei 9.296/96: Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Os mortos e ausentes também gozam desse mesmo direito, como atesta o parágrafo único do art. 20: “Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes”.

A autorização, portanto, necessária para o uso da imagem alheia do *de cujus* recai sobre os entes elencados no artigo mencionado anteriormente.

Há de se indicar os limites para o direito da imagem, pois não existem direitos absolutos: quem é pessoa notória, desde que não se invada sua privacidade, pois ela tem forte simbolismo em determinada área; quem exerce cargo público, pois sua função é naturalmente de destaque na sociedade; quem se dedica à justiça ou à polícia; quem for procurado pelas forças da Justiça; quem for portador de moléstia grave e contagiosa; quem for somente parte do cenário ou quem for performar ato público ou privado que demande identificação obrigatória.

O dano causado pelo ultraje ao direito da imagem é reparável através de pagamento de multa. O STJ se manifesta sobre a prova do dano na súmula 403: "Independe de prova do prejuízo à indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais".

1.2.4 A Vida Privada

Na esfera civil, se protege a vida privada através do art. 21/CC, que está compilado: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma"; podendo esse direito ser efetivado ao se impetrar, no Poder Judiciário, mandado de injunção, mandado de segurança, *habeas data*, *habeas corpus*, ações de responsabilidade, quando se configura dano material ou moral, e cautelares inominadas e ação popular, através de via reflexa.

No artigo são protegidos não só a vida privada, mas também a intimidade do indivíduo, visto que a proteção inclui os segredos, as confidências, os dados pessoais, as recordações próprias e das pessoas próximas, os hábitos cotidianos, enfim elementos essenciais para o funcionamento da vida normal do indivíduo (BITTAR, 1994, p. 274.).

1.2.5 A Pessoa Jurídica

Apesar dos Direitos da Personalidade se referir mais a Pessoa Física, é possível estender esse direito às Pessoas Jurídicas como aponta o art. 52 do Código Civil: "Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade". Vale apontar

também que as pessoas jurídicas têm o direito de manter reserva sobre seus negócios, comunicações, reuniões de diretoria, documentos, estratégias de mercado, interdição de suas instalações e produtos á presença ou conhecimento de estranhos (BARROS, 2012).

Fazendo uma interpretação do artigo pode-se aferir que as pessoas jurídicas obtêm seus direitos de personalidade através da analogia com as pessoas físicas, ou seja, observa-se o caso concreto fazendo um paralelo entre a pessoa jurídica e a pessoa física, se o direito da última coincidir com o direito da primeira, então se aplica.

O STJ tem uma súmula que corrobora tal tese, a 227: A pessoa jurídica pode sofrer dano moral; visto que para haver dano moral é necessário a ideia de personalidade. Também vale apontar outra decisão do STJ nas palavras do Ministro Ruy Rosado de Aguiar no Recurso Especial 60033-2/MG que corrobora essa tese: “Quando se trata de pessoa jurídica, o tema da ofensa à honra propõe uma distinção inicial: a honra subjetiva, inerente à pessoa física, que está no psiquismo de cada um e pode ser ofendida com atos que atinjam a sua dignidade, respeito próprio, auto-estima, etc., causadores de dor, humilhação, vexame; a honra objetiva, externa ao sujeito, que consiste no respeito, admiração, apreço, consideração que os outros dispensam à pessoa. Por isso se diz ser a injúria um ataque à honra subjetiva, à dignidade da pessoa, enquanto a difamação é ofensa à reputação que o ofendido goza no âmbito social onde vive. A pessoa jurídica, criação da ordem legal, não tem capacidade de sentir emoção e dor, estando por isso desprovida de honra subjetiva e imune à injúria. Pode padecer, porém, de ataque à honra objetiva, pois goza de uma reputação junto a terceiros, passível de ficar abalada por atos que afetam o seu bom nome no mundo civil ou comercial onde atua”.

1.3 - Esfera Penal

O Direito Penal Brasileiro é regido pelo conceito de *ultima ratio*, expressão latina traduzida como última razão, derivado do respeito pela dignidade humana previsto na Carta Magna, implicando que o uso do Direito Penal deve ser feito apenas em última circunstância e nunca em favor do Estado, que, se aplicado, se transformaria em instrumento de repressão. Vale apontar ainda que esse ramo do Direito lida com um dos bens mais preciosos do ser humano, sua liberdade.

Aqui se pune quem incorre categoricamente, segundo a letra do Código Penal.

1.3.1 Crimes contra a honra

O Código Penal, em seu Capítulo V, trata dos crimes que atentam contra a honra subjetiva ou a honra objetiva da pessoa, seja ofensa a dignidade pessoal seja à fama profissional, de modo que se tolha do indivíduo seu respeito pessoal. São categorizados como crimes contra a honra: a calúnia, a difamação e a injúria; crimes que aparentemente similares, mas na verdade são diferentes.

Esses crimes são cometidos através de qualquer meio de comunicação o qual seja possível transmitir uma ofensa, entre os quais podemos citar a televisão, a internet, o telefone, até mesmo a ofensa feita diretamente. A agressão pode ser manifestada mediante palavras, gestos, barulhos (como a imitação de animais) etc.

Às Pessoas Jurídicas se recorre ao art. 52/CC, onde de faz uma analogia com a pessoa física, e é concebido que há uma forma de honra nas pessoas jurídicas: a honra objetiva, que é o juízo que a sociedade tem da pessoa, ou seja, sua consideração social.

No contexto do mundo digital, tal modalidade de crime alcança novos horizontes porque, especialmente, as redes sociais disseminam as informações de forma muito mais rápida e com maior alcance, o que leva a uma maior ridicularização pública.

1.3.1.1 Calúnia

Está escrito no art. 138/CP. Configura-se calúnia quando alguém acusa outro, publicamente, de estar envolvido num fato criminoso que não cometeu. Incorre também nesse crime quem a propaga de alguma forma.

Esse crime pode se estender aos mortos, mesmo que não sejam sujeitos passivos, propriamente ditos, como se vê no §2º do artigo.

No panorama cibernético esse crime ganha proporções descomunais, pois uma frase caluniosa pode rapidamente se disseminar rapidamente pelo mundo, assim fica fácil cumprir o *caput*, pois é identificável quem iniciou a calúnia, porém quem a propagou pode atingir a cifra de milhões.

Existe, porém, a exceção da verdade que é quando o sujeito ativo pode comprovar a autenticidade do fato que apontou e sendo a calúnia por definição a atribuição de um fato falso, se comprovada que o fato é verdadeiro, então o crime se extingue (BITTENCOUT, 2013).

1.3.1.2 Difamação

Está redigido no art. 139/CP. Caracteriza-se difamação quando alguém imputa a outro, publicamente, fato, seja verdadeiro ou falso, que venha a danificar sua honra objetiva.

A grande diferença para com a calúnia é que na difamação, pouco importa a veracidade do fato, mas para a calúnia é importante que o fato imputado seja falso (HUNGRIA, 1945, p.75).

A exceção da verdade se faz contra funcionário público, como aponta o parágrafo único do artigo, pois há o interesse do Estado em apurar a conduta de seus agentes.

1.3.1.3 Injúria

Está grafada no art. 140/CP. Conforma-se injúria quando alguém abala a autoestima da pessoa, ofendendo sua dignidade, a ponto da pessoa ofendida mudar o que pensa de si própria.

Há diversas formas de concretizar a injúria, visto que ela é um crime derivado da liberdade de pensamento e de expressão de alguém oralmente, pela escrita, por desenhos, por músicas, entre outros (HUNGRIA, 1945, p.85)

Vale apontar a diferença entre injúria racial e racismo, no primeiro a intenção é ofender a pessoa como ouvinte, já no segundo a intenção é ofender a raça como um todo.

Há também a modalidade de injúria real, que é configurado com o uso de violência ou vias de fato que sejam aviltantes, isto é, empurrões, tapas, “cascudos”, entre outros, porém não se confunde com a tentativa de lesão corporal pela falta do animus de lesão (*idem*, 1945, p.97).

Esse crime não aceita a exceção da verdade, diferente dos casos anteriores, a calúnia e a difamação. Há simplesmente uma ofensa a pessoa com o objetivo de humilhar e ridicularizar o sujeito passivo, não havendo necessidade de verificar a veracidade nisso (*idem*, 1945, p.84).

1.3.1.4 Outros crimes contra a honra

Existem outros crimes contra a honra esparsos em outras legislações. No Código Penal Militar, oficialmente denominado Decreto-Lei 1001, os três crimes previamente

apontados também estão retratados nesse código nos artigos 214 (calúnia), 215 (difamação) e 216 (injúria), entretanto vale apontar um crime específico: o art. 219/CPM, que trata da ofensa da honra das Forças Armadas perante a sociedade, isto é, macular sua honra objetiva. No Código Eleitoral, oficialmente denominada Lei nº 4.737/1965, os três crimes são descritos nos arts. 324 (calúnia), 325 (difamação) e 326 (injúria), porém somente surtem efeitos quando realizados em época eleitoral. Na Lei de Imprensa, oficialmente denominada Lei nº 5.250/1967, o trio também aparece nos arts. 20 (calúnia), 21 (difamação) e 22 (injúria), porventura são aplicados apenas na seara da Imprensa.

Na Lei de Segurança Nacional, oficialmente denominada Lei nº 7.170/1983, no art. 26 aponta uma punição a quem difamar ou caluniar o Presidente da República, o do Senado Federal, o da Câmara dos Deputados ou o do Supremo Tribunal Federal. No Código Brasileiro de Telecomunicações, oficialmente denominado Lei nº 4112/1962, em seu art. 53, i é punível quem, através dos meios de radiodifusão, caluniar, injuriar ou difamar os Poderes Legislativos, Executivo ou Judiciário ou os respectivos membros.

1.3.2 Crimes na Internet

Mesmo a internet sendo um local de livre expressão do indivíduo, com entretenimento, notícias, convivência social, é também um meio o qual pessoas de má índole usam para cometer crimes, tanto crimes contra a honra como crimes de natureza sexual e contra a fé pública.

São definidos crimes informáticos os 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 (SILVA, 2003, p.56).

Desse modo, surgiram novos fatos criminosos que só existem no meio virtual como o *cyberbullying,* o *cyberstalking* e o *revenge porn,* porém eles podem ser combatidos através de uma nova interpretação de leis já existentes no Direito Pátrio. O primeiro é considerado um crime contra a honra no meio virtual, pois o *bullying* é a violência física ou psicológica intencional e repetida, praticada por uma ou mais pessoas, de modo que cause dor e angústia em outro, na legislação brasileira não há tipificação do *bullying* por definição, mas os atos do *bullying* podem ser enquadrados no Código Penal, como o rol dos crimes contra a

honra; o segundo é o uso de ferramentas informáticas para perseguir ou assediar alguém, nesse caso pode ser interpretado como perturbação à tranquilidade, observando o art. 65 do Decreto-lei 3.688/41, a Lei das Contravenções Penais, e o último é quando se expõe publicamente, na Internet, fotos ou vídeos íntimos de alguém, sem o consentimento desse, mesmo que se tenham se deixado filmar ou fotografar no âmbito privado no momento de gravação do vídeo,
sendo a vítima mais famosa a atriz Carolina Dieckmann, não existindo na legislação brasileira punição para este ato específico, porém se pode considerar um crime contra honra, mais especificamente a difamação.

Pode-se perceber que apesar da falta de legislação específica para crimes cibernéticos é possível estender o alcance da lei para o meio cibernético ao se atentar a internet como um meio para o crime. Também, a partir dessa ideia algumas ações feitas na internet incorrem em crime como a divulgação de pornografia infantil, o estelionato, a pirataria, a divulgação de segredo, a sabotagem, entre outros.

1.4 O Marco Civil da Internet

O Marco Civil da Internet é oficialmente denominado de Lei N° 12.965/14, sendo ele que regula o serviço de Internet no Brasil por meio da instituição de princípios, garantias, direitos e deveres para as empresas provedoras e usuários da rede mundial de computadores, bem como da determinação de diretrizes para a atuação do Estado.

A lei trata de temas como a neutralidade de rede, a privacidade, a retenção de dados, a função social a qual a rede precisará cumprir e, especialmente, garantir a liberdade de expressão e a transmissão de conhecimento, além de impor obrigações de responsabilidade civil aos usuários e provedores.

No *caput* art. 7º se afirma que "o acesso à internet é essencial ao exercício da cidadania", logo se evidencia o reconhecimento Estatal da importância da internet para o ser humano dos dias atuais. Nos incisos do mesmo artigo se elencam os direitos dos usuários de internet e são resguardados os direitos da Personalidade do mesmo, como se evidencia no inciso I, II e III aqui transcritos: "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas,

salvo por ordem judicial”.

A lei se estende bastante na proteção dos dados a ponto que se contesta que interfere no direito ao acesso à informação e pode atrapalhar na persecução a criminosos. A Associação Nacional dos Delegados da Polícia Federal assim se manifestou acerca da lei: "O projeto do Marco Civil concede ao direito à liberdade de expressão na rede mundial de computadores um valor absoluto, maior a todos os outros, negando, com isto, existência de outros direitos fundamentais previstos na Constituição", apontando ainda que “isso não deve ser feito com a supressão de outros direitos fundamentais protegidos pela constituição”.

Capítulo 2 – O Dilema da Personalidade na Internet

A base conceitual da privacidade advém de um artigo, intitulado "*The Right to Privacy*", publicado nos fins do século XIX na Universidade de Harvard o qual apontou abusos da mídia na sociedade estadunidense da época, especialmente jornais, que estavam dilapidando a reputação de pessoas, fazendo observações às inovações tecnológicas da época e salientando a importância das emoções e sentimentos do ser humano.

Esse artigo ecoa até hoje e reflete diretamente a realidade da internet. Nas redes sociais as pessoas divulgam informações suas inadvertidamente, elas transmitem informações de si ou de outros e não se sabe ao certo que consequências podem acarretar aos envolvidos.

A legislação da União Europeia, com foco na Regulamento 2016/679, é bastante interessante se comparada a do Brasil, não apenas pela semelhança dos sistemas jurídicos, visto que ambos aplicam o sistema romano-germânico, mas também por que carrega uma série de definições e princípios que condizem com o panorama principiológico e jurídico pátrio.

2.1 *"The Right to privacy"*

Right to privacy (traduzido como "direito à privacidade") é o direito à reserva de informações pessoais e da própria vida pessoal, também pode ser entendido como *the right to be let alone* (literalmente significa "o direito de ser deixado em paz"). Tal temática veio à tona em anos recentes, com o vazamento feito pelo website *Wikileaks* que revelou que o governo estadunidense vinha espionando diversos países e instituições, até mesmo sua população na caça a terroristas e também o vazamento de dados de vários usuários do Facebook no início de 2018. Isso gerou um temor mundial acerca da proteção dos dados de pessoas. Como mostra esse trecho de uma matéria extraída do jornal O Globo: "[…] O WikiLeaks publicou nesta terça-feira milhares de documentos que seriam da CIA, no que descreveu como o maior vazamento na História da agência de Inteligência americana. O material revela detalhes da espionagem digital, como a existência de softwares projetados para hackear smartphones, computadores e até smart TVs. Se a autenticidade dos documentos for comprovada, seria um novo golpe catastrófico para a Inteligência dos EUA. A publicação de informações confidenciais pelo WikiLeaks e seus aliados tem repetidamente causado embaraço a Washington.

Os 8.761 documentos se concentram principalmente em técnicas de hackers, incluindo como transformar uma smart TV em dispositivos de vigilância improvisados. Entre as afirmações explosivas feitas no material é que a CIA, em parceria com outras agências de Inteligência dos EUA e estrangeiras, conseguiu burlar a criptografia em aplicativos de mensagens populares, como WhatsApp, Telegram e Signal.”

Esse conceito foi criado num artigo jurídico escrito pelos advogados Samuel D. Warren e Louis D. Brandeis, sendo publicado em 1890 na revista *Harvard Law Review*, a revista jurídica da Universidade de Harvard. Os dois se revoltaram com o assédio da imprensa em constantemente se intrometer na vida privada da alta sociedade dos Estados Unidos, tornando público diversos fatos íntimos dessas pessoas, os expondo ao ridículo e a humilhação públicas. Logo se tornou um dos artigos mais influentes do país e um dos primeiros documentos a defender o Direito à Privacidade (*Right to Privacy*).

Sua influencia é tamanha que chegou até a Declaração Universal dos Direito Humanos, como ilustrado no seu art. 12: "Ninguém será objeto de ingerências arbitrárias em sua vidaprivada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques."

Também no Pacto Internacional dos Direitos Civis e Políticos, outro dos pilares fundamentais dos Direitos Humanos, em seu art. 17: “1. Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais a sua honra e reputação. 2. Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques.”

O artigo fala da importância do Direito perante as mudanças de paradigmas da sociedade advindos através, no contexto do artigo, da evolução tecnocientífica e da economia e que o direito, em sua perpétua juventude, não pode deixar de ignorar as mudanças que ocorrem. Também fala que o ser humano é um ser que não apenas sente fisicamente, mas também emocionalmente; portanto necessitando de proteções nessa esfera.

A mídia se tornara uma indústria que se alimenta de fofocas e mexericos, portanto se tornou seu principal foco a vida privada das pessoas, divulgando fatos que nem sempre são verdadeiros. Dessa forma maculam a imagem dessas pessoas perante a sociedade, tendo potenciais consequências desastrosas para seus relacionamentos.

Uma vez espalhado tal conteúdo, a perspectiva pela qual os amigos da pessoa e a

sociedade, de modo geral, observam o sujeito muda, por conseguinte eles mudam seu tratamento para com o sujeito, com ódio, desprezo, rancor ou indiferença; enfim desfazendo a teia de relações sociais que o sujeito demorou tempos para construir.

Em se tratando de expressões artísticas, cabe ao indivíduo o que é portador das informações se as quer públicas ou não. Seja um poema, uma pintura, um diário, uma carta, uma partitura, uma escultura, ou qualquer outra forma de expressão pessoal ou artística, sua publicação recai apenas ao autor, assim outro não pode publicá-la sem sua anuência.

No artigo, os autores apontam o caso do Príncipe Albert v. Strange para demonstrar tal tese. No caso, o Príncipe Albert e a Rainha Vitória tinham como hobby desenhar e eles, às vezes, davam esses desenhos para alguns amigos e conhecidos. Strange obteve alguns desses desenhos e os publicou, porventura o Príncipe Albert não gostou de ter os desenhos publicados e moveu uma ação contra Strange. O Príncipe Albert ganhou a ação, pois se assumiu que os desenhos faziam parte da privacidade do casal, assim se deu o pontapé inicial na ideia de privacidade.

Faz-se então a distinção da ideia de publicação deliberada de pensamentos e emoções por meios literários e artísticos e a expressão voluntária e casual desses sentimentos no dia adia da pessoa. A diferença está, como já dito, na vontade do criador do bem, isto é, se a pessoa quer ou não que o que foi produzido vá a conhecimento público.

O artigo também estabelece diversos paralelos acerca da proteção da propriedade privada, da lesão corporal e dos direitos autorais com a proteção à privacidade, de modo que atesta que sentimentos e emoções são bens importantes para o ser humano. Argumentam que esses sentimentos e emoções inerentes aos seres humanos são expressos através de ações, palavras e especialmente através manifestações artísticas, poesia, pintura, escultura, e que ele necessita de um espaço particular para exercer tais ações, sem estar sob risco de ser exposto a público e ser ridicularizado.

Portanto, sustentam que é imperioso que haja proteção jurídica para esses bens, que de certa forma atingem a sociedade com um todo, pois afeta a percepção que as pessoas têm umas das outras.

2.1.1 Right to be forgotten

Esse termo surgiu no Tribunal de Justiça da União Europeia em 2014. Ele apontou que links para dados "irrelevantes" ou "desatualizados" (assim considerados pelo tribunal)

podem ser apagadas. Em outras palavras, a corte da União Europeia, disse que a decisão se aplica a informações "inadequadas, não pertinentes ou já não pertinentes ou excessivas em relação ao objetivo pelo qual foram processadas tendo em conta o tempo decorrido".

Isso ocorreu quando, em maio de 2014, um homem espanhol requereu ao Google que fosse deletado um link de um antigo artigo de jornal que o apontava como falido, clamando que essa informação antiga não poderia mais estar disponível, pois poderia prejudicá-lo. O Tribunal de Justiça da União Europeia concedeu ao pedido e ordenou ao Google a remoção do link, porém surgiu um efeito cascata e milhares de outras pessoas também requereram a remoção de links comprometedores.

No Brasil, o direito ao esquecimento pode ser definido como a possibilidade da pessoa restringir que certas informações potencialmente embaraçosas suas de seu passado possam vir a público e serem vistos de forma descontextualizada, porém isso não significa apagar os fatos ou reescrever a história (FARIAS e ROSENVALD, 2016, p. 196). O Supremo Tribunal de Justiça, no Recurso Especial nº 1.334.097, definiu o direito ao esquecimento como um “direito de não ser lembrado contra a sua vontade, especificamente no tocante a fatos desabonadores”.

Na legislação brasileira o direito ao esquecimento pode ser constatado no art. 202 da Lei Execuções Penais que afirma que cumprida ou extinta a pena, não constarão da folha corrida, atestados ou certidões fornecidas por autoridade policial ou por auxiliares da Justiça, qualquer notícia ou referência à condenação, salvo para instruir processo pela prática de nova infração penal ou outros casos expressos em lei” e no parágrafo 1° do art. 43 do Código de Defesa do Consumidor: “os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. Vale ressaltar ainda o Enunciado 531 da VI Jornada de Direito Civil: “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento”.

Existem dois casos importantes a serem lembrados na jurisprudência brasileira que consolidam a adoção do direito ao esquecimento pelo direito pátrio, com desenlaces distintos: o primeiro caso foi o Recurso Especial Nº 1.334.097 – RJ: em 1993, policiais à paisana alvejaram crianças que dormiam na calçada da Igreja da Candelária, resultando na morte de oito jovens, sendo que seis eram menores de idade. Quase 10 anos depois, a Rede Globo retratou o caso em um episódio do programa Linha Direto, identificando Jurandir França como envolvido no caso, apesar de ele ter sido indiciado e inocentado pela justiça. Por

conta da exibição do programa, Jurandir França teve seu cotidiano afetado, com o retorno da revolta popular em torno de sua figura. A decisão do STJ foi de que a identificação ofendeu o direito ao esquecimento, e, por isso, condenou a rede Globo ao pagamento de uma indenização. O segundo caso foi o Caso Aída Curi no Recurso Especial Nº 1.335.153 - RJ: Em 1958, a jovem Aída Curi foi atacada, estuprada e acabou sendo arremessada do terraço de um prédio. Muitos anos mais tarde, a rede Globo, noutro episódio do programa Linha Direta, exibiu o caso, com fotos e simulações. A família da vítima alegou que esta exposição reavivara a dor e aflição experimentadas na época. Como o fato ficara conhecido por "Caso Aída Curi", mostrou-se impossível retratá-lo sem fazer alusão à vítima; o STJ, enfim, concluiu que nenhuma indenização seria devida, desde que não houvesse um viés sensacionalista.

Entretanto, observando os dois casos antes descritos, nota-se um conflito entre o direito ao esquecimento e o direito à informação. O primeiro visa proteger a pessoa de ser lembrada por fatos embaraçosos, humilhantes ou degradantes; já o segundo visa repassar às pessoas informações para que ela se situe no meio social. Portanto, nessa colisão, deve-se observar o caso concreto, individualmente e decidir qual deve prevalecer.

2.1.1.1 Memes

Segundo o website infoescola, essa expressão foi criada pelo cientista Richard Dawkings em 1976 em seu livro *O Gene Egoísta.* Os memes são análogos aos genes, isto é, da mesma forma que os genes são uma informação biológica que perpassa de um ser para sua descendência, os memes são, de forma semelhante, informações culturais que passam de uma pessoa para outra, através de livros, jornais, músicas, entre outros.

Os memes podem ser ideias, línguas, sons, desenhos, valores, sinais, enfim qualquer forma de produção cultural. De forma mais coloquial, meme significa a informação transmitida de uma mente para outra, assim se propagando pela humanidade.

A internet tomou esse conceito e consolidou seu próprio conceito de meme, sendo qualquer imagem, GIF (*Graphics Interchange Format*, livremente traduzido como formato para intercâmbio de gráficos) ou vídeo que esteja relacionado ao humor que se alastre pela rede mundial de computadores. As principais plataformas de disseminação desses memes são as redes sociais, pois as pessoas olham o meme, se gostarem repassam para outros e assim por diante.

São utilizadas diversas fontes para a produção dos memes de internet, eventos recentes, acontecimentos cotidianos, fatos históricos, alguma ocorrência curiosa, enfim qualquer coisa pode se tornar um meme na internet.Portanto é muito fácil que alguém, num momento infeliz por vontade própria ou não, tenha sua imagem transformada num meme e a depender da reação do público a vida da pessoa que teve imagem transformada em meme pode se tornar muito difícil, pois as pessoas vão percebê-la através do meme, portanto se observa que sua honra objetiva é maculada. Vale também dizer que ela terá eclipsada qualquer outra forma de manifestação própria, visto que o meme irá sempre estar à sua frente.

É possível, neste viés, que a pessoa pleiteie uma ação judicial com base no direito ao esquecimento, visto que se encaixa na definição do STJ.

2.1.1.2 O Efeito Streisand

Em 2003 a atriz estadunidense Barbra Streisand moveu um processo contra o fotógrafo Kenneth Adelman e o website Pictopia.com no montante de 50 milhões de dólares em uma tentativa de ter uma foto aérea de sua mansão removida da coleção de 12.000 fotos da costa da Califórnia disponíveis no site alegando preocupações com sua privacidade. Essas fotos foram tiradas com o objetivo de documentar a erosão costeira que ocorria na região derivada da especulação imobiliária e levar essa questão às autoridades. Após esse acontecimento o público foi atrás das fotos e as veiculou pela rede mundial de computadores, a ação foi dispensada e a atriz teve que ressarcir o fotógrafo.

Esse fato deu origem ao termo efeito Streisand: é o fenômeno na internet quando a tentativa de censurar ou remover algum tipo de informação da internet se volta contra o censor, ou seja, em vez de impedir que a informação se espalhe, ela se alastra pela internet.

No Brasil, pode-se constatar em matéria da revista Veja publicada em julho de 2018 que esse efeito atingiu a atriz e apresentadora Xuxa quando ela pediu ao Google que fosse removido links para websites que continham um filme pornô que a apresentava fazendo atos libidinosos com um adolescente, o caso levou muitas pessoas a procurar esse dito filme.

Há uma relação, portanto, entre o efeito Streisand e o direito ao esquecimento, visto que o primeiro é a consequência inesperada do segundo, na tentativa de apagar certas informações infames de alguém da internet, de acordo com o direito ao esquecimento, a informação termina por se disseminar pela curiosidade do público.

Pode-se considerar que esse efeito é uma consequência infeliz do exercício do

direito ao esquecimento ao mesmo tempo em que é manifestação do direito à liberdade de informação, pois também se leva em consideração os memes, o fenômeno de replicação da informação, especialmente forte através da internet.

2.1.2 Reality shows

Apesar das características dos direitos da personalidade de irrenunciabilidade e indisponibilidade existem programas midiáticos que, de certa forma, agressivamente violam tais direitos. Programas como “Big Brother” e “No Limite” transmitidos pela Rede Globo, “Casa dos Artistas” pelo SBT (Sistema Brasileiro de Televisão) e “A Fazenda” da Rede Record transmitem 24h da vida dos participantes para todo o país. Tudo o que fazem, o que dizem, com quem se relacionam é visto por pessoas de todo o mundo, portanto por se opor à privacidade concebida por lei é inviável a existência de tais programas.

A contraponto, os participantes assinaram um contrato com emissora em que flexibilizariam seus direitos da personalidade em troca da participação no programa com direito a um prêmio se vencer, isto é, de forma mais objetiva, eles deixam de exercer seus direitos da personalidade no tempo que permanecerem no programa em troca de exposição na mídia com a promessa de um prêmio.

Para corroborar tal posição, assim expressa o enunciado nº 4 da I Jornada de Direito Civil “O exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral” e combinado com a tese de que não existem direitos absolutos, leva a conclusão que há um fulcro legal para a existência de *reality shows*.

2.2 O Ciberdireito

Também chamado de direito informático, direito digital, direito da internet, direito eletrônico, direito da tecnologia da informação, a ideia de ciberdireito é clara, esse ramo do Direito se propõe a estudar as relações jurídicas provenientes da tecnologia da informação em geral englobando a telemática, comunicação à distância, e a informática, ciência do mundo digital. Vale também apontar que o ciberdireito possui um forte aspecto interdisciplinar, pois visa se coadunar com a legislação corrente nos tempos da era da informação onde há diversas relações jurídicas que estão ligadas ao mundo digital, ao mesmo tempo em que se torna um instrumento para que seja efetivada a aplicação da Justiça (PIMENTEL, 2000, p.153).

Essa matéria já existe se encontra consolidada como matéria jurídica também em outros países: na França, recebe a nomenclatura “Droit de l'informatique”, no Reino Unido, “Information Technology Law”, na Alemanha, “Informatikrecht”; na Espanha, “Derecho Informático” ou “Derecho de las Nuevas Tecnologías”; e nos Estados Unidos, “CyberLaw” ou ainda “Computer Law” (*idem*).

Apesar de parecer à primeira vista que o ciberdireito possa ser confundido com outras normas dispersas na legislação, pois o mundo digital pode ser visto apenas como uma mudança de meio para a realização de relações jurídicas, em verdade o ciberdireito é um conjunto único de normas que orbitam um objeto, a tecnologia da informação, possuindo metodologia própria e objetos de estudo próprios, a telemática e a informática (PIMENTEL, 2000, p.157 -158).

O Brasil possui uma legislação que pode ser consideradas como manifestação do ciberdireito: o Marco Civil da Internet, apelidado de Constituição da Internet; pois é o documento legal que regulariza o serviço de internet no país, ao estabelecer princípios, direitos, deveres e garantias para usuários e fornecedores, além de determinar a atuação do Estado, e a Lei Geral de Proteção de Dados Pessoais que protege os dados pessoais no mundo virtual, além de outras leis esparsas na legislação como a Lei 12.737/2012 e a Lei 12.527/2011.

2.2.1 Hackers

A ascensão da internet gerou um grupo social que ao mesmo tempo assusta e fascina pessoas e instituições, os *hackers*. Eles são pessoas que possuem habilidades extraordinárias no campo da informática, alguns vivem misturados à sociedade se comportando como pessoas comuns, mas outros seguem o perfil do imaginário popular, vivendo reclusos e abscondidos dos olhares alheios.

A palavra *hacker* surgiu no Instituto de Tecnologia de Massachusetts (em inglês, Massachusetts Institute of Technology – MIT) para indicar os alunos de computação que passavam a noite despertos pesquisando no laboratório. Em português a palavra “*hacker*” pode ser traduzida como “*fuçador*” (SILVA, 2003, 77-78).

Eles possuem um instrumento chamado “ética *hacker*” que aponta os valores morais e filosóficos da comunidade hacker, que foram aceitos de forma tácita pela comunidade hacker. Segundo o matéria publicada website Proddigital, esse termo foi criado

por Steven Levy no livro *Hackers: Heroes of the Computer Revolution,* essa ética pode ser resumida nos seguintes princípios: o acesso aos computadores deve ser total e ilimitado; toda a informação deve ser livre e utilizada por qualquer pessoa; todo o hacker tem o dever de partilhar o seu conhecimento com a comunidade e fora dela; as economias devem ser descentralizadas e as autoridades devem ser desacreditadas; os hackers devem ser julgados pelas suas capacidades de *hacking* e não por qualquer outro tipo de critérios discriminatórios; pode criar-se arte e beleza através de um computador e os computadores podem mudar a vida para melhor.

Porém o senso comum só reconhece os *hackers* através dos ataques cibernéticos. Em matéria website El País, versão brasileira, em maio de 2017, reportou acerca do ataque do vírus "Wannacry", o qual se espalhou pelo mundo sequestrando dados de sistemas em diversos países, afetando pessoas comuns, empresas, hospitais e departamentos governamentais; isso afetou duramente o sistema de saúde britânico, que teve diversas informações de pacientes vazadas e teve que ficar paralisado para manutenção do sistema, também fechou fábricas da montadora Renault na França e afetou o Ministério do Interior e uma empresa de telefonia na Rússia, sequer o Brasil escapou, aqui a Petrobras, o Ministério Público de São Paulo e a Sede da Telefónica no Brasil. O website Glamurama, em matéria de fevereiro de 2017, lembrou alguns outros eventos similares como o ataque à Sony Pictures em novembro de 2014, que vazou 100 terabytes de dados da companhia, revelando roteiros de filmes e informações confidenciais da companhia e o ataque ao site de relacionamentos Ashley Madison, que é bastante usado por pessoas que querem um relacionamento extraconjugal, em 2015, que revelou dados de milhares de usuários como nomes verdadeiros, endereços, números de cartões de crédito e até detalhes sobre as fantasias sexuais deles.

Inclusive o site Wikileaks, um site que frequentemente divulga documentos e informações de natureza confidencial de governos e grandes corporações, obtém seus documentos através da atividade de hackers. Também entra nesse hall o grupo Anonymous, que começou por "diversão" agora é focado no hacktivismo, que é a promover a ética, os direitos humanos, a liberdade de expressão e a justiça.

Se nem as grandes empresas e os governos estão preparados para um ataque hacker, quem dera a pessoa comum, que usa seu computador para atividades diárias.

Porém, dentro da comunidade *hacker*, existe uma diferenciação para o modo o qual a pessoa utiliza suas habilidades e segue o código de ética hacker. Se a pessoa usa suas habilidades para atividades ilegais ou prejudiciais a outros usuários de computadores, eles são

denominados *crackers* ou *black hats*; se a pessoa usa suas habilidades a serviço de empresas ou que seguem o código de ética hacker são denominados *white hats*; caso a pessoa invada o sistema, mas não causa estragos ou prejuízos a outros usuários, então são caracterizados *grey hats*.(SILVA, 2003, p.78)

Portanto não é todo hacker que faz mal, serão suas ações que vão caracterizá-lo como bom ou mal, se obedecem ao código de ética *hacker*, um conjunto de valores morais e filosóficos que norteiam a comunidade.

2.2.2 Fake news

As *Fake news* (notícias falsas, em português) não são tão novas quanto se pensa, elas existem desde as origens da humanidade, pois são definidas como informações ou de cunho falso ou oriundas de boataria.

Na sociedade atual, graças às mídias sociais, as *fake news* ascenderam a um novo nível, pela velocidade de disseminação e a quantidade de pessoas que alcança, como ocorreu na Índia, onde pessoas foram linchadas, algumas até a morte, por causa delas. No Brasil também houve uma vítima na disseminação de *fake news* como aponta uma matéria noticiada no website G1 em maio de 2014: uma dona de casa de 33 anos foi morta no Guarujá-SP, após ser confundida com o retrato falado de uma suposta sequestradora de crianças.

Vale apontar que a veiculação das *fake news* influenciou bastante as eleições nos EUA e no Brasil, também no Brexit, como é denominado o processo de saída do Reino Unido da União Européia.

Segundo o website Tecnoblog, a Malásia criminalizou as *fake news*, na lei denominada *Anti-Fake News Act;* porém é contestada a redação da lei por ser bastante vaga e abrir premissas para a censura, perseguição política e cercamento da liberdade de pensamento.

Em matéria publicada no website Mundo Advogados no dia 18 de setembro de 2018 no Brasil, não existe lei específica que puna a produção e disseminação de *fake news*, porém pode-se enquadrar como crime contra a honra, injúria, calúnia ou difamação, e se ocorrer em período eleitoral, visando ofender candidato, partido ou coligação, incorre no art. 57-D §3º. O Congresso Nacional tem o Projeto de Lei nº 6.812/2017 que versa exatamente a punição de divulgação ou compartilhamento de *fake news*, no momento está sujeita à apreciação do plenário.

2.3 Privacidade na Internet

Por privacidade na internet pode-se interpretar como a omissão de quaisquer informações que levem a revelação da identidade do usuário, em outras palavras, os dados pessoais que estão na rede não podem ser revelados. A Constituição Federal salvaguarda essa privacidade através do art. 5º, X, também o art. 31 da lei 12.527/2011, a Lei de Acesso à Informação, protege as informações pessoais em posse do Estado, há o reforço do Marco Civil da Internet que também expressa essa ideia e a lei 13.709/2018 que define a proteção aos dados pessoais.

Na sociedade atual, as redes sociais se popularizaram bastante. Nesses sites de internet a divulgação de dados é quase instantânea. Nelas fotos, mensagens de texto, documentos, entre outros arquivos são disseminados pelo mundo em questão de segundos.

Portanto se observa o cuidado que se deve ter com o que circula nas redes, pois uma informação pessoal pode facilmente cair nas mãos de um malfeitor ou um fato embaraçoso da vida de alguém, que ocorreu ou no presente ou no passado, pode tornar a pessoa num motivo de piada pública, dificultando sua vida social.

Em diversos sites, para se obter seu serviço a pessoa deve fornecer um conjunto de dados como o nome, o endereço, o CPF, o RG, os dados bancários, gostos pessoais, enfim o que for pedido pelo site. A partir daí as empresas se tornam responsáveis pela custódia dos dados fornecidos, devendo informar ao usuário o que será feito com esses dados, através dos Termos de Uso, se eles serão compartilhados com outras empresas, vendidos, se serão apagados do banco de dados depois de um determinado período ou não. Levando em consideração o art. 43 do Código de Defesa do Consumidor, que trata dos bancos de dados dos consumidores, e a teoria do risco que afirma que a pessoa é responsável pelos perigos que a atividade criou, no caso, ao armazenar dados em meio eletrônico a empresa corre o risco de ser *hackeada* e ter esses dados tolhidos.

Cada site tem sua própria política de privacidade e seu próprio manejamento dos dados que lhes são confiados, devendo o usuário estar atento ao que está concordando, entretanto isso não ocorre, e por um simples motivo: é muito longo. A redação dos Termos de Uso é longa e isso desencoraja muitas pessoas a lerem.

Ainda existem os sites falsos. Eles são sites feitos com a aparência dos sites legítimos e objetivo é simplesmente roubar dados do usuário, a partir de sua ignorância e distração dele. Também existem outros mecanismos, que podem ser usados por *crackers* para

roubar dados dos usuários.

Existem, também, programas na internet chamados *cookies*. Eles funcionam da seguinte maneira: quando se visita um site pela primeira vez, é enviado um *cookie* como resposta para o seu navegador, contendo as suas preferências, em formato de texto. Este pequeno arquivo fica armazenado em seu computador até que perca sua validade, que varia com a frequência que se usa o site. Enquanto o *cookie* estiver salvo em seu computador, toda vez que você digitar o endereço do site, o seu navegador enviará este arquivo para o site que você está conectado. Desta maneira, as suas configurações serão aplicadas de maneira automática.

Em outras palavras, através dos *cookies* o computador rastreia o que e com que frequência alguém acessa determinados sites e muitas empresas utilizam cookies para saber as preferencias dos usuários e mandar propaganda para eles. Porventura, se o aparelho for invadido é possível ao invasor rastrear os hábitos da pessoa na internet e até roubar informações.

É importante apontar que com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Não raro determinadas empresas obtêm dados pessoais do usuário (profissão, renda mensal, hobbies), com o propósito de ofertar seus produtos, veiculando a sua publicidade por meio de indesejáveis *spams*, técnica [...] ofensiva à intimidade e à vida privada (GAGLIANO, 2013, p. 218a). Alguns se manifestam, principalmente, em contas de *e-mail*, e muitos usuários acham irritante e invasivo, a ponto de fazerem uma troça com o nome "*spam*": ***S**tupid **P**ointless **A**nnoying **M**essages*, que, traduzindo para o português, significa mensagem ridícula, sem propósito, e irritante.

Entretanto os *spams* são comumente usados por crackers para instalar programas maliciosos que visam roubar dados do usuário, vigiar suas atividades, manipular os programas do computador, entre outros atos de má índole.

Em Portugal, há uma legislação que disciplina a atividades de quem usa *spams:* o art. 22 do Decreto-Lei n.º 7/2004[1], lei que introduz a Diretiva 2002/58/CE do Parlamento

[1] "Artigo 22.o
Comunicações não solicitadas
1 — O envio de mensagens para fins de marketing directo, cuja recepção seja independente de intervenção do destinatário, nomeadamente por via de aparelhos de chamada automática, aparelhos de telecópia ou por correio electrónico, carece de consentimento prévio do destinatário.
2 — Exceptuam-se as mensagens enviadas a pessoas colectivas, ficando, no entanto, aberto aos destinatários o recurso ao sistema de opção negativa.
3 — É também permitido ao fornecedor de um produto ou serviço, no que respeita aos mesmos ou a produtos ou serviços análogos, enviar publicidade não solicitada aos clientes com quem celebrou anteriormente transacções, se ao cliente tiver sido explicitamente oferecida a possibilidade de o recusar por ocasião da transacção realizada

Europeu.

No Brasil, não é crime enviar spam, porém houve tentativa de regulamentá-lo no PLS 21/2004, que foi arquivado.

É salutar apontar a existência de programas que protegem o computador contra *spams,* sendo conhecidos como *anti-spams.* Empresas como Microsoft e Google disponibilizam para seus usuários uma proteção *anti-spams* em seus serviços de *e-mail*.

2.3.1 Experiência europeia

Em 1995 foi editada a Diretiva 95/46/EC, também denominada Diretiva Europeia sobre Proteção de Dados Pessoais, essa legislação exigia que cada país-membro criasse no prazo de três anos estruturas legislativas e administrativas que aplicassem a Diretiva em seu território. A Diretiva, disponível no website EUR-Lex, trouxe um rol de conceitos que ajudaram em sua consolidação, por exemplo, dados pessoais são quaisquer informações relativas a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Essa definição pode ser detectada na redação da definição de dados pessoais na legislação brasileira, na Lei 13.709/2018 em seu art. 5º, I: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

Em 2001, houve a Convenção de Budapeste, um tratado internacional de matéria do direito penal e do direito processual penal firmado, a princípio, no âmbito do Conselho da Europa para definir de forma coesa quais são os crimes praticados por meio da Internet e o modus de persecução. Sua importância é tanta que até países fora do Conselho da Europa ratificaram essa Convenção, como os Estados Unidos, o Paraguai, o Japão e o Marrocos.

O texto da Convenção aborda temas como pornografia infantil e direitos autorais

e se não implicar para o destinatário dispêndio adicional ao custo do serviço de telecomunicações.
4 — Nos casos previstos nos números anteriores, o destinatário deve ter acesso a meios que lhe permitam a qualquer momento recusar, sem ónus e independentemente de justa causa, o envio dessa publicidade para futuro.
5 — É proibido o envio de correio electrónico para fins de marketing directo, ocultando ou dissimulando a identidade da pessoa em nome de quem é efectuada a comunicação.
6 — Cada comunicação não solicitada deve indicar um endereço e um meio técnico electrónico, de fácil identificação e utilização, que permita ao destinatário do serviço recusar futuras comunicações.
7 — Às entidades que promovam o envio de comunicações publicitárias não solicitadas cuja recepção seja independente da intervenção do destinatário cabe manter, por si ou por organismos que as representem, uma lista actualizada de pessoas que manifestaram o desejo de não receber aquele tipo de comunicações.
8 — É proibido o envio de comunicações publicitárias por via electrónica às pessoas constantes das listas prescritas no número anterior."

no mundo virtual, mas também aponta para outras formas de cibercrimes como a invasão de dispositivos informáticos e a falsificação de dados informáticos. Apesar do Brasil não ser signatário da Convenção de Cibercrimes, como também é conhecida a Convenção de Budapeste, constata-se que os crimes cibernéticos criados no Brasil estão em consonância com algumas das recomendações do dito tratado internacional de direito penal, criado em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004 (BITENCOURT, 2013, p. 513).

A União Europeia estabeleceu em 2016 o Regulamento Geral sobre a Proteção de Dados (RGPD), denominado Regulamento 2016/679. É uma regulamentação acerca da privacidade e da proteção de dados pessoais, sendo aplicado a todos os indivíduos na União Europeia e Espaço Econômico Europeu. Esse regulamento revogou a Diretiva de Proteção de Dados que tratava da mesma matéria, porém estando desatualizada, pois data de 1995.

Ao contrário do antecessor, que impunha sua redação nos Estados-membros dando pouca margem de adaptação, o RGPD coaduna as legislações acerca da proteção de dados dos Estados-membros, porém é foi permitida certa margem de autonomia aos Estados-membros para tratarem de especificidades, tendo em vista adaptar o Regulamento aos seus respectivos corpos jurídicos.

A regulamentação expande conceitos como o de dados pessoais, assim os definindo: “informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.”

É imposta responsabilidade às empresas que retém dados de seus clientes e sanções, caso haja falha na proteção desses dados. Isso está constatado no art. 82 do regulamento.

O direito a ser esquecido (*right to be forgotten*) é contemplado pela regulamentação no art. 17º, porém é imposto condições para que esse direito seja concretizado.

No art. 23 se impõe limitações à proteção dos dados, ou seja, os dados pessoais de alguém são resguardados até certo ponto e além desse ponto tais informações devem ser disponibilizadas. Por exemplo, a segurança do Estado, a Defesa, a segurança pública, entre

outras situações listadas no art. 23.

2.3.2 Âmbito brasileiro

No Brasil, a legislação específica para a privacidade na internet é o Marco Civil da Internet, oficialmente denominada Lei nº 12.965/2014, e há a Lei 13.709/2018, também denominada Lei Geral de Proteção de Dados Pessoais (LGPDP) que determina o modus o qual os dados dos cidadãos podem ser coletados e tratados, além de prever punições para eventuais transgressões. Vale ressaltar que essa lei entra em vigor em 2020, após um período de adaptação de 18 meses.

Os artigos 10º e 11º do Marco Civil da Internet tratam de dois tópicos importantes relacionados à privacidade dos usuários. O *caput* do art. 10 assim diz: "A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas", portanto é imputado às empresas provedoras de internet a proteção aos dados fornecidos pelo usuário no momento da compra do serviço.

O *caput* do art. 11 relata que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Portanto se percebe que esse artigo delimita a competência jurídica da legislação brasileira perante o fluxo constante de dados através da internet, num instante um dado coletado no Brasil pode, no outro segundo, ir para um servidor em Hong Kong, por exemplo.

A LGPDP define os dados pessoais, no art. 5º, I, como informação relacionada a pessoa natural identificada ou identificável e tem como fundamentos, arrolados no seu art. 2º, o respeito à privacidade, no inciso I; a liberdade de expressão, de informação, de comunicação e de opinião, no inciso III; a inviolabilidade da intimidade, da honra e da imagem, no inciso IV; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, no inciso VII. Esses são os incisos eminentes na proteção dos direitos da personalidade.

2.3.3 Crime cibernético

Pode-se categorizar a lei 12.737/2012 como a tipificação de um crime cibernético. A Organização para a Cooperação e Desenvolvimento Econômico (OECD), em seu relatório de 1984, *Computer-Related Crime: Analysis of Legal Policy*, que pode ser traduzido para o português "Crimes relacionados ao computador: Análise da política legal" onde se definiu que crime cibernético ou informático ou virtual como qualquer conduta ilegal, não ética, ou não autorizada, que envolva o processamento automático de dados e/ou a transmissão de dados. Tal definição é deveras genérica, mas se acomoda no cerne da questão: o uso de computadores para cometer crimes (REIS, 1996, p. 25-26). De forma mais elucidativa, pode-se definir crime cibernético como ação ou omissão, típica, antijurídica e culpável, produzida por meio de atividades que envolvam dispositivos integrantes de sistema informático (SILVA, 2003, p. 58).

A lei é de suma importância para que os crimes sejam prevenidos e punidos, pois é ela que tipifica as ações que são crimes, e o campo de ação delas é tanto no mundo material como no virtual. A função da lei é estabelecer limites para a conduta humana, ao estabelecer limites aos impulsos humanos para ações tidas como imorais ou ameaçadoras aos integrantes da sociedade. Atualmente, com a magnitude da relevância da internet, é necessário que haja limites efetivos para as ações virtuais (CORRÊA, 2000, p. 58-59). A doutrina classifica esses crimes em três categorias: puro, impuros e comuns. Os puros são os tipos novos que emergiram junto com a internet e não podem existir sem ela, os impuros são os que independem dela, mas que pode usá-la como meio para um delito cominado no código penal e os comuns são os crimes em que a internet é mera ferramenta para seu cometimento (SILVA, 2003, p. 60).

Os crimes puros são os que só podem existir graças à existência do mundo digital, quer dizer, atos dirigidos contra o sistema informático, seja contra o computador seja contra dados e programas deste (SILVA, 2003, p. 61). A própria lei 12.737/2012, por exemplo, só é possível a existência desse crime se houver algum aparelho eletrônico a ser invadido, também vale citar a lei 9.609/1998 conhecida como a Lei do Software a qual disciplina propriedade intelectual de programas de computador.

Os crimes cibernéticos impuros são os que estão cominados no Código penal, mas que o bem jurídico protegido se encontra numa plataforma virtual, assim se distinguindo dos

comuns. São exemplos desse tipo de os crimes contra a honra na internet (arts. 138, 139 e 140/CP) e a disseminação de pornografia infantil (art. 241-A c/c art. 241-E, do Estatuto da criança e do adolescente).

Os crimes cibernéticos comuns são os que já existiam desde antes do surgimento da internet e dos sistemas computacionais, isto é, crimes já categorizados no Código Penal e, portanto, eles servem meramente como uma forma de disseminação. Em outras palavras, pode-se dizer que a rede de computadores e os dispositivos de informática são meios a mais para o cometimento de tais ações delitivas, não sendo necessária a utilização do meio informático para que elas existam (REIS, 1996, p. 36). São exemplos de crimes desse tipo a apologia ou incitação ao crime (arts. 286 e 287) e estelionato (art. 171/CP).

Capítulo 3 – A Lei Carolina Dieckmann

A 12.737/2012, popularmente chama de lei Carolina Dieckmann, é uma das legislações brasileiras na seara do ciberdireito, pois é uma lei que aborda temas informáticos, especificamente da invasão de tais aparelhos.

Surgida de um fato notório, que foi o vazamento de informações sensíveis da atriz Carolina Dieckmann. A comoção nacional levou o Congresso Nacional a aprovar, em tempo recorde, uma medida de natureza penal para que tal fato não viesse a ocorrer novamente.

Entretanto tal medida não saiu como o esperado, pois há erros na redação da lei e fatos que enfraquecem a eficácia real da lei. Assim, infelizmente, a lei não surte o efeito esperado para um crime que é cada vez mais evidente e que pode afetar profundamente a vida das pessoas.

3.1 A Gênese da Lei

A atriz Carolina Dieckmann procurou a polícia no dia 7 de maio de 2012, quando teve trinta e seis fotos pessoais publicadas na internet, inclusive imagens ao lado do filho de quatro anos. Meses antes, ela vinha sendo chantageada a pagar a quantia de R$ 10 mil para que não fossem publicadas na internet.

A primeira suspeita foi de que as fotos tenham sido copiadas quando o computador portátil, que continha as fotos foi levado para conserto. Após o prosseguimento das investigações foi descoberto que hackers do interior de Minas Gerais e São Paulo haviam invadido o e-mail da atriz e roubaram as imagens, assim descartando a primeira hipótese.

O roubo teria ocorrido quando um e-mail usado como isca (*spam*), que, ao ser aberto, liberou uma brecha no sistema para a instalação de um programa que permitiu aos hackers entrarem no computador da atriz.

Surgiu uma comoção nacional, impulsionada pela mídia de massa, fazendo com que a lei tramitasse em regime de urgência e em tempo recorde no Congresso Nacional.

Ela foi apresentada no dia 29/11/2011 como PL 2793/2011 sob autoria dos deputados Paulo Teixeira – PT/SP, Luiza Erundina – PSB/SP, Manuela D'ávila – PcdoB/RS, João Arruda – PMDB/PR, Brizola Neto – PDT/RJ e Emiliano José – PT/BA; sendo tramitado sob regime de urgência conforme art. 155, Regime Interno da Câmara dos Deputados a partir do dia 19/12/2011. Após algumas tramitações internas, o PL foi aprovado na Câmara dos Deputados em 15/05/2012. O Plenário do Senado recebe o projeto em 05/11/2012 e o remete

para as tramitações da Casa, sendo aprovado pelo Senado em 07/11/2012. No dia 30/11/2012 é sancionada pela então Presidenta da República, Dilma Rousseff. Enfim, no dia 30/12/2012, é transformada na Lei Ordinária 12.737/2012.

3.2 As adições ao Código

O texto do *caput* do artigo 154-A/CP, introduzido pela lei 12.737/2012, diz que

> "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".

E, analisando sob a ótica da doutrina previamente reportada, se trata de um crime cibernético próprio, pois é um tipo de crime que somente pode ocorrer no ciberespaço.

O dispositivo aponta que o núcleo do tipo é invadir o dispositivo informático alheio, ou seja, acessá-los e de outro sem a devida autorização do dono do aparelho, além disso o invasor obter, adulterar ou destruir dados do aparelho invadido ou instalar vulnerabilidades, que seria por programas que facilitariam a invasão ao aparelho, não importa isso, pois a consumação do crime se dá com a invasão do aparelho.

Pode-se assumir o dispositivo informático como qualquer aparelho (instrumento eletrônico) que tenha a capacidade de armazenar e processar automaticamente informações ou programas eletrônicos, por exemplo, notebook, netbook, tablet, Ipad, Iphone, Smartphone, pendrive, entre outros. É importante observar que é irrelevante o fato de o dispositivo estar ou não conectado à rede interna ou externa de computadores, denominados intranet ou internet respectivamente (SANCHES, 2012, p.262).

O sujeito ativo, isto é, o autor pode ser qualquer pessoa; porém observando a habilidade necessária para se fazer a invasão de um dispositivo informático se deduz que o foco será nos *crakers,* hackers de má índole que usam suas habilidades para atividades ilegais.

O sujeito passivo é o dono do dispositivo invadido, tanto faz ser pessoa física ou jurídica. Convém ter em mente a ideia de que o sujeito passivo não se confunde com prejudicado; embora, via de regra, coincidam na mesma pessoa, ou seja, as condições de

sujeito passivo e prejudicado podem recair em sujeitos distintos. O sujeito passivo é o titular do bem jurídico protegido e, hipoteticamente, lesado, enquanto o prejudicado é qualquer pessoa que, devido ao crime, sofre prejuízo, seja dano material seja moral. No primeiro caso será a vítima na relação processual-criminal, e no segundo será testemunha, embora interessada (BITENCOURT, 2012, p. 514).

Observando a ideia do professor, pode-se entender que mesmo a pessoa que teve exposta informações pessoais e teve seus direitos da Personalidade ultrajados através do dispositivo de outrem, pode pleitear reparação dos danos na esfera civil.

A lei exclui a possibilidade de culpa, pois se trata de um crime formal no qual a intenção do agente é presumida pelo ato em si, como pode se verificar até no sentido do verbo "invadir" usado na redação do artigo, que significa adentrar num determinado lugar sem permissão e o agente tem total consciência do ato. Portanto, simplesmente invadir o aparelho já consuma o crime.

Por autorização significa que o invadido pediu que seu sistema fosse invadido. Por exemplo, certa empresa pede que uma empresa especializada em segurança virtual invada seu sistema para testar suas vulnerabilidades e lhe dar um parecer acerca da situação da segurança de seu sistema. O núcleo do tipo penal é o verbo invadir, que significa adentrar em determinado lugar a força, sem autorização, logo se a pessoa que entrou no aparelho informático com aval, não se configura uma invasão.

É possível que haja a possibilidade de tentativa de invasão do aparelho, pois se trata de um crime plurissubsistente, o qual é um crime com muitas fases para atingir seu objetivo e como se observa na definição de "tentativa" no art.14, I/CP "quando, iniciada a execução, não se consuma por circunstâncias alheias à vontade do agente", por exemplo, antes da invasão ser concluída há uma queda de energia elétrica ou há um antivírus instalado no aparelho que impede a invasão. Logo o fato de ser um crime divisível, isto é, plurissubsistente abre o precedente de um evento alheio a vontade do sujeito ativo impeça a concretização do crime, configurando a tentativa (JESUS, 2013, p. 344).

No parágrafo 1º, está escrito: "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*", portanto elenca um conjunto de atos conexos ao ato descrito no *caput* do artigo: produzir, oferecer, distribuir, vender ou difundir programas que facilitem a invasão. A invasão só pode ser concretizada se a pessoa tiver não só habilidade no

campo da informática, mas também tiver as ferramentas necessárias para a ação, isto é, programas que permitam ao invasor acesso à máquina; logo o legislador observou o objetivo comum entre as ações do § 1º e o do *caput*, assim decidindo por punir quem incorre nessas ações.

O parágrafo 2º diz: "aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico", relata a situação majorante, que é o prejuízo econômico advindo da invasão, isto é, se como resultado da invasão o aparelho informático deixa de funcionar ou não funciona da maneira correta (BITENCOURT, 2013, p. 521).

O parágrafo 3º aponta as qualificadoras, os elementos que tornam o crime mais grave e altera o patamar base da pena, elas estão relacionadas ao resultado da invasão reporta dessa forma: "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", apesar da natureza aberta do parágrafo, é possível aferir o que se configura na situação. Por informações privadas, é possível apontar os dados de natureza particular ou individual; segredos industriais ou comerciais, tais como fórmulas, projetos e planos de empresas, enfim o que não constituir dados pessoais; dados sigilosos, assim definidos em lei, são informações reservadas a certas pessoas como assim apenas uma lei definir; e a manipulação remota do aparelho é quando o autor do crime instala um programa que permite seu acesso e controle remoto sobre o dispositivo, deixando aparelho a sua mercê, tal ato está em consonância com o caput do art. que remonta a instalação de vulnerabilidades no aparelho (*idem*, p.522-524).

O parágrafo 4º descreve o seguinte: "a 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" se revela então outro caso de majoração, a hipótese de aumento no cálculo da pena, que é quando o que for obtido da invasão for objeto de comercialização, venda, negociação, transferência onerosa ou por bens economicamente viáveis; de publicação, disseminar tais dados ao público por qualquer meio, ou transmissão a outrem, que diferente da comercialização não envolve onerosidade (*idem*, p. 525 e 526).

O parágrafo 5º é também um caso de majoração, que é quando a vítima da invasão for alguém dos altos cargos do Poder Executivo (Presidente da República, governadores e prefeitos); do Poder Legislativo (Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara

Municipal), do Poder Judiciário (Presidente do Supremo Tribunal Federal) ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. Nesse parágrafo é intenção do legislador salvaguardar dispositivos que contenham dados de grande relevância para a nação e devem ser protegidos em prol da soberania nacional.

O professor Rogério Sanches (2012) nota certa peculiaridade na ordem dos parágrafos: "Pela posição topográfica das majorantes percebe-se que o § 2º incide nas figuras previstas no *caput* e § 1º; já o aumento do § 4º recai sobre a forma qualificada do delito".

Numa análise minuciosa, se verifica que o legislador tenta refrear as ações dos *crackers*, hackers de má índole que usam suas habilidades para atividades ilegais, pois o tipo penal descreve quase que exatamente o que eles fazem. Assim resguardando juridicamente os dados contidos nesses aparelhos, que no contexto da sociedade atual são de vital importância para o indivíduo.

Pode-se notar que esse crime é tratado como de menor potencial ofensivo, pois a pena máxima é inferior a dois anos. Vale apontar que se enquadra na competência dos Juizados Especiais, ao observar o art. 62 da Lei 9.099/1995. Entretanto, na realidade, os Juizados Especiais sofrem da mesma morosidade que da justiça comum, apesar de terem sido criados para desobstruir a quantidade elevada de processo nela, logo processos que tenham como foco o art. 154-A/CP ficarão presos na letargia processual do Poder Judiciário

O art. 266/CP, que trata da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, teve a inclusão dos parágrafos 1: Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento e 2: Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.[2]

A intenção do Legislador, ao incluir esses parágrafos, é aperfeiçoar a proteção às vias de transmissão, pois, como se pode deduzir pelo nome das vias, é através delas que os dados informáticos são transmitidos. Já na hipótese de calamidade pública, como definido

[2] Redação velha: Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

§ 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.

pela lei 7257/2010, é situação anormal, provocada por desastres, causando danos e prejuízos que impliquem o comprometimento substancial da capacidade de resposta do poder público do ente atingido observou-se que nessa situação a comunicação é crucial e pode salvar vidas. Foi alterado também o crime de falsificação de documento particular constante no art. 298/CP, incluindo no rol destes documentos os cartões de crédito e débito.[3]

A falsificação de cartões na internet, especialmente de crédito, é algo, infelizmente, cotidiano. As fraudes deste tipo pelo meio virtual são crescentes e os atacantes conseguem obter as informações do cartão de crédito de diversas formas, como invadindo um dispositivo, interceptando uma comunicação ou através da engenharia social, que é uma técnica utilizada para se obter informações pessoais por meio da persuasão sobre o usuário, muitas vezes se valendo de sua ingenuidade ou confiança. Por exemplo, a criação de uma página falsa que induzisse o usuário a inserir os dados de cartão de crédito, fazendo-o pensar que estivesse em um site legítimo, utilizando-as para realizar novas fraudes. A tipificação desta conduta foi de grande importância, pois muitos habitantes do Brasil sofreram diversos prejuízos somente por causa de fraudes pela internet, das quais, grande parte adveio de fraudes com cartões de crédito e débito, inclusive alguns tiveram seu nome inscrito no SERASA o que lhes deu grandes tribulações.

3.2.1 Erros e Acertos

Antes do advento dessa legislação, não havia dispositivo legal que efetivamente tipificasse tal conduta como crime; em suma, não havia outra opção senão a impunidade. A invasão de dispositivo informático pode causar prejuízos inestimáveis à vítima, pois que crime que tanto atenta contra a liberdade individual como contra a privacidade, podendo causar a exposição pessoal por meio do roubo de informações ou outros dados sigilosos.

É importante salientar que para a invasão ser considerada crime ela deve acontecer sem autorização expressa ou tática do proprietário do dispositivo informático, e deve também ter o interesse de obter, adulterar, destruir dados ou ainda instalar vulnerabilidades.

[3] Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

Falsificação de cartão

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

Essa tipificação foi bem feliz, considerando a dinâmica da sociedade contemporânea e a expansão da rede mundial de computadores. Isso também é oriundo da falta de renovação da Parte Especial do Código Penal, que data da década de 1940; a ocupação da lacuna que permitia que a invasão de violação aos direitos da personalidade no ciberespaço permanecessem impunes é um avanço importante.A lei, no entanto, não é tão efetiva como se esperava. Sua pena é demasiado baixa para a proteção de um conjunto de direitos tão importantes. Caso o criminoso se limite a efetuar o que consta no *caput* do art. 154-A/CP, meramente invadir o aparelho, ele só será detido entre três meses a um ano e multa, mas de uma simples invasão já se pode obter diversos dados da pessoa. Se incorrer no §3, a hipótese qualificadora, que é "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" reclusão de seis meses a dois anos e multa, observando ainda se durante o ato o autor não incorreu nos §§ 2 ou 4.

Os danos causados pela invasão de aparelhos informáticos à vítima são de grandes consequências, desde que esses aparelhos se tornaram partes fundamentais à vida contemporânea e neles estão estocados informações bastante sensíveis, a exposição de fatos embaraçosos e íntimos muda totalmente a perspectiva da sociedade acerca da pessoa, em outras palavras, a honra objetiva é afetada, geralmente, a seu desfavor, tornando sua vida um enorme suplício.

No website G1, em matéria publicada em novembro de 2013, foi reportado que no Piauí uma garota de 17 anos cometeu suicídio após um vídeo íntimo seu foi divulgado na internet e no Rio Grande do Sul outra garota também cometeu suicídio após fotos íntimas suas terem sido publicadas na internet.

Isso piora pelo fato de a ação penal ser somente feita pela vítima mediante representação feita perante a autoridade policial, conforme aponta o art. 154-B/CP, quer dizer, já não basta a vítima estar exposta na internet, sujeita a todos os comentários malévolos possíveis e imagináveis, também deve se apresentar à delegacia para que se investigue o ato. Isso dentro do prazo decadencial de 6 (seis) meses, conforme o art. 103/CP, contado a partir do dia que se tomou ciência da identidade do autor do crime. Logo a vítima pode se recusar a comparecer perante a autoridade policial por medo de ser ainda mais exposta e piorar sua condição psicológica.

Somente não há representação se o ato for 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, como aponta o parágrafo único.

Há uma inconsistência acerca do termo “mediante violação indevida de dispositivo de segurança”. O tipo penal é ao mesmo tempo aberto, o qual necessita de uma complementação técnica, ao mencionar “mediante violação indevida”, isto é, o modo como o agente violou o dispositivo, e fechado, o qual não necessita de complementação técnica, ao reportar “de dispositivo de segurança”, logo tornando o tipo semi-aberto, ao mesmo tempo aberto e fechado, logo se o dispositivo atingido não tiver nenhuma forma de segurança como firewall, antivítus ou senha a conduta ficará desconexa ao tipo penal descrito, deixando a conduta impune. Poderá, eventualmente, adequar-se a outro tipo penal, mas não este, sob pena de violar a tipicidade estrita (BITENCOURT, 2013, p.515-517).

Em consonância com o apontado pelo professor, não é incomum que muitos aparelhos informáticos não tenham qualquer forma de proteção contra invasões como antivírus ou senha, daí se interpreta que não há qualquer “violação de segurança” e observando o princípio da taxatividade, que indica que a interpretação da lei para o ato de ser o mais harmônico possível, portanto se percebe uma grande brecha na lei.

No art. 4º da lei 12.735/2012 é ordenado à Polícia que crie um núcleo especializado em combate a crimes virtuais, porém não foram todos os Estados da Federação que criaram as delegacias especializadas estipuladas pela lei, conforme aponta o website Safernet.

3.2.2 O Dilema das provas

Para o início de uma ação penal é necessário uma fase preparatória, pré-processual, de natureza investigatória denominada Inquérito Policial. Esse ato está regulado nos arts. 4º a 23 do Código de Processo Penal e sua função é averiguar se o ato cometido é crime conforme o tipo penal. É o principal elemento na ação penal, pois nele serão colocadas as provas de autoria e materialidade do crime. Entretanto os crimes praticados por computador são mais complexos e podem facilmente escapar da Justiça.

Hackers, mais exatamente os *crackers*, como explicado anteriormente, são pessoas especialistas em informática. Eles são capazes de entrar e sair de um aparelho informático, instalar vírus, fazer alterações ou supressões, sem deixar rastros. Além disso, há a elevada tecnicidade do campo que a torna muito hermética.

Um dos principais elementos do inquérito policial é a colheita de provas, que são os elementos probatórios que vão apontar a materialidade do crime e convencer o juiz quais das alegações ditas pelas partes são verdadeiras (MIRABETE, 2003, p. 270), e um dos principais documentos é o exame de corpo de delito, sendo que sua importância pode ser vista no *caput* art. 158[4] do Código de Processo Penal, o qual afirma ser indispensável quando há vestígios.

É definido que corpo de delito o conjunto de elementos materiais deixados na cena do crime, enfim a prova da existência do crime e o exame de corpo de delito é a análise realizada pela perícia criminal desse dito conjunto (NUCCI, 2008, p.397). Nos crimes virtuais, especialmente os cometidos por *crackers* habilidosos, quaisquer vestígios podem ser apagados ou criptografados a ponto que a polícia não tem como agir na busca do criminoso.

O exame de corpo de delito pode ser feito diretamente, quando a infração penal deixa vestígios claros, como nos crimes de homicídio, lesão corporal e estupro; caso inexistente os vestígios, segue-se o disposto no art. 167/CPP[5], assim é dispensado a perícia e são arroladas possíveis testemunhas, como nos crimes contra a honra e ameaça (MIRABETE, 2003, p. 286 e 287).

Entretanto, boa parte dos crimes virtuais não deixam vestígios para um exame de corpo de delito direto, pois os *hackers* podem realizar tal feito com seus conhecimentos, logo pela lei se buscaria testemunhas para um exame indireto, mas hackers preferem agir sozinhos ou em grupos secretos; logo, por essa linha de pensamento, um exame de corpo de delito é impossível e seguindo o que diz o art. 564, III, b/ CPP[6] o processo será nulo.

3.3 – Bancos de dados

[4] Art. 148, *caput*: Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.
[5] Art. 167: Não sendo possível o exame de corpo de delito, por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta.
[6] Art. 564, III A nulidade ocorrerá nos seguintes casos:
III - por falta das fórmulas ou dos termos seguintes:
b) o exame do corpo de delito nos crimes que deixam vestígios, ressalvado o disposto no Art. 167.

Na conjuntura atual da economia, houve a incorporação plena da internet em sua teia. Muitas empresas oferecem diversos tipos de serviços como comércio, redes sociais, notícias, entre outros e todos, para prestar melhores serviços ao usuário, requerem que ele faça um cadastro, ou seja, informe alguns de seus dados pessoais como, RG, CPF, endereço, e-mail, número do celular e data de nascimento. A notória ação de *hackers,* mais exatamente os *crackers,* que tem a capacidade de adentrar os bancos de dados da empresa, obter dados dos clientes e potencialmente utilizá-los para atividades ilegais, levanta a questão da confiança na empresa, se os dados que ela resguarda estão bem protegidos e se ela é responsável pela perda dos dados. De acordo com o art. 5º, IV da LGPDP, define-se banco de dados como o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Os arts. 7° e 8° da lei 12.965/2014, o Marco Civil da Internet, tratam justamente desse tema, eles apontam que a empresa dê "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades" e a lei 13.709/2018, a Lei de Geral de Proteção de Dados Pessoais, que diz que as empresas são responsáveis pelos danos que causarem nos limites de suas atribuições conforme dizem os arts. 42 a 44.

A responsabilidade é tratada no art. 927 do Código Civil que diz que "aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo" e é definida como a aplicação de medidas que obriguem alguém a reparar dano, seja moral ou material, a terceiro, em razão de ato por ele praticado, por pessoa por quem ele responde, por algo a ele pertencente ou por imposição legal (DINIZ, 2013, p. 51).

A responsabilidade das empresas pela guarda dos dados pode ser vista no viés da atividade de risco, pois se define essa atividade como exercício regular de uma atividade que possa que possa ser pernicioso ou adverso a direitos de terceiros (GAGLIANO, 2013, p.194). Vale ressaltar o enunciado 38 da Jornada de Direito Civil que afirma que "a responsabilidade fundada no risco da atividade, como prevista na segunda parte do parágrafo único do art. 927 do novo Código Civil, configura-se quando a atividade normalmente desenvolvida pelo autor do dano causar a pessoa determinada um ônus maior do que aos demais membros da coletividade".

Conclui-se que no exercício de guardar dados pessoais de alguém, uma empresa tem a responsabilidade de salvaguardar esses dados para que não sejam utilizados de forma ilícita, se não terá de arcar com os danos à vítima.

Vale apontar que o Estado é um dos maiores detentores de informações pessoais, pois é ele quem expede documentos pessoais como carteira de identidade, carteira de motorista, certidão de pessoa física, certidão de pessoa jurídica, entre outros, e a seguir pela mesma linha de pensamento que nas relações privadas, o Estado tem responsabilidade pela guarda das informações que possui.

3.4 - Relações com outras legislações

A Lei 12.737/2012 possui semelhanças e conexões com outras normas, não só do Código Penal, mas também com outras legislações.

O Marco Civil da Internet é a regulamentação do serviço de internet no país, a conexão com a Lei 12.737 é notável pelos conceitos que aborda no art. 5º, por exemplo, a internet é descrita no inciso I como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" e através dessa definição, e das outras abordadas nos outros incisos do artigo, a justiça pode aplicar com mais eficiência a lei.

A Lei 9.296/1996, em conjunto com o art. 5º, XII da Constituição Federal, regimenta a interceptação telefônica e no art. 10 comenta acerca da privacidade das comunicações telemáticas ou informáticas, afirmando que "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei", porém não se aplica a Lei 12.737 visto que existe o princípio da especialidade, que aduz que a norma específica afasta a norma geral.

A Lei de Acesso à Informação, oficialmente denominada lei nº 12.572/2012, é a legislação que determina a divulgação de informações produzidas ou armazenadas por órgãos e entidades públicas da União, Estados, Distrito Federal e Municípios. À primeira vista é a concretização do art. 5º, XXXIII da Carta Magna, mas a lei também determina a proteção às informações pessoais, conforme diz seu art. 31.

Em relação à LGPDP, oficialmente denominada lei 13.709/2018, consolida

definições importantes para uma melhor aplicabilidade não só da lei 12.737/2012, mas também outras leis que lidam com a internet. O art. 5º da lei assim diz sobre dados pessoais no inciso I: "informação relacionada a pessoa natural identificada ou identificável" e tratamento no inciso X: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"

3.4.1 Âmbito civil

A Lei 12.737/2012 tem um forte impacto na esfera civil, pois não apenas coaduna com a proteção de direitos já consagrados pelo Código Civil na esfera penal, como também possibilita uma melhor punição ao perpetrador no dano.

Na esfera penal, o mero ato de invadir já é o bastante para imputar o invasor, porém a punibilidade nessa esfera, como já vista, é por demais leniente, se comparado ao dano causado à vítima. Vale apontar ainda que há uma dificuldade, por parte da polícia, em rastrear a pessoas, visto que ela tanto pode apagar seus rastros no ciberespaço como a polícia não tenha condições de efetivamente encontrar o criminoso.

É na esfera civil que se podem obter melhores resultados de reparação, pois em todos os casos haverá dano, cujo ressarcimento não pode ser colocado em dúvida, os autores do artigo "*Right to Privacy*", Samuel D. Warren e Louis D. Brandeis, salientam, em seu tempo, que "fotos instantâneas e empresas jornalísticas têm invadido os recintos sagrados da vida privada e doméstica e numerosos engenhos mecânicos ameaçam fazendo boa a predição segundo a qual 'o que se sussurra no gabinete será proclamado no alto das casa'" [...] (DINIZ, 2013).

Uma só conduta, ou uma série de condutas, pode despertar ações judiciais tanto na esfera civil como penal, ocorrendo sincronicamente a persecução criminal e a ação civil, na primeira somente contendo a vítima e o algoz, já na segunda pode que uma terceira parte interessada tenha sida prejudicada pela ato e queira reparação pelo dano (VENOSA, 2005, 185).

O Código Civil no artigo 935 afirma que "a responsabilidade civil é independente da criminal, não se podendo questionar mais sobre a existência do fato, ou sobre quem seja o seu autor, quando estas questões se acharem decididas no juízo criminal" e o Código de

Processo Penal afirma no artigo 64 “[...] a ação para ressarcimento do dano poderá ser proposta no juízo cível, contra o autor do crime e, se for caso, contra o responsável civil”. Nota-se, portanto uma confluência entre os textos legais para a ocorrência de ações na esfera criminal e civil, entretanto é importante apontar que o art. 66/CPP aponta que “não obstante a sentença absolutória no juízo criminal, a ação civil poderá ser proposta quando não tiver sido, categoricamente, reconhecida a inexistência material do fato”, isto é, uma vez que a matéria criminal é decidida a existência do fato não pode ser questionada (VENOZA, 2005, 188).

É denominada matéria de fato o que for alegado pelas partes, sendo que devem demonstrá-las como verdadeiras através dos meios de prova e matéria de direito é a acordância entre o que for produzido como prova e o texto legal, tal comparação é feita pelo juiz.

4. Considerações finais

Enfim, a lei 12.737/2012 é de grande valia na proteção dos direitos da personalidade, tão infringidos pelo avanço tecno-científico e pela consolidação da Era da Informação; pois é o conjunto de direitos mais íntimo do ser humano, relacionando-se com a convivência da pessoa na sociedade.

Entretanto ela deixa a desejar na sua execução, certos furos, palavras mal colocadas e possibilidades de interpretação tornam a lei menos efetiva do que devia ser. Além disso, há a questão das condições materiais do Poder Judiciário em perseguir o criminoso, que, por vezes, é muito mais hábil que seus perseguidores.

É um assunto muito mais profundo que aparenta e há diversos caminhos a serem tomados, portanto se deve ter cautela com ele.

REFERÊNCIAS

ADAMI, Anna. **Infoescola.** Disponível em: <https://www.infoescola.com/comunicacao/memes/>. Acesso em 30/03/2019

ADOLESCENTE comete suicídio após ter fotos íntimas divulgadas na web. **Terra**, 20 nov. 2013. Disponível em: <https://www.terra.com.br/noticias/brasil/policia/rs-adolescente-comete-suicidio-apos-ter-fotos-intimas-divulgadas-na-web,1b975df8bd472410VgnVCM5000009ccceb0aRCRD.html>. Acesso em 21/10/2018

AGRELA, Lucas. O escândalo de vazamento de dados do Facebook é muito pior do que parecia. **Exame**, 6abr 2018 Disponível em: <https://exame.abril.com.br/tecnologia/o-escandalo-de-vazamento-de-dados-do-facebook-e-muito-pior-do-que-parecia/>. Acesso em 28/10/2018

ARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: **Âmbito Jurídico**, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 30/08/2018

ALECRIM, Emerson. Google melhora antispam do Gmail com sistema de inteligência artificial mais sofisticado. **Tecnoblog,** 2015. Disponível em: <https://tecnoblog.net/181277/google-gmail-antispam-ia/>. Acesso em 10/11/2018

BARRETO, Erick Teixeira. Crimes cibernéticos sob a égide da Lei 12.737/2012. In: **Âmbito Jurídico**, Rio Grande, XX, n. 159, abr 2017. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=18757&revista_caderno=17>. Acesso em 19/10/2018

BASTOS, Celso Ribeiro e MARTINS, Ives Gandra, **Comentários á Constituição do Brasil: promulgada em 5 de outubro de 1988**, 2º Volume, 1ª Edição, São Paulo: Saraiva 1989

BITENCOURT, Cezar Roberto, **Tratado de direto penal**, 2: parte especial: dos crimes contra a pessoa, 13ª Edição, São Paulo: Saraiva, 2013

BITTAR, Carlos Alberto**, Curso de direito civil**, volume 1, 1ª Edição, Rio de Janeiro: Forense Universitária, 1994

BULOS, Uadi Lammêgo, **Curso de Direito Constitucional**, 8ª Edição, São Paulo: Saraiva, 2011

CAMPANHOLA, Nadine Finoti. *Crimes Virtuais Contra a Honra*. Conteudo Juridico, Brasilia-DF: 17 abr. 2018. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.590568&seo=1>. Acesso em 17/10/2018

CARDOSO, Filipa. Hacker – O que é e qual o seu código de ética?. Disponível em: <https://proddigital.com.br/tecnologia/hacker-o-que-e-e-qual-o-seu-codigo-de-etica/>. Acesso em 26/05/2019

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei n.°12.737/2012, que tipifica a invasão de dispositivo informático**. Disponível em: <http://www.dizerodireito.com.br./2012/12/primeiros-comentarios-lei-127372012-que.html>**.** Acesso em 23/10/2018

COELHO, Fábio Ulhoa, **Curso de Direito Civil**: parte geral, volume 1, 6ª Edição, São Paulo: Saraiva, 2013

CORRÊA, Gustavo Testa, **Aspectos jurídicos da Internet**, 1ª Edição, São Paulo: Saraiva, 2000

COUNSIL OF EUROPE. Chart of signatures and ratifications of Treaty 185.Convention on Cybercrime. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. Acesso em 23/10/2018

CUNHA, Rogério Sanches, Manual de Direito Penal, Parte Especial (Arts. 121 a 361), 5ª Edição rev., atual., e ampl., 2013, Jus Podium

DELEGACIAS CIBERCRIMES. **Safernet** Disponível em: <https://new.safernet.org.br/content/delegacias-cibercrimes>. Acesso em 12/04/2019

DELEGADOS da Polícia Federal dizem que Marco Civil é inconstitucional. **G1**, 11 set. 2012. Disponível em: <http: //g1.globo.com/tecnologia/noticia/2012/07/delegados-da-policia-federal-dizem-que-marco-civil-e-inconstitucional.html>. Acesso em 17/10/2018

DINIZ, Maria Helena, **Curso de Direito Civil Brasileiro**, volume 1: teoria geral do direito civil, 31ª Edição, São Paulo: Saraiva, 2014

DINIZ, Maria Helena, **Curso de Direito Civil Brasileiro**, volume 7: reponsabilidade civil, 31ª Edição, São Paulo: Saraiva, 2013

EVARISTO, Silvana Aparecida Cardoso; CESAR, Claudio Evaristo. Direito x internet. In: **Âmbito Jurídico**, Rio Grande, XVII, n. 127, ago 2014. Disponível em: <http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14255>. acesso em 17/08/2018

EUR-LEX **32002L0058-PT**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT. acesso em 19/10/2018

FACEBOOK. **Cookies**. Disponível em: <https://pt-br.facebook.com/policies/cookies/>. Acesso em 08/11/2018

FARIAS, Cristiano Chaves de e ROSENVALD, Nelson, **Curso de direito civil**, volume 1, parte geral e LINDB, 14ª Edição ver., ampl. e atual., Salvador: Jus Podium, 2016

FERNANDES, Lauren, "**Qual a extensão da proteção constitucional ao domicilio da pessoa?".** Disponível em: <https://laurenfernandes.jusbrasil.com.br/artigos/492539639/qual-a-extensao-da-protecao-constitucional-ao-domicilio-da-pessoa>. Acesso em 20/09/2018

GAGLIANO, Pablo Stolze e FILHO, Rodolfo Pamplona, **Novo curso de direito civil**, volume 1, 15ª Edição rev., atual. e ampl., São Paulo: Saraiva, 2013

GAGLIANO, Pablo Stolze e FILHO, Rodolfo Pamplona, **Novo curso de direito civil**, volume 3, 11ª Edição rev., atual. e ampl., São Paulo: Saraiva, 2013

GARCIA, Leonardo de Medeiros, **Direito do Consumidor**, Código comentado e jurisprudência, 11ª Edição, rev., ampl. e atual., Jus Podium, 2015

HIRATA, Alessandro. **Direito à privacidade.** Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade>. Acesso em 25/08/2018

HUNGRIA, Nelson, **Comentários ao Código Penal**, volume VI, 1ª Edição, Rio de Janeiro: Forense Universitária, 1994

INVASÃO TOTAL: os ataques cibernéticos mais polêmicos dos últimos tempos. **Glamurama**, 04 fev. 2017. Disponível em: <https://glamurama.uol.com.br/invasao-total-os-ataques-ciberneticos-mais-polemicos-dos-ultimos-tempos/>. Acesso em 16/10/2018

JESUS, Damásio de, **Direito penal**, 2º volume, parte especial; Crimes contra a pessoa a crimes contra o patrimônio, 33ª Edição, São Paulo: Saraiva, 2013

JÚNIOR, Dirley da Cunha, **Curso de Direito Constitucional**, 6ª Edição ver., ampl. e atual., Jus Podium, 2012

MÃE de jovem achada morta após vídeo íntimo reclama de 'violação'. **G1**, 17 nov. 2013. Disponível em: <http://g1.globo.com/pi/piaui/noticia/2013/11/mae-de-jovem-achada-morta-apos-video-intimo-reclama-de-violacao.html>. Acesso em 21/10/2018

MENDES, Gilmar Ferreira e BRANCO, Paulo Gustavo Gonet, **Curso de Direito Constitucional**, 12ª Edição ver. e atual., São Paulo: Saraiva, 2017

MIRABETE, Julio Fabbrini, **Processo Penal**, 15ª Edição ver. e atual. até julho de 2003, São Paulo: Atlas, 2003

MONTEIRO, Washington de Barros, **Curso de Direito Civil 1**, Parte Geral, 44ª Edição, São Paulo: Saraiva, 2012

MULHER espancada após boatos em rede social morre em Guarujá, SP. **G1**, 05 maio 2014. Disponível em: <http://g1.globo.com/sp/santos-regiao/noticia/2014/05/mulher-espancada-apos-boatos-em-rede-social-morre-em-guaruja-sp.html>. Acesso em 30/03/2019

MUNDO DOS ADVOGADOS, 19 set. 2018. Disponível em: <https://www.mundoadvogados.com.br/artigos/o-que-diz-a-legislacao-brasileira-sobre-as-fake-news>. Acesso em 10/04/2019

NUCCI, Guilherme de Souza, **Manual de Processo Penal e Execução Penal**, 5ª Edição ver., atual. e ampl., São Paulo: Revista dos Tribunais, 2008

PIMENTEL, Alexandre Freire, **O direito cibernético: um enfoque teórico e lógico-aplicativo**, Rio de Janeiro: Renovar, 2000

PROTEÇÃO de dados e privacidade em linha. Disponível em: <https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pt.htm>. Acesso em 19/10/2018

REINALDO FILHO, Demócrito. **Lex Magister** Disponível em: <http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx>. Acesso em 10/11/2018

REVISTA SJRJ, Rio de Janeiro, v. 20, n. 37, p. 13-28, ago. 2013. Disponível em: <https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/450-1824-1-pb.pdf>. Acesso em 18/08/2018

REIS, Maria Helena Junqueira, **Computer crimes: a criminalidade na era dos**

computadores, Belo Horizonte: Del Rey, 1996

SAMPEI, Kamila. **Lei Carolina Dieckmann - A vida prática e a ineficácia da aplicação da pena**, 2015. Disponível em: <https://kamilasampei.jusbrasil.com.br/artigos/189641302/lei-carolina-dieckmann-a-vida-pratica-e-a-ineficacia-da-aplicacao-da-pena>. Acesso em 23/10/2018

SCHMITT, Guilherme. **Crimes cibernéticos.** Disponível em: <http://www.schmidtadvogados.com/portfolio-view/crimes-ciberneticos/>. Acesso em 10/11/2018

SILVA, Catarini Meconi da; BáRBARA, Natália Bueno; CABRELLI, Fernando Braga. Direito e Internet: A importância de uma tutela específica para o ciberespaço. In: **Âmbito Jurídico**, Rio Grande, XV, n. 106, nov 2012. Disponível em: <http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12390&revista_caderno=17>. Acesso em 17/08/2018

SILVA, Rita de Cássia Lopes da, **Direito Penal e Sistema Informático**, São Paulo: Revista dos Tribunais, 2003

SNOWDEN: Vazamento prova que EUA pagaram para espionar softwares. **O Globo**, 07 mar. 2017. Disponível em: <https://oglobo.globo.com/mundo/snowden-vazamento-prova-que-eua-pagaram-para-espionar-softwares-21026190>. Acesso em 30/03/2019

SUSPEITOS do roubo das fotos de Carolina Dieckmann são descobertos. **G1,** 13 maio 2012. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html>. Acesso em 19/10/2018

TAVARES, André Ramos, **Curso de Direito Constitucional**, 11ª Edição, São Paulo: Saraiva, 2013

VENTURA, Felipe. O que acontece quando um país transforma “fake news” em crime. **Tecnoblog**, 2018. Disponível em: <https: //tecnoblog.net/241364/malasia-lei-crime-fake-

news/>. Acesso em 19/10/2018

WARREN, Samuel e BRANDEIS, Louis, "***The Right to Privacy***", disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em 30/08/2018

WANNACRY no Brasil e no Mundo. **O Povo**, Fortaleza-CE 13 maio 2017. Disponível em: <https://www.opovo.com.br/jornal/economia/2017/05/wannacry-no-brasil-e-no-mundo.html>. Acesso em 17/10/2018

XUXA perde para o Google: site não irá remover buscas sobre filme erótico. **VejaRio**, 9 jul. 2018. Disponível em: <https://vejario.abril.com.br/cultura-lazer/xuxa-perde-para-o-google-site-nao-ira-remover-buscas-sobre-filme-erotico/>. Acesso em 24/10/2018