UNIVERSIDADE DO SUL DE SANTA CATARINA

VANESSA MERELL

DIREITO DIGITAL:
OS ASPECTOS JURÍDICOS DA EVOLUÇÃO DIGITAL

Florianópolis

2020

VANESSA MERELL

DIREITO DIGITAL:
OS ASPECTOS JURÍDICOS DA EVOLUÇÃO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Hernani Luiz Sobierajski, MSc.

Florianópolis

2020

VANESSA MERELL

DIREITO DIGITAL:
OS ASPECTOS JURÍDICOS DA EVOLUÇÃO DIGITAL

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina.

Florianópolis, 20 de novembro de 2020.

_____

Professor e orientador Nome do Professor, titulação
Universidade do Sul de Santa Catarina

_____

Prof. Nome do Professor, titulação
Universidade do Sul de Santa Catarina

_____

Prof. Nome do Professor, titulação

Universidade do Sul de Santa Catarina

TERMO DE ISENÇÃO DE RESPONSABILIDADE

DIREITO DIGITAL:
OS ASPECTOS JURÍDICOS DA EVOLUÇÃO DIGITAL

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Florianópolis, 20 de novembro de 2020.

_____

VANESSA MERELL

Dedico este trabalho a minha mãe e a meu pai, pelo apoio incondicional em toda minha trajetória, nada disso seria possível sem eles.

AGRADECIMENTOS

Agradeço primeiramente à minha família, por apoiarem minhas escolhas e me ajudarem em tudo que precisei, principalmente minha mãe e meu pai, que fizeram tudo que estava ao alcance para que eu concluísse o curso superior e apresentasse este trabalho.

Agradeço aos meus professores que me guiaram por esta jornada, principalmente meu professor orientador Hernani Luiz Sobierajski que acompanhou desde do começo o desenvolvimento deste trabalho, capítulo por capítulo.

Agradeço aos meus amigos pela paciência, porque, por muitos meses, o tema deste trabalho foi meu único assunto.

Agradeço acima de tudo a Deus, sem ele nada disso seria possível.

RESUMO

Com a crescente digitalização da vida humana a internet passou a ser parte indissociável da cotidiano das pessoas, e, como toda ação humana reflete no Direito, não poderia ser diferente com o uso constante da internet, culminando em um novo ramo do Direito: o Direito Digital. O objetivo desta pesquisa é introduzir o Direito Digital, suas características, peculiaridades, dificuldades e impacto na vida jurídica das pessoas, principalmente nos operadores do Direito, que carregam a grande responsabilidade de entender e atuar nesta área, levando para seus clientes e particulares o trabalho mais eficiente possível. A pesquisa usará o método dedutivo e qualitativo, com procedimento documental e bibliográfico, com uso de doutrina, legislação, artigos, aulas e jurisprudência. Ao final, concluir-se-á que o Direito Digital é um ramo complexo e que exige muito daquele que o encara, o que irá afastar muitos profissionais desta área, principalmente aqueles que não estiverem familiarizados com os termos técnicos da internet.

Palavras-chave: Direito. Direito Digital. Internet.

SUMÁRIO

1 INTRODUÇÃO

Quase em todas as áreas do Direito, primeiro é estudado como ele foi criado, desenvolvido e implementado ao longo dos anos, esta abordagem histórica tem como objetivo situar o estudante de direito naquela área, bem como demonstrar os objetivos daqueles institutos de Direito, cita-se como exemplo o estudo das ordenações de ofício no Direito Trabalhista ou da revolução francesa no estudo de direitos humanos.

Levando em consideração essa noção histórica, não se pode deixar de notar que pouco se fala no Direito Digital nos tempos atuais, esta é uma área relativamente nova e tem mostrado seus primeiros impactos na vida jurídica das pessoas, ou seja, este momento histórico é exatamente o nascedouro do Direito Digital, e os juristas contemporâneos têm a grande oportunidade de estudá-lo em seu momento de criação, de controvérsia, o que é uma oportunidade tão grande quanto presenciar aqueles momentos históricos que tanto são estudados na faculdade de direito.

A questão a ser respondida com esta pesquisa é de quais formas a criação e desenvolvimento do Direito Digital estão impactando a vida dos brasileiros, principalmente para quem atua na área jurídica; para isso, o trabalho será dividido em 3 (três) capítulos de desenvolvimento.

O capítulo 2 começa explicando como acontece a atuação do advogado na área digital, quais as peculiaridades que esta área apresenta, e quais desafios os advogados têm que enfrentar na atuação com Direito Digital; o segundo capítulo será focado na forma como as pessoas lidam com a internet, como suas manifestações refletem no Poder Legislativo e, consequentemente, em todos os outros poderes e instituições; o terceiro e último capítulo trará a manifestação do Poder Judiciário em casos escolhidos por amostragem envolvendo Direito Digital, como os juízes, que são incumbidos de resolver o litígio entre as pessoas independentemente de lei existente, estão lidando com esse tema tão recente e complexo.

O método utilizado no trabalho será o dedutivo, ou seja, serão apresentadas premissas verdadeiras maiores para chegar às menores, a fim de encontrar a verdade dos fatos.

A análise de dados será feita pelo método qualitativo, de forma a analisar os textos e questões levantadas pelos autores relacionados ao conteúdo do trabalho.

O procedimento utilizado será o documental e o bibliográfico, tendo como base doutrinas, trabalhos científicos, apresentações, legislação, decisões judiciais e artigos publicados em meio digital.

Por fim, o objetivo deste trabalho é apresentar uma noção inicial do que seria o Direito Digital e como atuar nesta área, de forma que, ao final da pesquisa, o leitor compreenda as peculiaridades deste ramo do Direito, sua criação, desenvolvimento e previsões para o futuro.

2 ATUAÇÃO JURÍDICA NA ÁREA DIGITAL

É previsível e até esperado que as leis positivadas não prevejam todas as possibilidades da vida humana, tanto as normas materiais quando às processuais estão sujeitas à insuficiência e à ineficácia com o passar dos anos.

A evolução digital tem criado uma mudança na forma em que as pessoas vivem, na forma como interagem entre si, como compram, como procedem operações bancárias, como trabalham, entre outras; uma verdadeira digitalização da vida humana, o que de um lado cria vantagens para os usuários da rede, de outro, também sujeita-os a novos tipos de ilícitos.

A sociedade digital demanda uma nova forma de atuação frente aos ilícitos cometidos online, a intenção do segundo capítulo é apontar um norte para a atuação jurídica na área digital, explicando as peculiaridades do Direito Digital e exemplificando a atuação do jurista nesta área.

2.1 ELEMENTOS FUNDAMENTAIS DA INTERNET

Explica o autor Leonardi (2019) que para a correta atuação em questões jurídicas relacionadas à internet, é imprescindível o conhecimento de certos elementos fundamentais:

> Ao operador do Direito, pode parecer estranha a necessidade de conhecer, ainda que superficialmente, alguns aspectos técnicos relacionados à internet. Afinal, em outras áreas, esse conhecimento técnico dificilmente é necessário: não é preciso saber o que mantém uma aeronave no ar, por exemplo, para pleitear reparação de danos decorrentes de um desastre aéreo, ainda que tal conhecimento possa ser útil.

Nesse mesmo pensamento, Haikal (2014, p. 317) explica que:

> Por vezes o operador do direito não se sente confortável a lidar com temas ligados à tecnologia, por não conseguir apreender certos conceitos ou abstrações, e acaba por fazer julgamento inadequado de determinado cenário, quer por excesso de higidez ou pela falta de severidade [...].

Passa-se agora ao estudo dos termos técnicos essenciais para a atuação em questões envolvendo Direito Digital.

Provedores: diversos autores apresentam uma classificação diferenciada dos provedores, porém a Lei do Marco Civil da Internet (Lei nº 12.965/2014) decidiu por uma classificação mais simples, dividindo os provedores em apenas dois: provedor de conexão à internet e provedor de aplicação de internet (BRASIL, 2014).

Para Ceroy (2014) os provedores de conexão à internet são “pessoas jurídicas fornecedoras de serviços que consistem em possibilitar o acesso de seus consumidores à internet”, exemplo: Claro, Tim, Oi etc., e os provedores de aplicação de internet são qualquer empresa que “forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”, exemplos: Google, Instagram e Youtube.

Explica Haikal (2014, p. 323) que os provedores de aplicação diferem-se dos de conexão, “pois atuam somente dentro da rede mundial, [...] e são os agentes responsabilizáveis por danos decorrentes dos conteúdos que forem exibidos em suas plataformas ou atividades praticadas, na forma da lei.”

Registro de Acesso à Aplicação de Internet: assevera o art. 5º, VIII, da Lei do Marco Civil da Internet (LMCI) que registro de acesso à aplicação na internet é “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP” (BRASIL, 2014) , ou seja, a data e hora que determinado IP acessou alguma funcionalidade de algum site, exemplo: publicou um texto no Facebook.

De acordo com a LMCI, cabe aos provedores de aplicação a guarda dos registros de aplicação por um período de 6 (seis) meses (BRASIL, 2014).

Registro de Conexão: mais uma vez a LMCI em seu art. 5º, VI conceitua registro de conexão como “o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados” (BRASIL, 2014).

Os registros de conexão, diferente dos de acesso às funcionalidades, guardam o momento em que o usuário acessou a rede mundial de computadores, e não o momento em que entrou em um site por exemplo.

Segundo a Lei nº 12.965/2014, os provedores de conexão à internet devem guardar os registros de conexão pelo prazo de 1 (um) ano (BRASIL, 2014).

Endereço de Protocolo de Internet (endereço IP): é conceituado pela LMCI (art. 5º, III) como “o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais” (BRASIL, 2014); de forma que o número do IP seja único na rede (LIMA, 2016).

É importante saber que um dispositivo normalmente disporá de dois endereços IP, o interno (fixo) e o externo (pode ser fixo ou dinâmico), explica Salutes (2019) que “cada aparelho ou dispositivo possui um IP fixo [interno], enquanto a conexão com a internet gera IPs dinâmicos”; isso significa que cada vez que um dispositivo se conecta à rede mundial de computadores lhe é atribuído um endereço de IP externo; este IP externo é atribuído por um provedor de conexão e pode ser tanto o mesmo número todas as vezes (fixo) ou pode lhe ser atribuído um número diferente para cada conexão (dinâmico), a maioria dos provedores de conexão trabalham com IP dinâmico, ou seja, a cada conexão o usuário recebe um número diferente de IP externo (LIMA, 2016).

Tanto nos casos de registros de acesso à aplicação quanto nos de registros de conexão, é o IP externo que está registrado, pois esta é a única informação que chega ao ponto de destino (LIMA, 2016).

Domínios e Subdomínios: domínio é “um conjunto de caracteres que você coloca no navegador para encontrar um site na internet, como por exemplo registrocom.com” (O QUE..., [2020]) em outras palavras, domínio é o nome completo do site, incluindo o .com; .br; .org etc.

No site Registro.br, responsável por registrar os domínios no Brasil, consta que qualquer pessoa física ou jurídica pode criar um domínio br, desde que esteja domiciliada no Brasil e possua um contato no território nacional (RESGISTRO, [2020]).

Subdomínios, segundo Araujo (2018), “são extensões do domínio principal, que tem a função de facilitar a navegação do usuário, levando-o para sessões específicas dentro dele”, o processo de criação de um subdomínio é mais simples, uma vez que basta localizar o painel de controle dentro do próprio site e criar quantos subdomínios foram necessários; o que chama atenção, juridicamente falando, é o formato que esses subdomínios podem ser criados, explica Lima (2016) que o nome do subdomínio é sempre seguido pelo nome do domínio, o autor dá como exemplo o domínio cnn.com e seus subdomínios edition.cnn.com e sportsillustrated.cnn.com, “como iniciam o endereço de uma página, subdomínios com nomes semelhantes a domínios conhecidos são bastante utilizados em golpes na internet”; pode ser dado como exemplo um subdomínio hipotético itau.cnn.com.

Cookies: segunda o autora Furutani (2018):

> cookies são arquivos de texto simples, enviados pelo site ao navegador, na primeira vez que você o visita. Em seu próximo acesso, o navegador reenvia os dados ao site para que suas informações sejam configuradas de forma automática. É por isso que você não precisa digitar seu email e senha toda vez que entra no Facebook.

Explica Lima (2016) que a “função mais controversa dos *cookies* está ligada ao seu uso massivo em publicidade *on-line*”, de forma que o usuário possa receber uma publicidade personalizada de produtos de seu interesse.

Atualmente, é direito do usuário ser informado de forma clara sobre utilização de cookies pelo site visitado, de acordo com o art. 17, VIII, da Lei do Marco Civil da Internet (BRASIL, 2014).

Computação nas Nuvens: segundo a escritora Débora Silva (2015) “computação em nuvem é a possibilidade de acessar arquivos e executar diferentes tarefas pela internet, sem a necessidade de instalar aplicativos no computador. O armazenamento de dados é feito em serviços on-line, em uma rede.”

Ou seja, em vez de o usuário armazenar suas informações e documentos em seu HD pessoal ele armazena em outro HD pertencente à empresa prestadora de serviço de computação nas nuvens, com a vantagem de poder acessar essas informações de qualquer outro aparelho com conexão à internet (CRUZ, 2015).

Por sua vez, as empresas armazenam estes HD's em *Data Centers,* prédios que "existem em todo o mundo e são verdadeiras fortalezas, com vários níveis de segurança, tanto digital quanto física" (CRUZ, 2015).

Porém, lembra Lima (2016) que o armazenamento nas nuvens não é 100% seguro, cita o autor uma falha de serviço na empresa *Apple* em 2014, o que possibilitou que várias atrizes de Hollywood tivessem fotos íntimas divulgadas na rede, porque, apesar de os documentos não estarem mais no aparelho pessoal das vítimas, estavam armazenados no sistema de nuvem da *Apple*.

Criptografia: a criptografia pode ser uma dor de cabeça para algumas pessoas, entretanto, entender como ela funciona é essencial para aqueles que atuam na área jurídica, porque vez ou outra, o uso desta tecnologia pode encobrir e facilitar crimes.

Em palavras simples, criptografar um conteúdo significa transformá-lo em algo difícil de ser lido por quem não tem a permissão, a criptografia pode ser feita de várias formas e com vários níveis de complexidade, por exemplo, ela pode ser feita de forma bem simples como trocar as letras do alfabeto por números, ou pode ser feita de forma complexa como aquela utilizada por empresas como *Apple* e *Whatsapp,* de qualquer forma, a intenção desta tecnologia é impedir a leitura/acesso ao conteúdo por terceiros não autorizados (MYERS, 2017).

Já a criptografia de ponta-a-ponta, muito comentada no Brasil por causa do aplicativo *Whatsapp,* é feita para proteger dados que estão em trânsito, ou seja, que são passados de um dispositivo para outro, como conversas no aplicativo por exemplo, nesse sentido, o conteúdo é codificado de forma que um agente externo não consiga compreendê-lo, e só pode ser decodificado pela outra ponta da conversa, ou seja, pelo aparelho destinatário (COUTINHO, 2019).

Malwares: são *softwares* desenvolvidos com função de causar dano a outros, englobam vírus, cavalos de Tróia, *worms, ransomwares,* entre outros (LIMA, 2016).

"Embora [um] malware não possa danificar o hardware físico dos sistemas [...], ele pode roubar, criptografar ou excluir seus dados, alterar ou sequestrar funções essenciais do computador e espionar atividades de seu computador [...]" (TUDO..., [2018]).

Várias são as formas de contrair *malwares* no dispositivo, uma dela é através de *download* de aplicativos móveis através de permissões abusivas, segundo Mota (2019) "entre as permissões mais nocivas estão o acesso à localização em tempo real e à câmera, inicialização automática do aplicativo e o *upload* de arquivos para o sistema sem necessidade de autorização prévia".

Outra forma de um dispositivo contrair *malwares* é através da prática de *phishing,* nesta técnica "disparam-se milhares ou milhões de falsos comunicados para que, por meio de uma pescaria (*phishing),* se consiga fraudar uma significativa quantidade daqueles que receberam as mensagens" (LIMA, 2016), é comum que essa prática seja feita através de email, mas pode ser feita também em anúncios em sites como Facebook e Twitter.

Assim, conclui Peck (2016):

> Na sociedade digital, o advogado tem que ser um estrategista. A complexidade da sociedade traz maior complexidade jurídica [...]. Cabe ao profissional do direito dar os caminhos e as soluções viáveis, pensando no contexto competitivo e globalizado de um cliente virtual-real, convergente e multicultural.

2.2 A QUESTÃO TEMPORAL

Quando tratamos da violação dos direitos na área digital a primeira palavra que vem à mente é: tempo, tempo de propagação do ilícito e tempo para a resposta estatal, isso porque, explica Hance (1997 *apud* PAESANI, 2014, p. 78), a internet apresenta certas peculiaridades, entre elas está o fato de a internet ser um meio de comunicação

tão rápido quando o telefone e, ao mesmo tempo, ser um meio de comunicação escrita quase permanente, evidenciando a extensão e o potencial difamatório de uma mensagem divulgada na rede.

A questão temporal é tão importante que a autora Patrícia Peck (2016, p. 83-84) faz menção à Teoria Tridimensional do Direito (fato, valor e norma), a fim de inserir um quarto elemento e ela: o elemento tempo.

Para compreender o pensamento da autora, faz-se necessário um breve apontamento sobre a Teoria Tridimensional do Direito, comumente atribuída a Miguel Reale.

Explica Reale (*apud,* AUGUSTO, M., 2012) que o Direito não se resume em apenas um elemento, não é apenas letra de lei ou apenas uma manifestação cultural, e sim um conjunto de três elementos:

> Direito não é só norma, como quer Kelsen, Direito, não é só fato como rezam os marxistas ou os economistas do Direito, porque Direito não é economia. Direito não é produção econômica, mas envolve a produção econômica e nela interfere; o Direito não é principalmente valor, como pensam os adeptos do Direito Natural tomista, por exemplo, porque o Direito ao mesmo tempo é norma, é fato e é valor.

Gonzaga e Roque (2017) explicam o que seria o fato, o valor e a norma, o fato é o conjunto de circunstâncias que rodeiam o ser humano; o valor representa o valor atribuído aos fatos pelo ser humano em determinado momento histórico; e a norma é o resultado da integração do fato ao valor.

Esses três elementos formam o Direito, ocorre que para a autora Patrícia Peck, o Direito Digital é acrescido pelo elemento Tempo, aduz a autora que o conjunto fato, valor e norma necessita ter certa velocidade de resposta para que tenha validade dentro da sociedade digital (PECK, 2016, p. 83), para isso, Peck faz uma relação entre o Tempo e o Fato causador do ilícito, explica a escritora que o tempo pode ter uma relação ativa, passiva e reflexiva com o caso concreto.

A relação passiva do tempo e do fato é aquela em que o tempo levado até a solução do conflito é tão grande que custa mais caro do que o próprio bem, o tempo passivo é muito usado por agentes delituosos que acreditam que a morosidade judicial irá desencorajar a pessoa a buscar seus direitos, muito comum no direito consumerista (PECK, 2016, p. 84), neste caso, a consequência é o não ajuizamento da ação judicial

Por sua vez, a relação ativa entre tempo e fato seria quando o tempo levado para a resposta judicial tem capacidade de esvaziar o próprio direito subjetivo (PECK, 2016, p. 84), neste caso, a ação judicial foi ajuizada, mas se não for decidida em tempo hábil o direito precluirá

Por fim, a relação reflexiva é aquela que age ativa e passivamente concomitantemente, em contras palavras, é o liame de tempo que consegue, ao mesmo tempo, desencorajar a procura judicial e também ensejar a perda do direito se a atuação estatal não for exercida em tempo hábil, o tempo reflexivo é utilizado em crimes digitais, como pirataria, hackers e pedofilia (PECK, 2016, p. 84).

Seguindo essa linha de pensamento, a atuação em área digital exige novas técnicas de resolução de ilícitos, de forma a otimizar o tempo e garantir a efetiva aplicação do direito.

O advogado e professor de Direito Digital Fernando Brizola é um grande defensor da atuação extrajudicial para remoção de conteúdo ilícito publicado online.

Explica Brizola (2020) que a atuação extrajudicial nos ilícitos digitais é, basicamente, o aproveitamento da estrutura e organização da internet para forçar os administradores do site a retirar o conteúdo de forma espontânea, independentemente de ordem judicial, essa atuação envolve conhecer a estrutura da internet, o domínio dos sites, quais os administradores do site, quem são seus parceiros e qual sua organização interna.

Primeiramente, a forma mais simples de retirada de conteúdo online é contatando os próprios administradores do site, normalmente os sites mais populares

sempre disponibilizam um aba para contato, basta para o advogado juntar petição requerendo a retirada do link específico, juntando procuração e todos os documentos necessários (BRIZOLA, 2020).

No site Registro.br, responsável por registrar os domínios no Brasil, costa que “domínios que não estão registrados, não podem ser encontrados na Internet”, e que, ao registrar um domínio br é necessário CPF ou CNPJ e um contato no território nacional (RESGISTRO, [2020]).

As informações sobre o titular do site são públicas e podem ser consultadas pela própria internet, sites como o próprio Registro.br disponíbilizam uma aba de pesquisa de domínios, onde, pelo simples nome do site, é possível obter informações como o nome do titular, seu CPF e seu email.

Mas entrar em contato com o administrador do site não é a única opção antes do processo judicial, o advogado ainda tem a opção de denunciar o site para o seu “parceiro” (BRIZOLA, 2020); o que Fernando Brizola chama de parceiros são, em outras palavras, os provedores de hospedagem do site; Delavy (2016) explica que os provedores de hospedagem são responsáveis por guardar os arquivos do site, isso é necessário, “pois o domínio não guarda nenhum conteúdo do site, ele é apenas o endereço eletrônico (ou URL). O que faz esse papel é o servidor [de hospedagem].”

Ou seja, todo o site precisa contratar um provedor de hospedagem para armazenar seu conteúdo, porque o domínio por si só não é capaz de armazená-lo.

Sabendo que todo o conteúdo do site fica armazenado no respectivo servidor de hospedagem, uma das técnicas do professor Brizola (2020) para remoção de conteúdo ilícito é a requisição de remoção para o próprio provedor, mais uma vez anexando procuração e link específico.

De novo, as informações sobre os provedores de hospedagem são públicas e podem ser pesquisadas pela internet, sites como Whoishostingthis.com informam qual o provedor de hospedam é utilizado pelo site pela simples pesquisa de domínio.

Continuando, a atuação extrajudicial não é a única técnica que pode ser usada pelo advogado para otimizar o tempo nos casos de ilícitos digitais, técnicas de atuação judicial também são uma opção.

Em uma aula ministrada na Universidade do Sul de Santa Catarina (Unisul) para o Curso de Graduação em Direito, o professor e advogado Guilherme Bossle (2019) explicou uma técnica processual usada para retirar um vídeo difamatório de seu cliente da plataforma Youtube.

A técnica consiste na utilização da tutela de urgência de natureza antecipada requerida em caráter antecedente prevista no novo Código de Processo Civil (CPC); diz Theodoro Júnior (2017, p. 669) que “a tutela de urgência é satisfativa quando, para evitar ou fazer cessar o perigo de dano, confere, provisoriamente, ao autor, a garantia imediata das vantagens de direito material para os quais se busca a tutela definitiva”; já o caráter antecedente da tutela:

> [...] é destinado especificamente a proporcionar oportunidade à estabilização da medida provisória satisfativa. Baseia-se na existência de elementos que permitam, sem maiores dificuldades, o deferimento da liminar *inaudita altera parte,* com grande probabilidade de a medida não ser contestada (THEODORO JÚNIOR, 2017, p. 679).

Segundo o art. 303 e ss. do CPC, o requerimento da tutela antecipada em caráter antecedente se faz com a apresentação do requerimento de antecipação da tutela antes do pedido principal, apenas indicando o pedido de tutela final, com a exposição da lide, do direito que se busca realizar, do perigo de dano e do valor da causa (BRASIL, 2015)

Neste procedimento, a tutela antecipada concedida torna-se estável se da decisão que a conceder não for interposto o respectivo recurso (BRASIL, 2015).

Ou seja, este tipo de procedimento é excelente quando houver grande probabilidade de o réu não recorrer, no caso concreto citado pelo professor Bossle (2019) havia um vídeo difamatório contra seu cliente na plataforma Youtube, imaginando que o Google (empresa dona do Youtube) não iria recorrer por um simples vídeo, utilizou-se do procedimento descrito nos arts. 303 e seguintes do CPC, ao final,

a tutela de urgência foi deferida e a empresa não recorreu, estabilizando-se os efeitos da decisão.

Assim, com a internet cada vez mais rápida e a infeliz morosidade do judiciário brasileiro, cabe aos juristas desenvolverem e explorarem novas técnicas de atuação, a fim de tornarem realmente efetivas as leis e garantirem a implementação da justiça, tanto no mundo físico quanto no digital.

2.3 MEIOS DE PROVA DIGITAIS

Segundo os autores Thamay e Tamer (2020) prova digital pode ser conceituada como “o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de um determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração“.

De acordo com Peck (2016, p. 262) “não há nenhuma legislação brasileira que proíba ou vete a utilização de prova eletrônica”, pelo contrário, o art. 369 do CPC aduz que “as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa [...]” (BRASIL, 2015).

Quanto à validade de um documento, segundo Faria e Silva (2006 *apud* TONELLI, 2020) para que um documento seja considerado um elemento de prova são necessários três requisitos básicos, quais sejam: autenticidade, integridade e tempestividade.

Começando por autenticidade, este requisito pode ser entendido por “a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital” (THAMAY e TAMER, 2020).

A assinatura digital é considerada um meio seguro de identificar o signatário porque, segundo Tonelli (2020):

> Quando assina-se um documento eletrônico com sua assinatura digital, a hora e data da assinatura, o conteúdo que fora assinado e a pessoa que o assinou são verificáveis. Assim, consegue-se determinar a validade do documento eletrônico, estando satisfeitos os requisitos da autenticidade, integridade, perenidade e tempestividade de seu conteúdo a partir do uso da ferramenta.

Adverte Tonelli (2020) que a assinatura eletrônica é gênero, da qual a assinatura digital é espécie, também são assinaturas eletrônicas as senhas, autenticação biométrica, números de PIN, entre outros.

A própria Medida Provisória nº 2.200-2/2001, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, aduz que o ICP foi criado exatamente para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica (art. 1º), bem como afirma em seu art. 10, §1º que “as declarações constantes dos documento de forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pelo ICP-Brasil presumem-se verdadeiras em relação aos signatários [...]” (BRASIL, 2001).

Como nem sempre as provas digitais apresentam assinatura digital, a própria MP nº 2.200-2/2001 assegura que “o disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e da integridade de documentos de forma eletrônica, inclusive os que utilizem certificados não emitidos pelo ICP-Brasil, desde que admitidos pelas partes [...]” (BRASIL, 2001); não bastasse o disposto na referida MP, o Código de Processo Civil já dispõe que não dependem de prova os fatos alegados por uma parte e confessados pela parte contrária (CPC, art. 374, II), bem como serão presumidas verdadeiras as alegações feitas pelo autor e não contestadas pelo réu (CPC, art. 344) (BRASIL, 2015).

Seria muito simples se todas as provas digitais viessem com a assinatura de seu autor, mas esta não é a realidade cotidiana, principalmente quando se trata da prova de um ilícito cometido online, casos como postagens ofensivas nas redes sociais, *hackers*, divulgação de conteúdo íntimo, violação dos direitos autorais, entre outros; nestes casos Thamay e Tamer (2020) ensinam que a maneira mais correta de “atestar a autenticidade de tal prova é realizando a quebra de sigilo da postagem, com

o fornecimento judicial das informações por parte dos provedores de aplicação e conexão".

Como exemplo, para saber a identidade de uma pessoa que utilizou sua internet doméstica para postar ofensas na rede social *Facebook*, será necessária a quebra de sigilo da postagem para acessar os registros de aplicação no site Facebook (provedor de aplicação); apenas com as informações fornecidas pelo provedor de aplicação é que será identificado o provedor de conexão, e, por fim, o provedor de conexão identificará a pessoa física (THAMAY e TAMER, 2020), isso acontece porque o provedor de aplicação mantêm guardado os registros de aplicação do usuário (data e hora que o IP externo acessou a funcionalidade) de acordo com o disposto na LMCI, bem como os provedores de conexão também mantêm seus registros armazenados pelo tempo legal, lembrando que é o provedor de conexão que fornece o número IP externo para seu cliente, desta forma fica simples para a empresa identificar a quem forneceu aquele número em determinado dia e hora.

Deve-se ter atenção com a quebra de sigilo de postagem como forma de obtenção de provas, isso porque a Lei do Marco Civil da Internet (Lei nº 12.965/14) determina que os provedores de aplicação devem manter os respectivos registros de acesso a aplicações de internet pelo prazo de apenas 6 (seis) meses (BRASIL, 2014).

Continuando sobre os requisitos de validade das provas, a integridade é a "característica daquilo que se apresenta ileso, intacto, íntegro. Um documento é considerado íntegro quando não houve adulteração de seu conteúdo posterior a sua criação" (FARIA e SILVA, 2006, p. 20, *apud* TONELLI, 2020).

Segundo Thamay e Tamer (2020) "é por essa razão que a coleta de prova deve ser revestida por procedimentos tecnicamente aptos a demonstrar que o elemento probatório permaneceu intacto e inalterado, do momento da realização do fato até a apresentação da prova".

Por exemplo, uma ata notarial é uma prova preferível à um *printscreen,* porque este pode ser facilmente adulterado, enquanto a ata notarial conta com a fé-pública do tabelião responsável pela sua lavratura (THAMAY e TAMER, 2020). Citar CPC

Diz Tonelli (2020) que outra forma de garantir a integridade da prova digital é fazendo uso da tecnologia de *Blockchain*.

Para entender como funciona essa tecnologia, em palavras simples, Bassotto (2018) explica que o *Blockchain* foi criado para garantir a inalterabilidade das informações que são inseridas nele, a tecnologia funciona da seguinte forma: ela armazena as informações em blocos, cada informação (documento, contrato, transação) é um bloco, cada bloco possui um resumo das informações contidas nele, este resumo é chamado de *hash,* esses blocos estão conectados (formando uma corrente) e são dependentes uns dos outros, cada bloco possui o número de seu *hash* e também o número de *hash* do bloco anterior a ele na corrente e assim sucessivamente, se alguém modificar o conteúdo de algum dos blocos, consequentemente o *hash* também será modificado, de forma que para modificar o conteúdo de um dos blocos sem ser percebido, é necessário mudar o conteúdo de toda a corrente; não bastasse isso, Bassotto (2018) continua explicando que, no *Blockchain*, essas informações ficam armazenadas em milhares de computadores espalhados pelo mundo, cada computador tem uma cópia dos registros, por isso se um *hacker* invadir um dos computadores para modificar seu banco de dados, aquele computadores será expulso pelos outros, de forma que uma vez inserida uma informação na corrente, torna-se muito difícil modificá-la.

No Brasil a empresa OriginalMy presta serviços de armazenamento de provas digitais por tecnologia *Blockchain*, segundo a empresa o seu sistema “faz uma cópia completa do conteúdo que está sendo visualizado no seu navegador e gera um relatório comprovando a sua existência. A partir do relatório gerado pelo plugin, é criado um hash, código único e exclusivo [...]” (ORIGINALMY, [2020]) .

Na opinião de Tonelli (2020):

> [...] O Blockchain consegue garantir a autenticidade, a integridade, a perenidade e a tempestividade de um documento, uma vez que possui *timestamp* e qualquer adulteração em seu conteúdo causará alterações na sequência que identifica este documento (Hash).

O *timestamp* citado pelo autor significa que o *Blockchain* além de armazenar a informação, contabiliza o tempo e a data que o evento ocorreu.

Chega-se então ao último requisito para a validade da prova digital: a tempestividade.

Como visto acima o próprio *Blockchain* tem um registro de tempo de data do documento, este registro, assim como as informações contidas no bloco, não pode ser modificado; mais uma vez, a empresa OriginalMy oferece funcionalidades de assinatura de contratos e documentos digitais.

Ainda como dito acima, a ata notarial também tem o condão de atestar o momento da verificação do ilícito; lembrando que vários são as formas que registram o tempo e data na internet, como a data de recebimento de email e data da postagem de uma publicação em mídia social, nestes casos, cabe ao juiz analisar a prova e atribuir a ela o valor que julgar adequado; uma vez que o novo CPC adotou o sistema de persuasão racional da prova, ou seja, o juiz "formará seu conhecimento com liberdade e segundo a consciência formada" (THEODORO JÚNIOR, 2017, p. 886).

Não pretendendo o esgotamento dos meios de prova, ainda cabe mencionar um dos mais importantes: a prova pericial digital.

Segundo Thamay e Tamer (2020):

> [...] o perito em tecnologia será responsável pela explicação do fato, esclarecendo o funcionamento dos dispositivos e tecnologias envolvidas e como essas foram utilizadas. [...] É, em regra, a prova necessária para a constituição do fato que teve a tecnologia como suporte.

A perícia digital pode ser utilizada, por exemplo, para a identificação da autoria de um ilícito cibernético e também constatação da prática de concorrência desleal por parte de uma empresa, entre outras possibilidades (THAMAY e TAMER, 2020).

Por fim, de acordo com o CPC (art. 369), qualquer prova lícita e moralmente legítima pode ser utilizada no ordenamento jurídico brasileiro (BRASIL, 2015),

podendo o juiz formar seu convencimento de maneira livre, desde que motivado e seguindo uma raciocínio lógico (THEODORO JÚNIOR, 2017, p. 886).

3 MANIFESTAÇÕES SOCIAIS E O REFLEXO NO PODER LEGISLATIVO

Os parlamentares são os representantes do povo por disposição constitucional (BRASIL, 1988), em suas opiniões e ações está refletida a vontade de seu eleitorado, sendo assim, quando a sociedade começa a exteriorizar uma posicionamento, seja considerado bom ou ruim, é comum os legisladores tentarem regulamentar suas ações.

A intenção do terceiro capítulo é demonstrar como a sociedade incorpora a internet na vida cotidiana e quais são as consequências (sociais e legislativas) que isso causa.

3.1 DISSEMINAÇÃO EM MASSA DE NOTÍCIAS FRAUDULENTAS (FAKE NEWS)

O termo *Fake New* em tradução literal significa notícia falsa, sobre este conceito, explicam Rais e Sales (2020):

> [...] talvez um conceito aproximado do Direito, porém distante da polissemia empregada em seu uso comum, poderia ser identificada como uma mensagem propositadamente mentirosa capaz de gerar dano efetivo ou potencial em busca de alguma vantagem.

Ainda, o termo notícia falsa ou fraudulenta é bastante vago, por isso na tentativa de demonstrar o que seriam as *fake news*, a jornalista e escritora britânica Claire Wardle (2017, tradução nossa) criou uma lista contendo sete tipos de notícias falsas que podem ser identificadas, são elas:

> Sátira ou paródia: sem intenção de causar mal, mas tem potencial de enganar;
> Falsa conexão: quando manchetes, imagens ou legendas não mantêm relação com o conteúdo;
> Conteúdo enganoso: uso enganoso de uma informação para usá-la contra um assunto ou um indivíduo;
> Falso contexto: quando um conteúdo genuíno é compartilhado com um contexto falso;
> Conteúdo impostor: quando fontes genuínas são falsamente representadas[1]
> Conteúdo Manipulado: quando uma informação genuína ou imagem é usada para enganar;

[1] Quando a autora diz que fontes são falsamente representadas, ela quer dizer que estão sendo atribuído àquelas pessoas palavras ou ações que não são delas.

> Conteúdo fabricado: novo conteúdo 100% falso e construído com o intuito de enganar e causar mal.

Esta lista serve como um norte para a compreensão do que seriam as notícias fraudulentas, não deve ser entendida, entretanto, como uma lista taxativa, porque novas formas de *fake news* ainda podem surgir, levando em consideração que a tecnologia está sempre em evolução e que o fenômeno das notícias falsas ainda é recente.

Com o conceito de *fake news* em mente, é necessário entender ainda o motivo pelo qual essas notícias são criadas, mais uma vez a autora Wardle (2017, tradução nossa) apresenta um rol de principais motivos para a criação de notícias inverídicas, são eles: jornalismo ruim, parodiar, provocar, por paixão, por partidarismo, por lucro, por influência política, por poder ou propaganda.

Certamente não foi a internet que criou as *fake news*, mas podemos afirmar que foi ela a maior facilitadora da propagação destas notícias, isso pelo fato de reunir um tráfego de pessoas grande e de fácil acesso, possibilitar o compartilhamento em poucos segundos, e ainda, proporcionar um aparente anonimato aos usuários, o que facilita a criação de notícias fraudulentas.

Na opinião do professor de filosofia Dr. Wilson Gomes (2019), as *fake news* contemporâneas são feitas exatamente para circularem no meio digital, apenas causando seus efeitos no mundo físico.

Talvez uma das maiores contribuições digitais para a propagação de *fake news* é o uso dos chamados robôs para disseminar as notícias falsas, segundo Ruediger (2017) os robôs são contas controladas por *softwares* se fazendo passar por seres humanos, que já dominam parte da vida nas redes sociais e participam ativamente das discussões em momentos políticos de grande repercussão.

Essas contas robotizadas agem se passando por seres humanos, participando de debates, postando opiniões e publicando notícias, muitas vezes fraudulentas, a fim de influenciar a opinião dos usuários. Todas essas postagens acontecem em uma velocidade inumana, fazendo com que os robôs dominem grande parte dos debates

online, falando sobre o assunto Ruediger (2017) explica que um estudo feito pela FGV/DAPP aponta que esse tipo de conta chegou a ser responsável por mais de 10% das interações no Twitter nas eleições presidenciais de 2014, e durante os protestos pelo Impeachment, essas interações provocadas por robôs representaram mais de 20% do debate entre apoiadores de Dilma Rousseff.

Não bastasse a criação robotizada em massa das *fake news*, segundo uma pesquisa feita pelo Instituto de Tecnologia de Massachusetts, comentada por Cymbaluk (2018), a chance de uma notícia falsa ser repassada é 70% maior do que a de notícias verdadeiras.

Tamanho sucesso para o compartilhamento dessas notícias deve-se principalmente ao caráter emocional de seu conteúdo, por ser um conteúdo falso ele é criado para ser viral, sem preocupação com manter relação com a verdade e muitas vezes com a lógica, é um conteúdo criado para assustar e causar irritações, e assim conseguir um maior engajamento social.

Agora, deixando de lado aquelas notícias falsas que são criadas apenas para causar alvoroço e focalizando nos esquemas organizados de disseminação em massa de notícias fraudulentas, é possível afirmar que as *fake news* atingiram seus interesses?

Para responder essa pergunta, cita-se um caso emblemático dos efeitos causados pelas notícias fraudulentas: a campanha eleitoral brasileira de 2018, onde as notícias fraudulentas causaram grande impacto na escolha dos candidatos e também definiram um comportamento que nunca antes foi visto com tanto peso nas eleições passadas: uma grande polarização política entre os eleitores, marcada por discursos de ódio.

Como já foi dito, o conteúdo de uma *fake new* é feito unicamente para viralizar, no casos daquelas notícias que circulavam à época das eleições de 2018, elas eram carregadas de informações difamadoras, criadas para causar desconforto e até ódio pelo candidato, como o vídeo do candidato Ciro Gomes agredindo sua ex-esposa Patrícia Pillar, a criação e distribuição do que foi chamado de kit gay pelo candidato

Fernando Hadad e a notícia de que a candidata Marina Silva invadiu uma fazenda no Acre, todas notícias fraudulentas (PEREIRA, TOLEDO e MONNERAT, 2018)

Falando sobre o assunto, com muita propriedade, escrevem Rais e Sales (2020):

> É claro que a desinformação polui o debate e cria uma atmosfera de incertezas e desconfiança, mas talvez o que parece ser ainda mais perigoso é a capacidade que essa poluição tem de alimentar e ampliar a polarização de opiniões na sociedade. Talvez a polarização seja a infecção, enquanto a desinformação seja apenas uma de suas febres.

O sentimento de ódio de um eleitorado polarizado ameaça principalmente a segurança dos próprios cidadãos, visto que os eleitores se tornam mais agressivos movidos pelo fanatismo político, o professor Eugênio Bucci (2018) cita alguns casos de extreminsto político como: os disparos de arma de fogo feitos contra a caravana promovida pelo Partido dos Trabalhadores no estado do Paraná, o assassinato da vereadora Marielle Franco no Rio de Janeiro e o atentado à faca que perfurou o intestino do candidato Jair Bolsonaro durante a campanha em Minas Gerais.

Entendido o fenômeno das notícias fraudulentas, como ele se propaga e quais seus efeitos, resta compreender como funciona a responsabilização das pessoas por trás da disseminação de tais notícias.

Deve ficar claro que as notícias consideradas fraudulentas não estão abrangidas pelo direito fundamental da liberdade de expressão como foi decidido no julgamento da ADI 4451, isso porque, as notícias fraudulentas modificam a realidade a fim de controlar a opinião alheia, talhando a própria liberdade nas manifestações, nas palavras do ministro Luiz Fuz:

> Nós temos hoje, basicamente, dois princípios no campo das fake news, essas notícias enganosas. Em primeiro lugar, há necessidade da lisura informacional, porque o voto é livre na medida em que ele é livre de suborno, corrupção e desinformação também. Se nós queremos um voto livre e consciente, não podemos chancelar fake news, que são notícias sabidamente inverídicas, propagáveis, massificadas, que viralizam num tempo recorde, sob o pálio da liberdade de expressão (BRASIL, 2019).

Falando de responsabilização, começando pelas pessoas (naturais ou jurídicas) que criam as notícias fraudulentas, para Camillo (2020), desde que estejam provados os pressupostos da responsabilidade civil, é cabível, na forma do art. 12 do CC (direitos de personalidade), a obtenção de tutela preventiva ou repressiva, reclamando-se, em qualquer hipótese, perdas e danos, sem prejuízo de outras sanções.

Quando fala-se em responsabilidade por criação e divulgação de *fake news* deve-se lembrar dos provedores de internet, como visto anteriormente a Lei do Marco Civil da Internet (Lei nº 12.965/2014) apresenta dois tipos de provedores, os provedores de conexão com a internet e os provedores de aplicação de internet (BRASIL, 2014).

Existe uma diferença de responsabilização para estes dois provedores, para o provedor de conexão, a Lei nº 12.965/2014 afirma que este não será responsabilizado civilmente por danos causados por terceiros (art. 18), já para os provedores de aplicação, em regra também não há responsabilização por danos causados por terceiros, salvo se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (art. 19) (BRASIL, 2014).

Mas essa postura branda adotada pela LMCI talvez esteja com os dias contados, isso porque tramita no Congresso Nacional um Projeto de Lei (PL 2630/2020) que pretende instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, com o objetivo principal de combate à desinformação e, para atingir tal objetivo, atribui vários deveres aos provedores de aplicação (BRASIL, 2020), o PL não faz menção aos provedores de conexão, o que faz concluir que o texto do art. 18 da LMCI continua inalterado.

Referido PL traz em seu texto inicial várias responsabilidades aos provedores de aplicação, entre elas estão: a obrigatoriedade de o provedor desenvolver procedimentos para melhorar as proteções da sociedade contra comportamentos ilícitos (art. 5º, §3º); dever de transparência que determina a publicação pelo provedor

de aplicação de várias informações, principalmente relacionadas à contas que promovem conteúdo desinformativo (art. 6º e ss.); adoção de medidas contra desinformação (art. 9º e ss.) e; limitação de número de encaminhamento de mensagens em épocas de eleições, calamidades públicas e situações de emergência (art. 13, §1º), entre outras (BRASIL, 2020).

O PL 2630/2020 é polêmico desde sua criação, isso porque, apesar de conter vários artigos que garantam a liberdade de expressão, inclusive fazendo menção aos princípios norteadores da Lei do Marco Civil da Internet, ele foi recebido com receio por muitos que acreditam que suas obrigações seriam uma limitação injustificada na liberdade de expressão e, consequentemente, uma censura.

Para refletir sobre essa preocupação, antes devemos voltar alguns parágrafos acima e lembrar que já foi decidido no STF que a disseminação de notícias fraudulentas não é abrangida pela liberdade de expressão, por todos os fundamentos já expostos.

Na opinião da advogada Raquel Saraiva (2020), a PL chega a censurar na medida em que as pessoas não vão conseguir se expressar, havendo uma ameaça clara aos debates públicos em ambientes como o Twitter, pois a qualquer momento a conta poderá ser denunciada e o usuário terá que se identificar, a advogada ainda acrescenta que esse fenômeno causaria uma autocensura nas mídias sociais.

Por outro lado, falando sobre a supervalorização da liberdade de expressão em detrimento de outros direitos, Martins e Longhi (2020) citam:

> [...] há quem sempre levante a bandeira da liberdade de expressão independente do conteúdo do que é dito. Qualquer restrição seria censura e ponto. Criticando essa posição, tendo em mente o sistema americano, Mary Anne Franks chama de "fundamentalistas" da Primeira Emenda os que justificam queima de bandeiras, saudações nazistas, pornografia infantil virtual, videogames violentos, doações corporativas a políticos, pornografia de vingança, instruções de fabricação de bombas, vídeos de recrutamento de terroristas, teorias da conspiração, registros médicos hackeados, spam, vírus de computador e até impressoras 3D. Caso de alguma maneira se restrinja o conteúdo ou se responsabilize seu criador: "Censura. Censura em qualquer lugar".

Ainda segundo o pensamento de Martins e Longhi (2020), ao contrário do que alguns autores pensam, a PL 2630/2020 não promove censura, e sim atribuí aos provedores de aplicação deveres de combate à desinformação, bem como assegura mais de uma vez em seu texto a liberdade de expressão, citam o art. 5º, §1º da PL, que dispõe: “as vedações do *caput* não implicarão restrição ao livre desenvolvimento da personalidade individual, à manifestação artística, intelectual, de conteúdo satírico, religioso, ficcional, literário ou qualquer outra forma de manifestação cultural [...]” (BRASIL, 2020).

A real intenção da PL 2630/2020 é exatamente garantir a liberdade de expressão na rede, como diz Nohara (2020):

> [...] O Estado não pode exercer censura, mas não significa que ele não deva criar, via regulação condições para que haja uma internet livre. Ademais, um dos grandes desafios de manter as condições para que haja reflexões mais equitativas a partir do acesso à informação seria a manutenção da neutralidade da rede.

Ainda, a possível censura causada pela PL não é a única crítica a ela, segundo Saraiva (2020) o projeto traz ameaças também a privacidade do usuário, cita a autora a obrigação das plataformas identificarem todas as contas de usuários que forem denunciados, aponta que o artigo é muito vago e que ainda pode ser instrumentalizado de forma que alguns usuários sofram perseguições online por alguma denúncia feita por um opositor contrário a diversidade de opinião.

A fim de provar a necessidade da criação da PL, Martins e Longhi (2020) lembram do sistema americano de responsabilização dos provedores, que baseia-se no *notice and takedown* (notificação e retirada), o que significa basicamente que o conteúdo ilícito só será removido após notificação, muito parecido ao art. 19 da LMCI, este sistema “é alvo de críticas pela doutrina local, já que a imunidade dos provedores criou ao longo de décadas uma situação que incrementa riscos de discursos de ódio, desinformação, *cyberbullying* às vítimas”.

Concluindo sobre o assunto, Martins e Longhi escrevem (2020):

> [...] o Marco Civil, ao imunizar o provedor antes de ordem judicial nos termos do art. 19, deixa as vítima de ataques *online* em situação de vulnerabilidade agravada, pois põe sob seus ombros o dever de procurar a Justiça, indicar os *links* e aguardar o cumprimento de decisão judicial pelo provedor para retirar um conteúdo que lhe cause dano. Ao mesmo tempo, enaltece o poder privado dos provedores pois são eles que redigem unilateralmente as cláusulas contratuais de suas políticas de conteúdo, e têm ampla liberdade para retirar ou não determinado conteúdo, taxá-lo de violento, falso ou qualquer outro, mas, acima de tudo, lucrar com a publicidade advinda dos dados dele decorrentes sem se responsabilizar.

A internet possibilitou a qualquer um falar qualquer coisa, o que desaguou em notícias fraudulentas, muitas vezes caracterizadas por discursos de ódio, que radicalizam o comportamento humano e põem em risco a democracia e a própria segurança física das pessoas envolvidas.

É neste cenário que nasceu a PL 2630/2020, aprovada pelo Senado Federal e com muita possibilidade de ser aprovado na Câmara dos Deputados, o que demonstra que o movimento social reflete diretamente no desenvolvimento legislativo de um país, moldando o Direito às necessidades manifestadas pela população.

3.2 PORNOGRAFIA DE VINGANÇA (*PORN REVANGE)*

Segundo Crespo (2014 *apud* CARVALHO, 2019, p. 55) *porn revange*:

> [...] é uma forma de violência moral (com cunho sexual) que envolve a publicação na internet (principalmente nas redes sociais) e distribuição com o auxílio da tecnologia (especialmente com smartphones), sem consentimento, de fotos e/ou vídeos de conteúdo sexual explícito ou com nudez. As vítimas quase sempre são mulheres, e os agressores, quase sempre são ex-amantes, ex-namorados, ex-marido ou pessoas que, de qualquer forma, tiveram algum relacionamento afetivo com a vítima [...].

A prática de pornografia de vingança antige de forma descomunal a vida íntima da vítima, levando em alguns casos ao suicídio (LIMA, 2016), apenas a título de exemplo, Rocha (2017 *apud* PANIAGO, 2020) cita o caso de Júlia Rebeca dos Santos, adolescente de 17 anos, que se suicidou dias após um vídeo sexual seu ser vazado na rede em 2013.

Ainda, a prática da pornografia de vingança pode ser considerada um ataque de gênero; Valente, Neris, Ruiz e Bulgarelli (2016, p. 13), após pesquisas em

jurisprudência, estudo de casos e entrevistas, concluíram que a maioria das vítimas são mulheres, bem como a maioria dos infratores, homens.

A prática de *porn revange* se torna ainda mais danosa pelo fato de que, não bastasse a exposição da intimidade, a vítima ainda é apontada como principal culpada por suas fotos ou vídeos terem sido divulgados:

> [...] discursos no sentido que as mulheres “não deveriam ter feito isso” (ter realizado prática sexual, ou ter-se deixado fotografar ou filmar nessa prática), como *normativa primordial,* a se *sobrepor ou mesmo substituir* a condenação moral do compartilhamento não autorizado das imagens íntimas [...] (VALENTE, NERIS, RUIZ e BULGARELLI, 2016, p. 16).

No que diz respeito ao dano causado à vítima, a pornografia de vingança está intimamente ligada aos direitos de personalidade, principalmente à imagem, honra e intimidade, causando, inegavelmente, um dano moral, além de poder causar dano material, com a perda do emprego, por exemplo (VIEGAS e PAMPLONA FILHO, 2020).

Explicam Gagliano e Pamplona Filho (2016, p. 231) que o direito à intimidade se traduz, primordialmente, no direito à vida privada, ou seja, a exigência de que alguns aspectos da vida pessoal de cada ser humano não chegue a conhecimento de terceiros.

Já o direito à honra e à imagem englobam o que Gagliano e Pamplona Filho (2016, p. 233-235) chamam de direito à integridade moral do ser humano, sendo a honra traduzida na forma em que a sociedade enxerga a pessoa (honra objetiva), a sua reputação em outras palavras, bem como na forma em que a pessoa enxerga ela mesma (honra subjetiva) como consciência da própria dignidade; no que diz respeito à proteção da imagem, significa que nenhuma pessoa pode ter sua imagem divulgada sem sua autorização, exceto nos casos de necessidade de manutenção da ordem pública ou administração da justiça (CC, art. 20), aproveitam os autores para caracterizar a imagem como a “essência da individualidade humana”, merecedora de uma resposta judicial firme nos casos de sua violação.

Segundo o artigo 12 do Código Civil, provado o dano aos direitos de personalidade, a vítima pode “exigir que cesse a ameaça, ou a lesão [...], e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei” (BRASIL, 2002); iniciando a busca por reparação, primeiramente deve-se compreender quem será o réu da ação, se é a pessoa natural que praticou o ato ou o provedor de aplicação em que a foto ou vídeo está exposto.

Esta questão depende se a vítima pretende a reparação dos danos causados ou se simplesmente busca a retirada da foto ou vídeo da rede, se pretender a retirada, será demandado o provedor preferivelmente, porque detém de meios mais rápidos para retirar a postagem da rede, cito o exemplo dado na capítulo anterior A Questão Temporal, em que o provedor de aplicação Google retirou um vídeo difamatório de Youtube em dias, sem ao menos contestar a decisão.

Já se a vítima pretende a reparação do dano, ela pode acionar tanto o infrator quanto o provedor de aplicação em alguns casos.

Anteriormente no capítulo Divulgação em Massa de Notícias Fraudulentas (*Fake News*) foi dito que os provedores de aplicação só poderão ser responsabilizados se, após ordem judicial, não tornarem indisponível o conteúdo apontado como infringente, ocorre que nos casos de pornografia de vinguança essa regra é excetuada.

O artigo 21 da LMCI permite a responsabilização subsidiária dos provedores de aplicação que, após notificação da própria vítima ou seu representante, não retirarem da rede imagens, vídeos ou outros materiais contendo cenas de nudez ou atos sexuais de caráter privado divulgadas sem autorização dos participantes (BRASIL, 2014).

Entretanto, o caput e parágrafo único do artigo 21 ainda trazem algumas condições para a responsabilização subsidiária dos provedores, são elas: a) o provedor só está obrigado a promover as diligências no âmbito e nos limites técnicos de seu serviço; b) o pedido deve ser feito por parte legítima e; c) a vítima deve

apresentar elementos que permitam a identificação específica do material apontado como violador da intimidade (BRASIL, 2014).

Sobre os itens B e C explica Gonçalves (2017, p. 158) que a identificação específica do conteúdo é feita pelo endereço virtual que contém as imagens violadas, o URL em outras palavras, uma vez que “grandes provedores não conseguem identificar, no mar de dados que administram, quais são aqueles violadores da intimidade”, quanto à legitimidade, diz o autor que o ofendido deve provar estar no vídeo ou na foto, caso contrário o provedor não deve retirar o conteúdo.

Nos casos em que a vítima pretende demandar a pessoa física que foi a responsável pelo compartilhamento do conteúdo, dois pontos devem ser destacados: a prova de autoria e a prova de materialidade.

Em uma entrevista concedida a Valente, Neris, Ruiz e Bulgarelli (2016, p. 61-62) a delegada Magali Vaz explica que “é muito comum que a vítima, impulsionada pela vergonha, não guarde as evidências necessárias para processar um possível autor - a vítima acaba apagando arquivos, mensagens, *printscreens*”.

Nesse sentido deve-se ter em mente que, se a vítima pretende ser ressarcida dos danos a ela causados, deve proceder a coleta de provas antes de qualquer ação (judicial ou extrajudicial) para retirada do conteúdo da rede.

Lembrando que, na produção de provas, devem ser seguidos os requisitos já explicados na capítulo anterior Meios de Prova Digitais, a fim de se assegurar a força probante dos documentos, são eles: autenticidade, integridade e tempestividade, no que couberem ao caso.

Para provar a materialidade na prática do *porn revange* a vítima pode se valer de *printscreens,* atas notariais ou tecnologia *blockchain,* lembrando que a ata notarial ainda é o meio de prova mais preferível, como dizem Thamay e Tamer (2020), uma vez que conta com a fé-pública do tabelião responsável pela sua lavratura.

Quanto à prova de autoria, a medida mais eficiente ainda é a identificação através de quebra de sigilo de postagem (THAMAY e TAMER, 2020), seguindo o procedimento anteriormente explicado, primeiramente requisitar judicialmente a quebra do sigilo de postagem para identificação do IP externo pelo provedor de aplicação, para posteriormente identificar o provedor de conexão através do número do IP externo, e, por fim, identificar as informações particulares do titular do plano de internet que serão fornecidas pelo provedor de conexão, isso se o réu estiver usando sua internet doméstica, se não, as investigações deverão tomar rumos mais complexos.

Como não poderia deixar de ser, as ações feitas pela sociedade refletem diretamente no processo legislativo, tendo em vista que a pornografia de revanche atinge em sua maioria mulheres, foi criada em 2018 a Lei nº 13.772/2018, que alterou o art. 7º, II da Lei nº 11.340/2006 (Lei Maria da Penha) a fim de acrescentar a violação da intimidade como forma de violência à mulher (BRASIL, 2018b).

Além disso, referida lei ainda acrescentou ao Código Penal o artigo 216-B que tipifica o ato de produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participante, e comina pena de 6 (seis) meses a 1 (um) ano (BRASIL, 1940).

Se debruçando sobre a questão se o termo violação da intimidade se restringiria apenas ao aspecto sexual, ou se abrangeria outros questões cotidianas (como brigas de família), os autores Leitão e Oliveira (2019), opinão pela primeira opção, afirmando que a intenção do legislador foi ampliar a proteção à mulher apenas no âmbito sexual, explicam os autores:

> Em respostas as estas inquietações e seguindo a linha de interpretação (e exegese) sempre com observação da “mens legis”, pensamos que o legislador ordinário por meio da alteração legislativa em comento, quis ampliar o âmbito de proteção da mulher, vítima de violência de gênero, mas apenas no campo da intimidade sexual. Tanto é verdade, que na parte da lei incriminadora trouxe também um dispositivo legal sob rubrica de **“registro de imagem não autorizada de intimidade sexual”** (o que reforça nosso ponto de vista do viés apenas de a violação de intimidade estar relacionada com a intimidade sexual). (Grifo do autor)

Por mais que as formas de repressão (civil e penal) funcionem, ou seja, por mais que o infrator pague indenização e cumpra a sanção penal imposta, não significa que a prática de *porn revange* terminará ou diminuirá, por isso é necessário um investimento preventivo, a fim de extinguir ou diminuir o dano causado à vítima.

Lamentam Valente, Neris, Ruiz e Bulgarelli (2016, p. 162) que em 2015 foi retirada do Plano Nacional de Educação (PNE) a proposta de "superação de desigualdades educacionais, com ênfase na promoção de igualdade racial, regional, de gênero e de orientação sexual" e foi substituída por uma proposta genérica, como a "promoção da cidania e erradicação de todas as formas de discriminação", em decorrência de pressão de uma ala conservadora de parlamentares federais.

Ainda sobre o assunto prevenção, a sociedade civil também tem se organizado para tentar conversar com os jovens sobre esse tipo de assunto, em uma entrevista concedida à Valente, Neris, Ruiz e Bulgarelli (2016, p. 160), a ativista Marilda Santos, atuante no projeto Sementeiras de Direito, explica que a intenção do projeto é valorizar o corpo feminino, em suas palavras:

> O que trabalhamos com elas não é o que a mídia anda fazendo ou o que os meninos fizeram, mas sim a valorização do corpo delas. Se você quer e você se expõe o corpo é seu, ninguém tem que andar de burca para que não seja exposto, mas você tem que ter uma postura, uma firmeza para que ninguém saia te apontando ou intitulando na rua de qualquer coisa. O que o IBEAC e o Projeto Sementeiras têm feito é muito isso, é a valorização. A gente não está indo atrás dos meninos para puni-los ou julgá-los, mas sim para auto afirmar que as meninas podem fazer com o corpo delas o que elas quiserem. Se querem se expor, beleza, mas isso possui um preço, mas é de direito. Mas isso não deve ser colocado como punição ou como "quebrei as regras da sociedade".

Apesar de a maioria das vítimas serem mulheres, a pornografia de revanche atinge todos os sexos, e cabe primoldialmente ao poder público reconhecer e combater essa atitude por todos os meios que estão ao seu alcance, no âmbito dos poderes executivo, judiciário e legislativo, de forma que as ações feitas pela sociedade civil organizada sirvam como um complemento à atuação estatal.

3.3 HERANÇA DIGITAL

Com a virtualização da vida humana é comum que as pessoas armazenem seus dados em arquivos digitais, como *e-mails*, *drives,* redes sociais e aplicativos, muitos destes dados possuem valor econômico e afetivo inclusive, surge então a questão sobre quem teria direito e se teria direito à suceder esses bens digitais deixados pelo falecido.

Para Ribeiro (2016, p. 32) “a herança digital é o conteúdo imaterial, incorpóreo, intangível, sobre o qual o falecido possuía titularidade, formado pelos bens digitais com valoração econômica e sem valoração econômica”.

Barreto e Nery Neto [2016, p. 3] explicam que os ativos digitais podem incluir:

> [...] contas de email, conteúdos de redes sociais, arquivos de música e de livros adquiridos em lojas de aplicativos online, áudios, vídeos, sons e imagens, nomes de usuário e suas respectivas senhas, arquivos armazenados em nuvens ou conteúdo armazenado em qualquer dispositivo informático.

Entrando na questão sobre a possibilidade da sucessão dos ativos digitais, dada a omissão legislativa brasileira, os doutrinadores têm feito diferenciação entre bens com valor econômico e bens sem valor econômico, sendo os primeiros passíveis de sucessão e os segundos não, explica-se:

Segundo Gagliano e Pamplona Filho (2016, p. 331) o patrimônio jurídico de uma pessoa engloba “o complexo de direitos reais e obrigacionais, [...] ficando de lado todos os outros que não têm valor pecuniário”, como os direitos de família e direitos puros de personalidade, denominados direitos extrapatrimoniais.

Quanto aos bens digitais que têm valor pecuniário, afirmam Viegas e Silveira (2018) que eles são passíveis de sucessão, exatamente por serem compatíveis com o conceito de patrimônio jurídico.

Ocorre que algumas empresas ainda se negam a transferir o patrimônio adquirido online, Barreto e Nery Neto [2016, p. 3-4] citam o exemplo da *Amazon*

através do aplicativo *Kindle,* mesmo o cliente comprando o livro online, a empresa alega que isso é apenas uma licença de utilização, e veda expressamente em seus termos de uso “vender, alugar, arrendar, distribuir, sublicenciar ou transferir quaisquer direitos ao Conteúdo Kindle ou qualquer parte dele a terceiros [...]” (TERMOS…, 2020); vale mencionar que o Google *Play* contém uma restrição quase idêntica a do *Kindle* em seus termos de uso, afirmando que “não é permitido: vender, fazer empréstimos, fazer leasing, redistribuir, transmitir, comunicar, modificar, sublicenciar, transferir nem atribuir um Conteúdo a terceiro, inclusive com relação aos downloads de Conteúdo [...]” (GOOGLE PLAY, 2020), o Google *Play* ainda é mais abrangente do que o *Kindle,* comercializando livros, revistas, filmes, músicas, jogos e “outros conteúdos ou serviços digitais”.

Apesar da negativa de algumas empresas em transferir o patrimônio adquirido pelo *de cujus,* Barreto e Nery Neto [2016, p. 7-8] afirmam que não podem os termos de uso se sobreporem a um direito fundamental à herança, lembram que a relação entre os usuários e essas empresas é consumerista e ressaltam a aplicação do art. 51 do Código de Defesa do Consumidor, que trata da proteção do consumidor contra cláusulas abusivas, principalmente aquelas que impliquem renúncia ou disposição de direitos.

No que diz respeito aos bens digitais sem valor econômico, surge um impasse na doutrina, isso porque, por não terem valoração econômica não se encaixam no conceito de patrimônio jurídico e não farão parte da herança em tese, mas, ainda assim possuem valor emocional para os familiares, surge então um conflito entre o direito à herança e o direito à privacidade do falecido.

Primeiramente, cabe esclarecer que os bens digitais com ou sem valor econômico podem ser deixados em testamento ou codicilo se for o caso (TARTUCE, 2018), o Código Civil (CC) admite inclusive disposição testamentária de conteúdo exclusivamente extrapatrimonial, dispõe o art. 1857, §2º do CC: “são válidas as disposições testamentárias de caráter não patrimonial, ainda que o testador somente a elas se tenha limitado” (BRASIL, 2002).

Quando o titular de um bem digital sem valoração econômica falece e não deixa nenhuma manifestação de última vontade apta a transferir o bem, a questão que está sendo levantada é a de que esses bens são intransferíveis, porque fazem parte dos direitos de personalidade do falecido, com grande ênfase no direito à privacidade.

Fraga (2019) explica que o acesso irrestrito dos herdeiros às contas privadas do falecido, além de atingir o direito do próprio *de cujus,* com a leitura de mensagens privadas e até fotos enviadas e recebidas por ele, atingiria também a privacidade de terceiros que trocaram mensagens ou outros conteúdos com o falecido, conteúdos estes que foram trocados de forma privada com o titular da conta, não sendo correto que seus herdeiros tenham acesso a essas informações de cunho pessoal.

Na mesma linha de raciocínio, Mendonça (2020) cita um decisão em processo judicial na cidade de Pompeu/Minas Gerais, no processo era autora a mãe da falecida e a ré era a empresa *Apple,* a autora buscava acesso à conta virtual da *de cujus,* em sua decisão, o juiz Manoel Jorge de Matos Junior julgou improcedente o pedido, fundamentado no direito à privacidade da falecida, vejamos um trecho da sentença:

> [...] Dada essa digressão, tenho que o pedido da autora não é legítimo, pois a intimidade de outrem, inclusive da falecida Helena, não pode ser invadida para satisfação pessoal. A falecida não está mais entre nós para manifestar sua opinião, motivo pela qual a sua intimidade deve ser preservada [...]. (MENDONÇA. 2020).

Diante do conflito entre o direito à herança e o direito à privacidade, Magalhães (2019) conclui que o último deve prevalecer, pois abrange os sentimentos pessoais do ser humano que vão além de questões patrimoniais, além do mais, o acesso aos dados do falecido pode causar diversos transtornos, inclusive descobertas que mudem completamente a memória da família sobre o *de cujus.*

Com o desenvolvimento da ideia de herança digital, alguns provedores de aplicação começaram a oferecer funcionalidades aos seus usuários no sentido de deixarem uma manifestação de última vontade digital, em alguns casos a pessoa pode inclusive nomear um herdeiro, cita-se como exemplo o *Facebook* e o Google.

No servidor *Facebook* são colocadas à disposição do usuário as seguintes funcionalidades: a) o usuário pode deixar registrado em sua conta a intenção de exclusão permanente desta após o seu falecimento, desta forma assim que o *Facebook* for notificado do falecimento, todas as mensagens, fotos, publicações, comentários, reações e informações do usuário serão permanentemente removidos (FACEBOOK, [2020a]); b) transformar a conta em memorial: se o usuário não tiver expressamente optado pela exclusão da conta, familiares e amigos podem preencher um formulário para transformar a conta do falecido em um memorial, desta forma a conta permanecerá ativida no *Facebook* e será administrada pelo contato herdeiro escolhido pelo *de cujus,* ou se ele não tiver escolhido um contato herdeiro, a conta não será administrada por ninguém (FACEBOOK, [2020c]); c) escolher um contato herdeiro: o usuário que tiver 18 anos ou mais pode nomear um contato herdeiro que gerenciará (em certos limites) a conta do falecido transformada em memorial, o contato herdeiro pode, entre outras coisas, escrever uma publicação no perfil, decidir quem pode ver e publicar homenagens, excluir homenagens publicadas, atualizar a foto de perfil e solicitar a exclusão da conta, o contato herdeiro não pode entrar na conta do falecido, ler suas mensagens e excluir amigos ou fazer novas solicitações de amizade (FACEBOOK, [2020b])

Seguindo a linha do *Facebook,* a empresa Google também tem uma funcionalidade semelhante, possibilitando que seus usuários deixem uma disposição de última vontade no caso de a conta se tornar inativa, o usuário pode: a) escolher excluir a conta permanentemente, neste caso todos os produtos associados a conta também serão excluídos, como *Drive* e *Gmail; e* b) nomear um contato de segurança e conceder (ou não) a ele acesso aos seus dados, o usuário pode inclusive escolher quais dados pretende compartilhar, por exemplo compartilhar o canal no *Youtube* mas não a conta de *Gmail* (GOOGLE, [2020]).

Embora essas manifestações de última vontade pareçam um testamento, não existe previsão de Código Civil/2002 de um testamento feito por meio de provedores de aplicação, na lei brasileira, a espécie de testamento que mais se aproxima dessas disposições de última vontade é o testamento particular, que mesmo assim ainda tem sua validade condicionada a alguns requisitos, como ser lido e assinado pelo testador na presença de pelo menos 3 testemunhas, que o devem subscrever (BRASIL, 2002).

Quanto à atuação legislativa brasileira, existiram dois Projetos de Lei que versavam sobre o assunto, ocorre que atualmente ambos se encontram arquivados, eram eles: PL nº 4.099/2012 e PL nº 4.847/2012.

O PL nº 4.099/2012 propunha acrescentar um parágrafo único ao artigo 1.788 do Código Civil.

O art. 1.788 determina que “morrendo a pessoa sem testamento, transmite a herança aos herdeiros legítimos; o mesmo ocorrerá quanto aos bens que não forem compreendidos no testamento; e subsiste a sucessão legítima se o testamento caducar, ou for julgado nulo” (BRASIL, 2002), a PL nº 4.099/2012 acrescentaria um parágrafo único, dispondo: “serão transmitidos aos herdeiros todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança” (BRASIL, 2012a).

Percebe-se que referido Projeto de Lei não fazia diferenciação entre bens com valor econômico e bens sem valor econômico.

A proposta também sugeria que se o falecido não tivesse deixado um testamento, a herança digital iria para os herdeiros legítimos, o que vai de encontro com as disposições do *Facebook* e *Google* que permitem que o contato herdeiro ou contato de segurança seja qualquer pessoa escolhida pelo *de cujus,* lembrando que as manifestações de vontade configuradas nestas plataformas não se encaixam nos requisitos exigidos para a validade de um testamento.

Conforme consta na movimentação do PL no Senado Federal, ele foi arquivado em 2018 sob o número 75/2013, porque se encontrava em tramitação há mais de duas legislaturas, com fundamento no artigo 332, §1º do Regimento Interno do Senado Federal (BRASIL, [2018]).

Já o PL nº 4.847/2012 era mais abrangente, sugerindo a inclusão de um capítulo inteiro no Código Civil com 3 artigos, denominado: Da Herança Digital.

O artigo 1.797-A conceituava herança digital como o “conteúdo intangível do falecido, tudo que é possível acumular ou guardar em espaço virtual” (BRASIL, 2012b), novamente, este PL não faz diferenciação entre bens com valor econômico e bens sem valor econômico.

A proposta continuava (art. 1797-B), sugerindo que se o falecido, tendo capacidade para testar, não o tivesse feito, a herança digital seria transmitida para seus herdeiros legítimos (BRASIL, 2012b); aqui reitera-se o mesmo apontamento feito ao PL 4.099/2012, no sentido de o referido artigo ir contra as disposições das empresas *Facebook* e Google.

O último artigo (art. 1797-C) atribuía aos herdeiros o direito de definir o destino das contas do falecido, podendo transformar em memorial, apagar todos os dados do usuário ou remover a conta do antigo dono (BRASIL, 2012b).

O PL nº 4.847/2012 foi julgado prejudicado em 2013 pela Câmara dos Deputados e teve nova decisão de arquivamento em 2019, após reclamação do deputado Marçal Filho, autor do PL (BRASIL, 2012b).

Pela análise dos referidos Projetos de Lei, percebe-se que a legislação brasileira não seria suficiente para elucidar as principais questões envolvendo herança digital, seja com relação a quais bens digitais integram a herança, seja pela prevalência ou não das manifestações de última vontade deixadas pelo falecido nos próprios provedores de aplicação.

Infelizmente, ambos os PL’s foram arquivados sem ao menos serem suficientemente debatidos, mas, tendo em vista a constante evolução da sociedade, principalmente no meio virtual, tem-se como certo o surgimento de mais questões envolvendo a matéria, e talvez, um novo projeto sobre o assunto.

4 A POSIÇÃO DO PODER JUDICIÁRIO EM CASOS ENVOLVENDO DIREITO DIGITAL

É ao Poder Judiciário que os cidadãos se socorrem quando a *lide* já está formada, e cabe a ele, existindo lei ou não, solucionar o caso concreto, na área digital poucas leis foram criadas, na verdade, a maioria ainda se encontra em tramitação, isso faz com que os julgadores tenham que decidir com base em princípios e analogia com as leis já existentes, mas ainda ajustados ao mundo virtual.

Sendo assim, sem legislação específica, a posição do Poder Judiciário ainda é imprevisível para cada caso concreto, porém deverá refletir os ditames da Constituição Federal e os princípios que norteiam o direito brasileiro.

4.1 CONSEQUÊNCIAS JURÍDICAS DE CURTIR ALGO NAS REDES SOCIAIS

A evolução digital introduziu diversas vantagens para a humanidade, uma delas é a facilidade da interação humana e da manifestação do pensamento, que pode ser feito de forma bem clara como uma publicação postada em um site, mas também pode ser feita de forma mais sutil e menos evidente, como curtidas em postagens online, a questão a ser respondida é se o mero ato de curtir algo nas mídias sociais é o suficiente para causar consequências jurídicas.

Começando a análise com um caso que aconteceu no estado da Paraíba, e que foi julgado pelo Tribunal de Justiça do estado em 2017; no caso, a magistrada Aylzia Fabiana Borges Carrilho publicou em seu perfil do *Facebook* uma matéria sobre um ilícito penal divulgada em um site de notícias, após isso seus seguidores começaram a comentar na postagem, proferindo palavras de ofensa ao autor do delito (PARAÍBA, 2017), tais como:

> o agente trabalhando cumprindo a rotina do dia, ai vem um filhinho de papai, um irresponsável, um louco, um animal tirar uma vida de um ser humano deixando três filhos. Era Coordenador da Lei Seca do Estado da Paraíba. O mais revoltante nisso é que ficará impune..."(PARAÍBA, 2017).

A magistrada então curtiu os comentários feitos por seus seguidores na época, ocorre que após o ocorrido ela foi designada como juíza competente para julgamento

do infrator em questão, no 1º Tribunal do Júri da Comarca da Capital (PARAÍBA, 2017).

A defesa do Réu alegou que a magistrada manifestou um claro posicionamento parcial diante da causa ao curtir comentários que eram ofensivos ao infrator, ressaltou também que a juíza não curtiu todos os comentários, ou seja, não era um mero ato de cordialidade com seus amigos e seguidores, e sim uma exposição de juízo de valor sobre o ocorrido (PARAÍBA, 2017).

Em sua defesa, a magistrada alegou, entre outras coisas, que “no que diz respeito a “curtidas” de comentários de terceiros, entendo que é uma forma cordial de se relacionar nas redes sociais e, ao mesmo tempo, sem emitir qualquer opinião sobre o comentário feito” (PARAÍBA, 2017).

A decisão do Tribunal de Justiça do Estado da Paraíba foi no sentido de não reconhecer a parcialidade da julgadora, sob a fundamentação de que simples interações nas redes sociais não têm o condão de interferir na parcialidade da magistrada, bem como os comentários feitos na postagem não foram tecidos pela juíza, e que uma mera curtida nesses comentários não significa, necessariamente, que ela concordaria com o que foi dito (PARAÍBA, 2017).

Enquanto o Tribunal de Justiça da Paraíba considera curtidas em postagens uma mera cordialidade entre amigos, e não, necessariamente uma concordância, o Tribunal Regional do Trabalho da 15ª Região tem decidido em sentido oposto, como percebe-se em sua jurisprudência, vejamos:

Em 2018, o sindicato trabalhista SindSaúde de Bauru/São Paulo publicou em sua página de *Facebook* um comunicado informando que seria realizada uma assembléia com a empresa FAMESP para discussão de questões trabalhistas, após isso um dos funcionários da empresa comentou: “Agora é a hora de unirmos nossas forças pessoal.... Vamos mostrar ora VAMERDA q UNIDOS somos mais FORTES.... # PARTIU PRA CIMA!", fazendo um trocadilho com a sigla que representa a empresa, substituindo FAMESP por VAMERDA, comentário este que foi curtido por outra funcionária da empresa (SÃO PAULO, 2019).

A empresa FAMESP por sua vez demitiu ambos os funcionários, tanto aquele que comentou quanto aquela que curtiu, sob o fundamento do artigo 482, alínea k, da Consolidação das Leis do Trabalho (SÃO PAULO, 2019), que assim dispõem:

> Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
>
> (...)
>
> k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem; (BRASIL, 1943).

Interessante notar que os dois funcionários tiveram sentenças diferentes em primeiro grau, primeiramente a funcionária que curtiu o comentário teve sua demissão por justa causa confirmada em primeiro grau, para o magistrado que proferiu a decisão, ficou clara a concordância da ex-trabalhadora com o comentário publicado por seu colega, concordância que está representada na prática de curtir publicamente uma ofensa explícita ao empregador (SÃO PAULO, 2019).

Ocorre que no caso do funcionário autor do comentário, sua demissão por justa causa não foi reconhecida pelo juiz de primeiro grau, que entendeu que, apesar de o autor ter agido com desrespeito e falta de polidez, sua atitude não configurava algo tão grave a ponto de ferir a reputação da empresa (SÃO PAULO, 2019).

Neste último caso, a empresa FAMESP recorreu da decisão para o Tribunal Regional do Trabalho da 15ª Região, que reformou a sentença de primeiro grau, reconhecendo a justa causa na demissão do funcionário, inclusive ressaltando no acórdão o fato de sua colega de trabalho ter sido demitida pela simples curtida ao comentário (SÃO PAULO, 2019), o que demonstra a opinião rígida deste Tribunal em relação às manifestações em rede social.

O terceiro e último caso ocorreu na cidade Criciúma/Santa Catarina, e traz uma hipótese de responsabilidade civil por dano moral; em 2018 um dos sócios da empresa Criciúma Construções processou algumas pessoas que comentaram e curtiram uma publicação desrespeitosa sobre ele nas redes sociais (SANTA CATARINA, 2018).

O processo correu em Juizado Especial Cível, e o julgamento do juiz de primeiro grau foi tão pontual e minucioso sobre a questão, que os julgadores da Quarta Câmara Recursal de Criciúma/SC decidiram manter a sentença por seus próprios fundamentos (SANTA CATARINA, 2018).

Começou o magistrado explicando que os sócios da empresa Criciúma Construções não estavam isentos de responsabilidade com a sociedade, isso porque a empresa estava em um estado de depreciação financeira, supostamente por culpa de seus gestores, sendo assim, não conseguiu entregar imóveis previamente adquiridos por seus clientes, tal estado da pessoa jurídica culminou, inclusive, na prisão de algumas pessoas, entre elas o autor do processo ora descrito (SANTA CATARINA, 2018).

Apesar do juiz ter reservado alguns parágrafos de sua decisão para falar sobre a liberdade de expressão e de sua importância para a sociedade democrática, não foi por esse motivo que julgou improcedente os pedidos, mas sim pelo direito de concordar ou não com uma opinião, que não se confunde com o ato de manifestar pensamento (SANTA CATARINA, 2018).

A opinião do magistrado da causa pode ser bem explicada pelo o que José Afonso da Silva (2016, p. 243) chama de liberdade de opinião, que abrange tanto o pensamento íntimo quanto a sua manifestação, o indivíduo tem o direito de acreditar em algo em seu íntimo, proferindo juízo de valor ou não.

A liberdade de consciência ainda é assegurada pela Constituição Federal em seu artigo 5º, inciso IV, que assim dispõe: “é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias” (BRASIL, 1988).

Continuando com a análise do último processo, o julgador continua sua decisão dizendo que apenas em países totalitários uma pessoa pode ser punida por simplesmente concordar ou discordar com uma ideia; e termina sua explanação dizendo que uma curtida em rede social não necessariamente significa concordância,

pode ter outros significados, como ironia por exemplo, e que, a menos que se possa ler a mente do usuário, não é possível identificar quais foram as suas intenções quando curtiu uma postagem ou comentário (SANTA CATARINA, 2018).

Fica claro que ainda não se tem uma concordância entre os órgão do poder judiciário sobre o assunto, mas, é importante salientar que os três processos mencionados tratam (propositadamente) de assuntos distintos, o primeiro é uma análise de suspeição de uma juíza, onde se aplicam os dispositivos específicos da Lei Complementar nº 35 de 1979 (LOMAN), além daquelas previstas nos Códigos de Processo Civil ou Penal, ou seja, não se destina a saber se a magistrada feriu ou não a honra e a moral do indivíduo, mas sim se sua ação de curtir uma postagem tem o condão de provar sua parcialidade na causa, impedindo sua atuação.

Para o segundo, é aplicado um dispositivo da CLT que exige a prática, pelo empregado, de ato lesivo à honra ou boa fama do empregador, repare-se que aqui nem se menciona em dano moral, basta apenas um ato que atinja a honra ou a boa fama da empresa (ou empregador pessoa física).

Para o terceiro, é aplicado o direito civil (Código Civil), trata-se de reparação por danos morais, que é mais complexo e exige um abalo anímico, mais do que um simples ato de desapreço por exemplo.

Por fim, percebe-se que curtidas em redes sociais é uma forma de interação humana muito sutil, que pode ter diferentes significados em diferentes contextos, bem como pode se encaixar em certa conduta descrita em uma lei e não se encaixar em outra conduta descrita em outro diploma legal, as consequências jurídicas dessa relação digital ainda não é entendimento pacífico entre os órgãos do poder judiciário, o que possivelmente pode resultar no reconhecimento de repercussão geral sobre o assunto, deixando essa decisão nas mãos dos tribunais superiores.

4.2 O DEVER DE AUXÍLIO AO JUDICIÁRIO E A QUESTÃO DA CRIPTOGRAFIA

Muitos são os dispositivos no ordenamento jurídico brasileiro que reiteram a obrigação das pessoas de cooperar com o poder judiciário, pode-se citar o artigo 139 do CPC/2015 que permite ao juiz "determinar todas as medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento da ordem judicial" (BRASIL, 2015), bem como o dever de cooperação imposto pelo art. 6º do CPC/2015: “ todos os sujeitos do processo devem cooperar entre si para que se obtenha, em tempo razoável, decisão de mérito justa e efetiva” (BRASIL, 2015); e ainda, o crime de desobediência previsto no artigo 330 do Código Penal (CP) que tipifica o ato de "desobedecer a ordem legal de funcionário público", punindo com detenção, de quinze dias a seis meses, e multa (BRASIL, 1940).

Entretanto, algumas grandes empresas ainda insistem na impossibilidade de cooperação com certas ordens judiciais, como o *Whatsapp* e a *Apple.*

Começando por um dos aplicativos mais populares do Brasil: o *Whatsapp,* ao todo o *Whatsapp* já foi suspenso três vezes por ordem de juízes brasileiros, cita-se a ordem de bloqueio expedida pela 1ª Vara Criminal da Comarca de São Bernardo do Campo/SP em 2015, em decorrência do não cumprimento da ordem de interceptação de conversas no aplicativo; o bloqueio expedido pelo Juízo da Comarca de Lagarto/SE em 2015, por falta de entrega de informações requeridas; e por fim, o bloqueio feito a mando do Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ em 2016, também por não cumprimento da ordem de interceptação de mensagens no *App* (GOMES, S., 2020).

Tomaremos como exemplo a ordem expedida pelo Juízo da Comarca de Lagarto/SE, no caso, a intimação que foi dirigida ao *Facebook* Brasil Ltda (empresa dona do *Whatsapp*), que mais tarde alegou sua ilegitimidade passiva (SERGIPE, 2016), continha a seguinte ordem:

> [...] implementar interceptação do aplicativo WHATSAPP e fornecer o acesso irrestrito às conversas de texto, fotografias, vídeos, conversas de voz, agenda de contatos, bem como ao conteúdo dos grupos ao quais os envolvidos estavam adicionados, dos alvos/terminais que foram relacionados, bem como fornecesse, via e-mail, conversas de texto, fotografias, vídeos, conversas de

> voz e agenda de contatos, ficando estipulada multa de R$ 50.000,00 diários [...] (SERGIPE, 2016).

Após a empresa requerida não ter cumprido com a decisão, o Juízo de Lagarto determinou a suspensão do aplicativo *Whatsapp* por 72 horas (SERGIPE, 2016), além da suspensão do *App,* o descumprimento da decisão também resultou na prisão preventiva do vice-presidente do Facebook na América Latina, Diego Jorge Dzodan, sob o fundamento no artigo 2º, §1º da Lei nº 12.850/2013 (RODAS, 2016), que dispõe:

> Art. 2º Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa:
>
> Pena - reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas.
>
> **§ 1º Nas mesmas penas incorre quem impede ou, de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa** (grifo nosso) (BRASIL, 2013).

Sobre a prisão do vice-presidente, ela foi revogado pelo TJ/SE no mesmo dia, mas sobre a decisão de bloqueio do aplicativo em questão, a empresa Whatsapp Inc. impetrou mandado de segurança para o Tribunal de Justiça do Sergipe onde alegou, entre outras coisas, a desproporcionalidade na decisão e a impossibilidade de interceptação de mensagens criptografadas no aplicativo, bem como a violação ao Marco Civil da Internet, uma vez que a referida lei apenas permite a suspensão das atividades no caso de violação de dados dos usuários e que a interrupção dos serviços de internet é vedada por seu artigo 7º e 9º (SERGIPE, 2016).

Vejamos o teor dos artigos que tratam sobre suspensão das atividades citados pela *Whatsapp inc.*:

> Art. 11. 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.
>
> (...)
>
> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam

> sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:T
>
> (...)
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11 (BRASIL, 2014).

Em decisão não unânime, o TJ/SE decidiu que a principal questão envolvendo o caso não era a possibilidade da suspensão do aplicativo, porque, segundo o acordão, a LMCI permite tal medida, porém o verdadeiro empecilho é o choque de direitos fundamentais sigilo/bem comum/acesso à informação, isso porque a suspensão do aplicativo gerou um verdadeiro caos social, pela dificuldade dos usuários de realizarem atividades laborativas, de lazer, familiares etc, a comoção foi tanta que levou o grupo de *hackers Anonymous* a tornar indisponível o site do Tribunal de Justiça de Sergipe em forma de protesto (SERGIPE, 2016).

Sobre o ataque *hacker,* o grupo *Anonymous* publicou, à época, uma justificativa em sua conta do *Facebook,* segundo o grupo já era de conhecimento das autoridades que o *Whatsapp* utiliza a tecnologia criptografia de ponta-a-ponta, e que por isso mesmo é impossível entregar informações dessas conversas, sendo claro que a medida foi tomada a fim de restringir a liberdade e privacidade proporcionada pelos meios de comunicação, terminaram seu comunicado dizendo: “Se o WhatsApp ficará bloqueado por 72h, assim será também então com o site do Tribunal de Justiça de Sergipe, em forma de protesto pelos motivos expostos. Não nos calarão” (ANONYMOUS BRASIL, 2016).

Outro motivo citado na decisão do TJ/SE, é o fato de que não ficou claro se a empresa *Whatsapp* poderia ou não fornecer informações de conversas criptografadas, talvez por um processo de descriptografia, sugeriu a decisão, mas os próprios julgadores admitiram que, naquele momento, não tinham condições de afirmarem isso (SERGIPE, 2016).

Em decorrência das reiteradas tentativas do judiciário brasileiro em suspender o aplicativo *Whatsapp,* o Partido Popular Socialista (PPS) impetrou a Ação de Descumprimento de Preceito Fundamental nº 403 perante o Supremo Tribunal Federal (STF), na fundamentação da petição inicial, o partido político citou os casos do bloqueio ocorrido em São Bernardo do Campo/SP, o bloqueio feito a mando do

Juízo de Lagarto/SE, a tentativa de bloqueio pelo Juízo de Teresina/PI, bem como a prisão do vice-presidente do *Facebook* da América Latina, sustentou que o aplicativo no Brasil deixou de ser mera diversão, sendo um dos mais usados no país para comunicação, e que a sua suspensão de maneira arbitrária atingiria o direito fundamental da liberdade de expressão (BRASIL, [2020]).

A votação da ADPF se encontra suspensa após pedido de vista feito pelo Ministro Alexandre de Moraes em 28/05/2020, porém, o relator Ministro Edson Fachin já teve a oportunidade de proferir seu voto; na opinião do relator o pedido formulado na ação é procedente para declarar a inconstitucionalidade parcial do inciso II do artigo 7º e inciso III do artigo 12 da Lei nº 12.965/2014, de forma a "afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet", a Ministra Rosa Weber acompanhou o voto do relator (BRASIL, [2020]).

Mas as autoridades brasileiras não são as únicas com problemas com a tecnologia de criptografia, apenas a título de exemplo, vale citar a questão envolvendo a empresa *Apple* e a justiça estadunidense; em 2016 um atirador deixou 14 pessoas mortas na cidade de San Bernardino/EUA após um ataque terrorista, assim, o Departamento Federal de Investigação dos Estados Unidos - FBI (sigla em inglês) precisava ter acesso às informações que estavam no *Iphone* do atirador, porém foram impedidos pela forte tecnologia de segurança do aparelho (KHARPAL, 2016, tradução nossa).

Após a empresa *Apple* se negar a ajudar nas investigações, o caso foi parar nas mãos do poder judiciário do país, que determinou que a *Apple* deveria fornecer uma assistência razoável ao FBI (KHARPAL, 2016, tradução nossa), segundo Rodrigues (2017), os pedidos do Departamento eram:

> [...] desativar a função opcional de apagamento automático dos dados das pessoas após dez tentativas falhas de inserção de senha no dispositivo existente na versão 9 do sistema operacional do Iphone (IOS); permitir que o FBI tentasse senhas eletronicamente e não apenas manualmente, remover a função de atraso do dispositivo que

> previne o usuário de tentar inserir sua senha por períodos de tempo cada vez maiores a cada tentativa incorreta.

Em outras palavras, o que o FBI estava requisitando era o desenvolvimento de um *Software* que driblasse o sistema de segurança do *Iphone.*

Em 25/02/2016 a empresa *Apple* apresentou suas justificativas à Corte Distrital dos Estados Unidos, Distrito Central da Califórnia, alegando, entre outras coisas, que o que o FBI estava requisitando da empresa era um verdadeiro *Backdoor*[2]*,* que eles acreditam que desenvolver esse tipo de *Software* abriria diversas oportunidades de ataques ao sistema IOS, como permitir que as senhas sejam colocadas eletronicamente iria possibilitar que o *Iphone* fosse invadido por "força bruta", testando centenas de milhões de senhas em questão de segundos, enfraquecendo a criptografia do *Iphone* (ESTADOS UNIDOS DA AMÉRICA, 2016, tradução nossa).

Ainda em suas justificativas, a empresa alegou que vez criado, o *Software* nunca mais pararia de ser requisitado pela justiça americana em todos os tipos de casos, sendo apenas uma questão de tempo até cair nas mãos de países estrangeiros e *hackers:*

> O governo diz: "só dessa vez" e "só esse telefone", mas o governo sabe que essas alegações não são verdadeiras. De fato o governo já fez outras petições para ordens similares, algumas que estão pendentes em outras cortes. [...] Se essa ordem for permitida de permanecer, será apenas uma questão de dias até que algum outro procurador, em algum outro caso importante, perante algum outro juiz, busque uma ordem similar usando esse caso como precedente. [...] Uma vez que as comportas estiverem abertas, elas não poderão ser fechadas, e o dispositivo de segurança que a Apple trabalhou tão incansavelmente para alcançar será desfeito sem mesmo uma votação no congresso (ESTADOS UNIDOS DA AMÉRICA, 2016, tradução nossa).

No final, o FBI conseguiu de fato acessar o *Iphone,* mas não com a ajuda da *Apple,* e sim com o auxílio de alguém que eles chamaram de "terceira parte"

---

[2] Segundo Rodrigues (2017) *backdoor* poder ser conceituado como "uma vulnerabilidade (frequentemente colocada intencionalmente) em um sistema que possibilita a um atacante contornar os mecanismos de autenticação convencionais para obter acesso não-autorizado a dados desse sistema.

(KHARPAL, 2016, tradução nossa), até agora, não há notícias de que a empresa *Apple* tenha cedido às requisições judiciais e criado um *Backdoor* para o sistema IOS.

Voltando ao poder judiciário brasileiro, na ADPF nº 403, o relator Ministro Edson Fachin já deixou claro que não pretende entrar no mérito da possibilidade técnica ou não da interceptação de mensagens criptografadas, aliás, pelo voto do próprio relator e também da Ministra Rosa Weber, percebe-se que a votação será no sentido de decidir pela inconstitucional ou não desse tipo de requisição (BRASIL, [2020]).

O caso da *Apple* e a justiça americana é semelhante ao caso do *Whatsapp* no Brasil, as discussões sobre o assunto são recentes, e o judiciário nacional terá a grande tarefa de resolver esse conflito entre direitos fundamentais, isso se não for melhor, como a própria *Apple* sugeriu, uma votação no poder legislativo.

4.3 O DIREITO AO ESQUECIMENTO NA INTERNET

A internet é um meio de comunicação onde as pessoas podem publicar coisas sobre a própria vida e também sobre a vida alheia, de uma forma ou de outra, o conteúdo publicado na rede tem o potencial de ser permanente, depende de quem o propaga e também do interesse do público, o que pode ser devastador para a pessoa de quem se fala, principalmente se o assunto envolve a vida privada ou o cometimento de crimes, nas palavras de Rosen (2010, tradução nossa) “como viver bem as nossas vidas em um mundo onde a internet grava tudo e não esquece de nada?”.

Segundo Ortega (2015) O direito ao esquecimento é o direito que uma pessoa possui de não permitir que um fato, ainda que verídico, ocorrido em determinado momento de sua vida, seja exposto ao público em geral, causando-lhe sofrimento ou transtornos.

Como veremos a seguir, o direito ao esquecimento é reconhecido e aplicado pelo poder judiciário nacional, cita-se o teor do enunciado 531 da VI Jornada de Direito Civil: “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento” (CONSELHO DA JUSTIÇA FEDERAL, 2013).

O primeiro caso é um Agravo Interno em Recurso Especial, onde é agravante a empresa Google Brasil Internet Ltda, e agravada uma pessoa física, que teve o nome resguardado; originalmente, a pessoa propôs uma ação contra a empresa Google para retirar/bloquear qualquer pesquisa relacionada ao seu nome, isso porque as pesquisas poderiam levar à páginas com fotos de nudez suas, o acórdão do TJ/SP decidiu pela possibilidade dos pedidos, com fundamento no direito ao esquecimento, indicando que não existiria interesse público nas fotos, relacionando-se apenas com a vida privada da pessoa (BRASIL, 2016).

Em suas fundamentações, a empresa Google alegou a impossibilidade de bloquear as palavras-chaves indicadas pela pessoa, porque o Marco Civil da Internet exige a indicação clara do conteúdo infringente para sua localização (BRASIL, 2016).

Em sua decisão, a terceira turma do Superior Tribunal de Justiça começou explicando que o artigo 7º da LMCI trata parcialmente sobre o direito ao esquecimento na internet, mas que esse artigo não seria aplicável aos sites buscadores em regra, e, principalmente, naquele caso concreto (BRASIL, 2016), vejamos o artigo citado pelos julgadores:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> (...)
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (BRASIL, 2014).

Primeiramente, a decisão explicou que os dados da requerente não estavam armazenados no Google, e sim em sites de terceiros, e o Google, sendo um provedor de pesquisa, não hospeda, organizada ou gerência de nenhuma forma as páginas que aparecem em sua busca (BRASIL, 2016).

A terceira turma do STJ também decidiu que os provedores de pesquisa devem ser responsabilizados apenas pelas atividades desenvolvidas por eles, e não existe obrigação legal, nem na LMCI nem no Código de Defesa do Consumidor, que imponha

a esses provedores o dever de filtrar ou eliminar algum termo ou expressão de sua busca, em suma, não cabe ao Google garantir o direito ao esquecimento da vítima (BRASIL, 2016).

Essa decisão do STJ criou um precedente muito importante para o poder judiciário nacional, inclusive impactando um processo antigo de uma das personalidades mais famosas na mídia brasileira: a apresentadora Xuxa Meneghel; em 2010 a apresentadora propôs uma ação judicial contra a empresa Google, requerendo que a empresa se abstivesse de apresentar qualquer resultado para a pesquisa do termo “Xuxa pedófila”, bem como deixasse de disponibilizar qualquer imagem da autora nua (MARTINES, 2017).

O processo correu no estado do Rio de Janeiro e teve seus pedidos julgados improcedentes pelo juiz de primeiro grau, fundamentado, inclusive, nos precedentes firmados pelo STJ; a autora recorreu ao Tribunal de Justiça/RJ, alegando cerceamento de defesa e também citando o julgamento ocorrido no Tribunal de Justiça da União Europeia em 2014, que condenou o Google a fazer a filtragem de termos (RIO DE JANEIRO, 2017).

Inclusive, neste processo foi feita uma prova pericial digital a fim de comprovar se o Google tinha ou não possibilidade técnica para realizar essa filtragem, o *expert* concluiu que:

> [...] é possível à Ré buscar e encontrar expressões, palavras chaves, imagens e páginas web específicas, identificadas individualmente, que se referem a Autora, armazenadas no seu banco de dados, para que não sejam apresentadas aos seus usuários nos resultados das buscas (RIO DE JANEIRO, 2017).

Entretanto, a perícia feita se tornou quase irrelevante para o processo, isso porque o precedente do STJ não trata sobre a possibilidade ou não da filtragem, e sim sobre a falta de legislação específica para obrigar os provedores de pesquisa de fazerem uma filtragem genérica, o acórdão do TJ/RJ também menciona que é possível à autora indicar o URL específico da página que deseja não ser encontrada, mas não um bloqueio de forma genérica dos termos nas pesquisas, ainda, deixaram claro os desembargadores de que não se tratava de uma negação ao direito de esquecimento

da autora, mas sim do reconhecimento da desobrigação da empresa ré (RIO DE JANEIRO, 2017).

Apesar do TJ/RJ não ter se manifestado sobre o precedente internacional citado pela autora, o próprio STJ já tinha firmada entendimento sobre ele, no caso que foi julgado pelo Tribunal de Justiça Europeu em 2014, ficou decidido que o provedor de pesquisa é responsabilizável pelos dados pessoais dos usuários, e que pode ser obrigado a suprimir de sua pesquisa termos que violem o direito do usuário, mesmo quando a publicação no site de terceiros seja lícita (BRASIL, 2016).

Ocorre que a referida decisão estrangeira foi firmada em uma lei específica sobre proteção de danos pessoais, e, segundo o Superior Tribunal de Justiça, tal precedente não é aplicável ao Brasil, principalmente pela falta de legislação nacional específica de proteção de dados (BRASIL, 2016).

Apenas a título de informação, sem pretensão de fugir do tema deste capítulo, em 2018 foi criada a Lei nº 13.709 que dispõe sobre a proteção de dados pessoais, a lei não faz menção expressa ao direito ao esquecimento, mas garante a inviolabilidade da intimidade, da honra e da imagem, e determina em seus artigos 15 e 16 que uma vez que os dados deixem de ser necessários ou pertinentes ao alcance da finalidade almejada, eles devem ser eliminados (BRASIL, 2018a)

Quando se trata de direito ao esquecimento na internet, ele pode até ser reconhecido pelo judiciário e doutrina, mas o grande empecilho para exercê-lo ainda é a identificação das várias páginas digitais que disponibilizam o conteúdo, não sendo permitido tomar o caminho mais curto e simplesmente requisitar ao provedor de pesquisa.

Outro exemplo disto, são as jurisprudências disponibilizadas no site JusBrasil, cita-se dois exemplos julgados pelo Tribunal de Justiça do Rio Grande do Sul:

Em 2015 o TJ/RS julgou uma ação promovida por uma pessoa física contra o site JusBrasil, alegava a pessoa que foi ré em uma ação penal extinta pela prescrição, porém, mesmo após a extinção de seu processo, o site JusBrasil continuou divulgando

informações a respeito dele, inclusive o inteiro teor das decisões, o que teria lhe causado danos, e que as decisões não poderiam permanecer públicas "*ad eternum"* (RIO GRANDE DO SUL, 2015).

Em sua decisão, o referido tribunal mencionou que o JusBrasil é uma mera ferramenta de busca, sua função se restringe a localizar na web as páginas que contenham os termos pesquisados pelo usuário, e, por isso mesmo, não tem ingerência sobre o conteúdo disponibilizado no site de terceiros, fundamentaram nos precedentes do STJ (RIO GRANDE DO SUL, 2015).

Embora as decisões sobre o JusBrasil o definam como mero mecanismo de busca, a verdade é que ele é um facilitador para encontrar informações de terceiros, enquanto um advogado entra diretamente no site de um tribunal para fazer suas pesquisas, uma pessoa pode simplesmente digitar o nome de seu desafeto no Google e encontrar suas informações processuais no site JusBrasil, a diferença é que os processos constantes na base de dados dos sites governamentais não podem ser encontrados pela pesquisa no Google.

Em outro exemplo, também proveniente do TJ/RS, a autora da ação relatava que era possível encontrar informações privadas suas em um processo criminal em que foi vítima de roubo e estupro através de pesquisa pelo seu nome no site JusBrasil, o que não era possível através do mecanismo de busca oficial do tribunal competente (RIO GRANDE DO SUL, 2018).

No acórdão, o Tribunal de Justiça do Rio Grande do Sul caracterizou o JusBrasil como um facilitador de dados, possibilitando encontrar informações que na prática seriam impossíveis, lembraram os julgadores de que aquele caso não se tratava de retirada de informações do site, nem mesmo de censura ou de julgar ilícita a divulgação do conteúdo, mas sim, do reconhecimento do direito que o sujeito tem de poder questionar se os seus dados estão sendo utilizados de forma danosa, e requisitar que eles sejam removidos se for o caso (RIO GRANDE DO SUL, 2018).

No caso concreto, o Tribunal julgou, em sede de agravo de instrumento, que era possível a desvinculação do resultado da pesquisa pelo nome da vítima, informação que não era acessível pelas vias oficiais (RIO GRANDE DO SUL, 2018).

Por fim, percebe-se que o direito ao esquecimento é reconhecido no âmbito digital, entretanto, a complexidade da internet pode criar dificuldades na hora de exercê-lo, assim, cabe ao poder judiciário verificar qual a melhor saída para o caso concreto, seguindo a legislação brasileira mas também tendo em mente que não existe direito absoluto, e que às vezes é necessária uma mudança de entendimento e atuação para conseguir efetivar os direito na era digital.

5 CONCLUSÃO

Após todo o exposto pode-se concluir que o Direito Digital é um ramo muito complexo do Direito, que provavelmente será para a atuação de poucos, isso porque a necessidade de entender os termos técnicos vai afastar muitos advogados desta área, será necessário um bom conhecimento na área de informática e internet, caso contrário, o advogado não conseguirá diligenciar em processos envolvendo Direito Digital, o que vai impactar o processo, causando dano adicional ao cliente, lembrando que o juiz fica adstrito aos pedidos feitos pelas partes.

Para os juízes a necessidade de conhecimento de termos técnicos vai além, os juízes não podem escolher entre julgar ou não, eles são incumbidos do dever de julgar todo o litígio que for apresentado ao poder judiciário, e, por mais que o advogado dê o rumo do processo na maioria das vezes com requerimentos e diligências, é o julgador quem decidirá sobre os pedidos e dará a palavra final sobre a controvérsia, por isso um juiz sem conhecimento técnico tende a cometer erros gravíssimos no decorrer do processo, seja por ficar muito apegado à lei (que muitas vezes é incompatível com o meio digital), seja por confundir a forma como funcionam as coisas na internet (provedores, IP's, registros, hospedagem etc), proferindo assim, uma decisão ineficaz.

Enquanto os profissionais do Direito lutam para conseguir se adaptar aos dias contemporâneos, a sociedade (principalmente as gerações mais novas) não tem esse problema, as pessoas simplesmente usam os meios postos a sua disposição, seja para interação amigável, romântica ou até ilícita, compram bens digitais, expõe suas vidas e suas opiniões, causando consequências impensáveis, como a prática de pornografia de vingança e *fake news,* deixando nas mãos dos advogados e dos juízes o verdadeiro imbróglio que é a resolução destas questões.

Quanto ao poder legislativo, como representantes do povo os parlamentares estão sempre tentando positivar essas manifestações da sociedade, como é o caso da polêmica lei das *fake news* que tramita no congresso federal, aqui vale uma crítica a essa positivação, a mesma crítica que tanto foi dita nos parágrafos acima: falta de conhecimento técnico; a falta de conhecimento de como funciona a internet também

assombra os parlamentares, cita-se como exemplo os projetos de lei que tentaram estabelecer uma herança digital no Brasil, tais projetos se limitavam basicamente a dizer que os bens digitais iriam para os herdeiros legítimos, ignorando todas as manifestações de vontade que o falecido deixa nas próprias plataformas, ignorando a distinção entre bens com valoração econômica e bens sem valoração econômica, nem ao menos conceituando propriamente “bens digitais”, deixando mais uma vez essa tarefa a encargo do poder judiciário.

Percebe-se que a área de Direito Digital não é simples para nenhum operador do direito, mas, mesmo com as dificuldades apresentadas, a sociedade necessita urgentemente de profissionais que dominem o assunto, uma vez que a internet está se tornando parte indissociável da vida das pessoas, principalmente das gerações mais novas, e, é razoável pensar que em alguns anos, um profissional sem conhecimento técnico para atuar na área digital não terá um destaque no mercado de trabalho.

Por fim, é de se lamentar que existam poucos autores que estudam a fundo o Direito Digital e suas peculiaridades, merecem destaque neste trabalho Patrícia Peck. Fernando Brizola, Rennan Thamay, Maurício Tamer e Glaydson de Farias Lima, doutrinadores que se propuseram a estudar esse ramo complexo e controverso do Direito, e, esta pesquisadora almeja para o futuro um estudo mais aprofundado e menos superficial sobre este tópico, adentrando no mundo de verdadeiros *hackers* da internet, de forma a garantir a proteção da sociedade em todas as esferas de suas vidas.

REFERÊNCIAS

ANONYMOUS BRASIL. **Publicação.** *[S.l],* 02 de maio de 2016. Disponível em: https://www.facebook.com/AnonBRNews/photos/a.286106798104849/989794774402711/?type=3. Acesso em: 05 nov. 2020.

ARAUJO, Ester. **O que é um subdomínio e como criar o seu?.** *[S.l]*, 29 de junho de 2018. Disponível em: https://br.godaddy.com/blog/o-que-sao-subdominios-e-como-criar-o-seu/. Acesso em: 30 set. 2020.

AUGUSTO, Igor Antônio Michallene. **O que é a Teoria Tridimensional do Direito?.** *[S.l.]*, 1º de junho de 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-101/o-que-e-a-teoria-tridimensional-do-direito/. Acesso em: 04 set. 2020.

BARRETO, Alessandro Gonçalves; NERY NETO, José Anchiêta. **HERANÇA DIGITAL.** *[S.l.]*, [2016]. Disponível em: http://direitoeti.com.br/site/wp-content/uploads/2016/03/BARRETO-Alesandro-Gon%C3%A7alves-NERY-NETO-Jos%C3%A9-Anchi%C3%AAta-Heran%C3%A7a-Digital.pdf. Acesso em: 20 out. 2020.

BASSOTTO, Lucas. **O que é blockchain? Como funciona a tecnologia?.** *[S.l.],* 2018. Disponível em: https://cointimes.com.br/o-que-e-blockchain-como-funciona/. Acesso em: 10 set. 2020.

BOSSLE, Guillherme. **Aula ministrada para o curso de graduação em Direito.** *In:* Universidade do Sul de Santa Catarina (Unisul) - Curso de Graduação em Direito. 2019, Florianópolis.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 nov. 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4099 de 2012**. Brasília, DF: Câmara dos Deputados, 2012a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548678. Acesso em: 11 nov. 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4847 de 2012.** Brasília, DF: Câmara dos Deputados, 2012b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=563396. Acesso em: 24 out. 2020.

BRASIL**. Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 nov. 2020.

BRASIL. **Decreto-lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Brasília, DF: Presidência da República, 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 2 nov. 2020.

BRASIL. **Lei nº10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 21 out. 2020.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 02 de nov. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 nov. 2020.

BRASIL. **Lei nº 13.105, de 16 de março de 2015.** Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 02 nov. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 nov. 2020.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018.** Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília, DF: Presidência da República, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm#:~:text=Registro%20n%C3%A3o%20autorizado%20da%20intimidade%20sexual&text=Produzir%2C%20fotografar%2C%20filmar%20ou%20registrar,Par%C3%A1grafo%20%C3%BAnico.. Acesso em: 11 nov. 2020

BRASIL. **Medida Provisória bº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 10 nov. 2020.

BRASIL. Senado Federal. **Projeto de Lei da Câmara n° 75, de 2013.** Brasília, DF: Senado Federal, [2018]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/114625. Acesso em: 24 out. 2020.

BRASIL. Senado Federal. **Projeto de Lei nº 2630 de 2020**. Brasília, DF: Senado Federal, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 10 nov. 2020.

BRASIL. Superior Tribunal de Justiça. **Agravo Interno no Recurso Especial nº 1593873**. Relatora: Ministra Nancy Andrighi. 10 de novembro de 2016. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/862954456/agravo-interno-no-recurso-especial-agint-no-resp-1593873-sp-2016-0079618-1/inteiro-teor-862954466. Acesso em: 06 nov. 2020.

BRASIL. Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental nº 403.** Relator: Ministro Edson Fachin, [2020]. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 05 nov. 2020.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4451/DF.** Relator: Ministro Alexandre de Moraes, 06 de março de 2019. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur399151/false. Acesso em: 24 out. 2020.

BRIZOLA, Fernando. **Direito Digital Aplicado:** Como Atuar com o Direito Digital. *[S.l]*, 16 de abril de 2020. 1 vídeo de (41:36 min). Publicado pelo canal Direito Digital por Fernando Brizola. Disponível em: https://www.youtube.com/watch?v=FV2BunavcSI&t=242s. Acesso em: 15 set 2020.

BUCCI, Eugênio. **Disseminação de "fake news" para atacar candidatos marca eleição.** [Entrevista cedida a] PEREIRA, Pablo; TOLEDO, Luiz Fernando; e MONNERAT, Alessandra. *[S.l],* 1º de outubro de 2018. Disponível em: https://exame.com/brasil/disseminacao-de-fake-news-para-atacar-candidatos-marca-eleicao/. Acesso em: 24 out. 2020.

CAMILLO, Carlos Eduardo Nicoletti. **O fenômeno das *Fake News* e a sua repercussão na responsabilidade civil no sistema jurídico brasileiro.** *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

CARVALHO, Alexandre. Revenge Porn e a Lei nº 13.718/2018. **Conceito Jurídico**. *[S.l.]*, nº 26, p. 55-58, fevereiro de 2019. Disponível em: https://issuu.com/alexsandercarvalho54/docs/revista_conceito_jur_dico_26. Acesso em: 13 out. 2020.

CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil** da Internet. *[S.l]*, 25 de novembro de 2014. Disponível em:

https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet. Acesso em: 06 ago. 2020.

CONSELHO DA JUSTIÇA FEDERAL. Enunciado 531. *In:* VI Jornada de Direito Civil. 6., 2013, Brasília. **Anais eletrônicos [...].** Brasília: Coordenadoria de Serviços Gráficos do Conselho da Justiça Federal, 2013. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vijornadadireitocivil2013-web.pdf. Acesso em: 12 nov. 2020.

Coutinho, Mariana. **O que é criptografia de ponta-a-ponta? Entenda o recurso de privacidade:** presente no WhatsApp e Telegram, tecnologia permite que mensagens interceptadas não possam ser lidas. *[S.l],* 12 de junho de 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml. Acesso em: 17 nov. 2020

CRUZ, Felipe Branco. **Como Funciona o Armazenamento em Nuvem.** *[S.l]*, 04 de setembro de 2015. Disponível em: https://super.abril.com.br/mundo-estranho/como-funciona-o-armazenamento-em-nuvem/. Acesso em: 28 set. 2020.

CYMBALUK, Fernando. **Fake news apelam e viralizam mais do que notícias reais, mostra estudo**. São Paulo: 08 de março de 2018. Disponível em: https://www.uol.com.br/tilt/ultimas-noticias/redacao/2018/03/08/fake-news-apelam-e-viralizam-mais-do-que-noticias-reais-mostra-pesquisa.htm. Acesso em: 27 jun. 2020.

DELAVY, Eduarda. **O que é uma hospedagem de site.** *[S.l.]*, 15 de dezembro de 2016. Disponível em: https://www.hostgator.com.br/blog/o-que-e-uma-hospedagem-de-site/#:~:text=Um%20servidor%20%C3%A9%20um%20computador,o%20termo%20hospedagem%20de%20site. Acesso em: 15 set 2020.

ESTADOS UNIDOS DA AMÉRICA. **APPLE INC'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE.** Califórnia: 22 de março de 2016**.** Disponível em: https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf. Acesso em: 08 nov. 2020

FACEBOOK. **O que acontecerá com a minha conta no Facebook se eu falecer?**. *[S.l],* [2020a]. Disponível em: https://www.facebook.com/help/103897939701143/. Acesso em: 22 out. 2020.

FACEBOOK. **O que é um contato herdeiro e o que ele pode fazer com minha conta do Facebook?.** *[S.l],* [2020b].

https://www.facebook.com/help/1568013990080948. Acesso em: 22 out. 2020.
FACEBOOK. **Solicitação de Memorial.** *[S.l],* [2020c]. Disponível em: https://www.facebook.com/help/contact/651319028315841. Acesso em: 22 out. 2020.

FRAGA, Claudia Barreto. **Herança Digital e Direito à intimidade:** A Ponderação de Normas Constitucionais na Proteção da Intimidade de Terceiros. *[S.l.],* 04 de dezembro de 2019. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/heranca-digital-e-direito-a-intimidade-a-ponderacao-de-normas-constitucionais-na-protecao-da-intimidade-de-terceiros/. Acesso em: 21 out. 2020.

FURUTANI, Karola. **Aprenda o que são Cookies e qual é a função deles no seu computador.** *[S.l]*, 14 de fevereiro de 2018. Disponível em: https://www.meupositivo.com.br/doseujeito/tendencias/o-que-sao-cookies/. Acesso em: 23 set. 2020.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil:** Responsabilidade Civil. 16 ed. São Paulo: Saraiva Educação, 2018.

GOMES, Helton Simões. **Whatsapp vai ser bloqueado? Entenda o processo que corre no STF.** *[S.l],* 20 de maio de 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/05/20/whatsapp-vai-ser-bloqueado-entenda-o-processo-que-corre-no-stf.htm. Acesso em: 03 nov. 2020.

GOMES, Wilson. **As Fake News entre digitalização e polarização política**. *[S.l]*, 25 de outubro de 2019. Disponível em: https://revistacult.uol.com.br/home/as-fake-news-entre-digitalizacao-e-polarizacao-da-politica/. Acesso em 18 ago. 2020.

GONÇALVES, Victor Hugo Pereira. **Marco Civil da Internet Comentado.** 1ª ed. São Paulo: Atlas, 2017. E-book. Acesso restrito via Minha Biblioteca.

GONZAGA, Alvaro de Azevedo; ROQUE, Nathaly Campitelli. **Teoria Tridimensional do Direito.** *[S.l]*, abril de 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/64/edicao-1/tridimensional-do-direito,-teoria. Acesso em: 04 set. 2020.

GOOGLE. **Sobre o Gerenciador de contas inativas.** *[S.l],* [2020]. Disponível em: https://support.google.com/accounts/answer/3036546?hl=pt-BR. Acesso em: 22 out. 2020.

GOOGLE PLAY. **Termos de Serviço do Google Play**. *[S.l],* 04 de agosto de 2020. Disponível em: https://play.google.com/intl/pt_br/about/play-terms/index.html. Acesso em: 21 out. 2020.

HAIKAL, Victor Auilo. **Das significações jurídicas dos conceitos integrantes do art. 5º:** Internet, Terminal, endereço internet protocol - IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao país; endereço IP; conexão à internet; registro de conexão; aplicações de internet; e registros de acesso a aplicações de internet. *In:* LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet.** São Paulo: Editora Atlas, 2014. p. 317-324. E-book. Acesso restrito via Minha Biblioteca.

KHARPAL, Arjun. **Apple vs FBI: All you need to know.** *[S.l],* 29 de março de 2016. Disponível em: https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html. Acesso em: 04 nov. 2020.

LEITÃO, Joaquim Leitão Júnior; OLIVEIRA, Marcel Gomes de. **Comentários à Lei nº 13.772 de 2018**. *[S.l]*, janeiro de 2019. Disponível em: https://jus.com.br/artigos/71187/comentarios-a-lei-n-13-772-de-2018. Acesso em: 08 out. 2020.

LEONARDI, Marcel. **Fundamentos de direito digital**. 1ª edição, São Paulo: Thomson Reuters Brasil, 2019. E-book.

LIMA, Glaydson de Farias. **Manual de direito digital**. Curitiba: Appris, 2016. E-book.

MAGALHÃES, Thalita Abadia de Oliveira. **A possibilidade de acesso aos dados privados no perfil do Facebook de usuário falecido:** colisão entre o direito à privacidade e o direito à herança. *In:* LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coord.). **Estudos Essenciais de Direito Digital.** Uberlândia: LAECC, 2019. E-book.

MARTINES, Fernando. **Google não terá que apagar resultado de buscas para a expressão "Xuxa pedófila".** *[S.l.],* 12 de maio de 2017. Disponível em: https://www.conjur.com.br/2017-mai-12/google-nao-apagar-resultado-buscas-xuxa-pedofila. Acesso em: 08 nov. 2020.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. **Fake news vs. liberdade de expressão:** uma análise favorável ao PL 2.630/20 do Senado Federal. *[S.l],* 1º de junho de 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/328010/fake-news-vs--liberdade-de-expressao---uma-analise-favoravel-ao-pl-2-630-20-do-senado-federal. Acesso em: 10 nov. 2020.

MENDONÇA, Maria Cecília da Fonte Netto de. **Herança digital:** o direito sucessório nos bancos de dados virtuais. *[S.l]*, 05 de julho de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/heranca-digital-o-direito-sucessorio-nos-bancos-de-dados-virtuais-05072020. Acesso em: 21 out. 2020.

MOTA, Tatiane. **Apps com malware foram baixados mais de 2 bilhões de vezes; saiba excluir**. *[S.l]*, 12 de novembro de 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/11/apps-com-malware-foram-baixados-mais-de-2-bilhoes-de-vezes-saiba-excluir.ghtml. Acesso em: 28 set. 2020.

MYERS, Lysa. **Tudo sobre criptografia: o que é e quando devemos usar?** Entre os diversos assuntos de segurança, a criptografia deixa muita gente confusa. Por isso, vamos explicar de forma breve o que é e para que serve. *[S.l],* 31 de agosto de 2017. Disponível em: https://www.welivesecurity.com/br/2017/08/31/tudo-sobre-criptografia-quando-usar/. Acesso em: 17 nov. 2020.

NOHARA, Irene Patrícia. **Desafios da Ciberdemocracia diante do fenômeno das *Fake News:*** regulação estatal em face dos perigos da desinformação. *In:* RAIZ,

Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

O QUE é um domínio de internet?. **Registrocom.** *[S.l],* [2020]. Disponível em https://www.registrocom.com/abc_do_dominio/dominio-significado.jsf. Acesso em: 09 nov. 2020.

ORIGINALMY. **PACWeb**. *[S.l.],* [2020]. Disponível em: https://originalmy.com/pacweb. Acesso em: 11 nov. 2020.

ORTEGA, Flávia Teixeira. **O que consiste o direito ao esquecimento?.** *[S.l],* 2015. Disponível em: https://draflaviaortega.jusbrasil.com.br/noticias/319988819/o-que-consiste-o-direito-ao-esquecimento#:~:text=Em%20mar%C3%A7o%20de%202013%2C%20na,inclui%20o%20direito%20ao%20esquecimento. Acesso em: 09 nov. 2020.

PAESANI, Liliana Minardi. **Direito e Internet.** 7ª edição, São Paulo: Atlas, 2014. Acesso Restrito via Minha Biblioteca.

PANIAGO, Isabella Pereira Rosa. **"Porn Revange":** não seja a próxima vítima**.** *[S.l.]* 1º de maio de 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/revenge-porn-nao-seja-a-proxima-vitima/. Acesso em: 13 out. 2020.

PARAÍBA. Tribunal de Justiça. **EXCEÇÃO DE SUSPEIÇÃO CRIMINAL Nº 0009593-77.2017.815.2002 – 1° Tribunal do Júri.** Relator: Desembargador Carlos Martins Beltrão Filho. 15 de janeiro de 2018. Disponível em: http://tjpb-jurisprudencia-dje.tjpb.jus.br/dje/2018/1/24/a5f01c03-5641-4343-87e7-8aa41181dbae.pdf. Acesso em: 29 out. 2020.

PECK, Patrícia. **Direito Digital.** 6ª edição, São Paulo: Saraiva, 2016. E-book. Acesso restrito via Minha Biblioteca.

PEREIRA, Pablo; TOLEDO, Luiz Fernando; MONNERAT, Alessandra. **Disseminação de "fake news" para atacar candidatos marca eleição.** *[S.l]*, 1º de outubro de 2018. Disponível em: https://exame.com/brasil/disseminacao-de-fake-news-para-atacar-candidatos-marca-eleicao/. Acesso em: 03 ago. 2020.

RAIZ, Diogo; SALES, Stela Rocha. **Fake News, Deepfakes e Eleições.** *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

REGISTRO. **Registros de novos domínios.** *[S.l]*, [2020]. Disponível em: https://registro.br/ajuda/registro-de-novos-dominios/. Acesso em 15 set 2020.
RIBEIRO, Desirée Prati. **A HERANÇA DIGITAL E O CONFLITO ENTRE O DIREITO À SUCESSÃO DOS HERDEIROS E O DIREITO À PRIVACIDADE DO DE CUJUS.** 2016. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Santa Maria, Santa Maria: 2016. Disponível em: https://egov.ufsc.br/portal/sites/default/files/a_heranca_digital_e_o_conflito_entre_direito_a_sucessao.pdf. Acesso em: 20 out. 2020.

RIO DE JANEIRO. Tribunal de Justiça. **Apelação Cível nº 0024717-80.2010.8.19.0209.** Relator: Desembargadora Valéria Dacheux. 02 de maio de 2017. Disponível em: https://www.conjur.com.br/dl/xuxa-perde-acao-google-qual-tentar.pdf. Acesso em: 08 nov. 2020.

RIO GRANDE DO SUL. **Tribunal de Justiça. Agravo de Instrumento nº 0294879-78.2018.8.21.7000.** Relator: Desembargador Carlos Eduardo Richinitti. 28 de novembro de 2018. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Acesso em: 08 nov. 2020.

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Civil nº 0332928-96.2015.8.21.7000**. Relator: Desembargador Marcelo Cezar Muller. 05 de novembro de 2015. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Acesso em: 08 nov. 2020.

RODAS, Sérgio. **Executivo do Facebook é preso por causa de apuração envolvendo WhatsApp.** *[S.l],* 1º de março de 2016. Disponível em: https://www.conjur.com.br/2016-mar-01/executivo-facebook-preso-causa-apuracao-envolvendo-whatsapp. Acesso em: 02 nov. 2020.

RODRIGUES, Gustavo Ramos. **DE VOLTA ÀS CRIPTOGUERRAS:** o caso Apple contra o FBI. 2017. Artigo apresentado no I encontro da rede de pesquisa em governança da internet. Rio de Janeiro: 14 de Novembro de 2017. Disponível em: http://redegovernanca.net.br/public/conferences/1/anais/RODRIGUES,%20Gustavo_2017.pdf. Acesso em: 04 nov. 2020.

ROSEN, Jeffrey. **The Web Means the End of Forgetting.** *[S.l],* 21 de julho de 2020. Disponível em: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html. Acesso em: 05 nov. 2020.

RUEDIGER, Marco Aurélio. **Os Robôs nas Redes Sociais**. *[S.l.]*, 2017. Disponível em: http://dapp.fgv.br/artigo-os-robos-nas-redes-sociais/. Acesso em: 27 jun. 2020.
SALUTES, Bruno. **O que é IP.** *[S.l],* 21 de outubro de 2019. Disponível em: https://canaltech.com.br/software/o-que-e-ip/. Acesso em: 21 set 2020.

SANTA CATARINA. Quarta Câmara de Recursos de Criciúma. **Recurso Inominado nº 0302227-54.2018.8.24.0020 - Criciúma.** Relator: Juiz Pedro Aujor Furtado Júnior. 11 de setembro de 2018. Disponível em: https://tj-sc.jusbrasil.com.br/jurisprudencia/625149456/recurso-inominado-ri-30222754201882400 20-criciuma-0302227-54201882400 20/inteiro-teor-625149531?ref=juris-tabs. Acesso em: 03 nov. 2020.

SANTOS, Marilda. **O Corpo é o Código:** estratégias jurídicas de enfrentamento ao revenge porn no Brasil. [Entrevista cedida a] VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. São Paulo: InternetLab, 2016. E-book. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf. Acesso em: 14 out. 2020.

SÃO PAULO. Tribunal Regional do Trabalho. **Processo TRT 15ª REGIÃO Nº 0010510-24.2018.5.15.0091.** Relatora: Desembargadora Larissa Carotta Martins da Silva Scarabelim. 07 de maio de 2019. Disponível em: https://trt15.jus.br/jurisprudencia/consulta-de-jurisprudencia. Acesso em: 31 out. 2020.

SARAIVA, Raquel. **PL das fakes news: censura? Lei da mordaça? Entenda o que pode mudar:** aprovado pelo Senado nesta terça, projeto de lei, que tem como objetivo combater notícias falsas, carrega inúmeras preocupações que ferem direitos do usuário. [Entrevista cedida a] NAKAGAWA, Liliane. *[S.l],* 02 de julho de 2020. Disponível em: https://olhardigital.com.br/noticia/pl-das-fakes-news-censura-lei-da-mordaca-entenda-o-que-pode-mudar/102964. Acesso em: 10 nov. 2020.

SERGIPE. Tribunal de Justiça. **Mandado de Segurança nº 201600110899.** Relator: Desembargador Ricardo Múcio Santana de A. Lima. 31 de agosto de 2016. Disponível em: https://www.tjse.jus.br/portal/consultas/jurisprudencia/judicial. Acesso em: 04 nov. 2020.

SILVA, Débora. **O que é Computação em Nuvem?**. *[S.l]*, 02 de outubro de 2015. Disponível em: https://www.estudopratico.com.br/o-que-e-computacao-em-nuvem/. Acesso em: 28 set. 2020.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 40ª ed., São Paulo: Malheiros, 2017.

TARTUCE, Flávio. **Herança Digital e Sucessão Legítima - Primeiras Reflexões.** *[S.l]*, 26 de setembro de 2018. Disponível em: https://migalhas.uol.com.br/coluna/familia-e-sucessoes/288109/heranca-digital-e-sucessao-legitima---primeiras-reflexoes. Acesso em: 16 out. 2020.

TERMOS de uso da loja Kindle. **Amazon**, *[S.l.]*, 23 de julho de 2020. Disponível em: https://www.amazon.com.br/gp/help/customer/display.html?nodeId=201014950. Acesso em: 21 out. 2020.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital**. São Paulo: Thomson Reuters Brasil, 2020. E-book.

THEODORO JÚNIOR; Humberto. **Curso de Direito Processual Civil**. 58ª ed, Rio de Janeiro: Forense, 2017.

TONELLI, Bruna Bizinotto. **A validade das provas e documentos digitais para o direito brasileiro.** In: CAMPOS, Adérica Ynis Ferreira *et al.* **Direito e Tecnologia: questões atuais.** Uberaba: Ed. do Autor, 2020. E-book.

TUDO sobre Malware. **br.Malwarebytes.** *[S.l],* [2018]. Disponível em: https://br.malwarebytes.com/malware/. Acesso em: 09 nov 2020.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. **O Corpo é o Código:** estratégias jurídicas de enfrentamento ao revenge

porn no Brasil. São Paulo: InternetLab, 2016. E-book. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf. Acesso em: 14 out. 2020.

VAZ, Magali. **O Corpo é o Código:** estratégias jurídicas de enfrentamento ao revenge porn no Brasil. [Entrevista cedida a] VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. São Paulo: InternetLab, 2016. E-book. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf. Acesso em: 14 out. 2020.

VIEGAS, Cláudia Mara de Almeida Rabelo; PAMPLONA FILHO, Rodolfo. **Pornografia de vingança: uma violência de gênero que gera responsabilidade civil e penal.** *[S.l]*, 2020. Disponível em: https://claudiamaraviegas.jusbrasil.com.br/artigos/859759057/pornografia-de-vinganca-uma-violencia-de-genero-que-gera-responsabilidade-civil-e-penal?ref=feed. Acesso em: 14 out. 2020.

VIEGAS, Cláudia Mara de Almeida Rabelo; SILVEIRA, Sabrina Bicalho. **A herança digital:** considerações sobre a possibilidade de extensão da personalidade civil post mortem. *[S.l.]*, 2018. Disponível em: https://claudiamaraviegas.jusbrasil.com.br/artigos/686500746/a-heranca-digital-consideracoes-sobre-a-possibilidade-de-extensao-da-personalidade-civil-post-mortem. Acesso em: 20 out. 2020.

WARDLE, Claire. **Fake news. It's complicated.** *[S.l.],* 16 de fevereiro de 2017. Disponível em: https://firstdraftnews.org/latest/fake-news-complicated/. Acesso em: 27 jun. 2020.