ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR E TÉCNICO
CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA (ASCES-UNITA)

FABRÍCIO PEREIRA ALMEIDA
JEANE MORGANA DA SILVA MEDEIROS
RAFAELLA THAYS MUNIZ SOUZA

OS DESAFIOS DO SISTEMA JURÍDICO BRASILEIRO EM FACE DE ATOS ILÍCITOS COMETIDOS NAS REDES SOCIAIS

CARUARU
2023

FABRÍCIO PEREIRA ALMEIDA
JEANE MORGANA DA SILVA MEDEIROS
RAFAELLA THAYS MUNIZ SOUZA

OS DESAFIOS DO SISTEMA JURÍDICO BRASILEIRO EM FACE DE ATOS ILÍCITOS COMETIDOS NAS REDES SOCIAIS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Tabosa de Almeida (ASCES-UNITA) como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: **Prof. Dr. Emerson Francisco de Assis.**

CARUARU

2023

FABRÍCIO PEREIRA ALMEIDA
JEANE MORGANA DA SILVA MEDEIROS
RAFAELLA THAYS MUNIZ SOUZA

OS DESAFIOS DO SISTEMA JURÍDICO BRASILEIRO EM FACE DE ATOS ILÍCITOS COMETIDOS NAS REDES SOCIAIS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Tabosa de Almeida (ASCES-UNITA) como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: **Prof. Dr. Emerson Francisco de Assis.**

Caruaru, _____ de _____ de 2023.

Banca Examinadora

_____

Prof. Orientador: Dr. Emerson Francisco de Assis.

_____

Prof. Avaliador

_____

Prof. Avaliador

RESUMO

Este trabalho científico visa examinar a aptidão do sistema jurídico brasileiro no enfrentamento dos crimes cometidos no ambiente virtual, com foco nas redes sociais, bem como a efetividade da condenação dos transgressores nas esferas cível e penal enquanto medida disciplinar. Considerando as novas formas de interações sociais ocasionadas pelo grande avanço tecnológico das últimas décadas, será apresentada uma breve cronologia da evolução histórica da rede mundial de computadores, chegando no advento das redes sociais e determinando sua aplicabilidade e efeitos na contemporaneidade. Além disso, serão abordados os possíveis mecanismos legais de controle da criminalidade cibernética vigentes no ordenamento pátrio, a fim de determinar sua eficácia prática. Tendo em vista o tipo de pesquisa exploratória empregado e considerando sua natureza investigativa, a tendência prática do estudo levará ao destrinchar das possíveis falhas do sistema ante o controle das relações virtuais, utilizando-se de uma estrutura hipotético-dedutiva enquanto aporte metodológico, a qual toma por base o aprofundamento teórico de um determinado problema. Para tanto, fora empregada como fonte de análise a revisão bibliográfica e documental, cuja combinação interpretativa culminará em propostas a serem implementadas no âmbito jurídico.

Palavras-chave: Redes Sociais Virtuais. Crimes Informáticos. Responsabilidade Civil. Responsabilidade Criminal. Direito Digital.

ABSTRACT

This paper aims to analyse the ability of Bazilian's legal system in the deal with virtual crimes, specially on social network media, as well as the efficacy of the civil and criminal convictions as disciplinary measures. Considering how society's relationships has changed since the great technological advance of the past few decades, a brief chronology of the historical evolution of worldwide computer network will be presented, turning through the advent of social networks by setting its applicability and effects at conteporaneity. In addition, the current main legal mechanisms for cybercrime's control will also be studied in order to determine its practical effectiveness. Once it is an exploratory research within an investigative nature, this essay might turns out some possible failures of the national's juridical system when it comes about the control of virtual relationships, using a hypothetical-deductive structure as a methodological contribution, which is based on the in-depth study of a specific problem. To this end, the bibliographic and documentary review was used as a source of analysis, whose interpretative combination will help providing some recomendations to be inputted at the legal sphere.

Keywords: *Virtual Social Networks. Computer Crimes. Civil Liability. Criminal Liability. Digital Law.*

SUMÁRIO

1 INTRODUÇÃO

A ascensão tecnológica da contemporaneidade rompeu com os paradigmas evolutivos sociais, colocando a humanidade em um patamar inédito de consciência e de frenético progresso. Tamanha é a velocidade de disseminação de conteúdo através dos modernos aparatos digitais, que tem sido um verdadeiro desafio para os demais setores da sociedade acompanharem à expressiva demanda da população, a fim de serem capazes de suprir as necessidades provenientes desta. O fato é que tal desenvolvimento não acontece de forma proporcional em todos os âmbitos. É com base nesta hipótese que se faz possível pressupor que na esfera jurídica a realidade não seja diferente, na qual a compreensão e a adaptação a este novo modo de vida virtual têm ocorrido vagarosamente, com discretas adesões tecnológicas ao meio.

Tendo em vista que as novas relações sociais determinam igualmente novas formas de funcionamento do Direito, a intenção deste estudo é justamente localizar possíveis pontos falhos desse sistema e apontar possibilidades de ampliação da atuação do ordenamento jurídico vigente. Em suma, a partir de uma pesquisa exploratória analisar-se-á se determinadas ferramentas legais específicas ao meio cibernético estão aptas a moderar as relações sociais neste ambiente, de modo que através de uma abordagem sistemática e analítica embasada na coleta de dados bibliográficos e documentais relativos ao Direito Digital (textos de artigos científicos, livros, periódicos e legislação) seja possível estabelecer um panorama geral contundente das melhorias necessárias no setor jurídico.

Por conta de sua natureza investigativa a metodologia utilizada na presente lide seguirá o método de estudo hipotético-dedutivo, uma vez que busca transformar premissas genéricas em conceitos mais específicos, colaborando com o mapeamento de um novo campo de trabalho. Assim, por meio da combinação de interpretações e ideias sobre o assunto, objetivar-se-á arquitetar uma teoria inicial acerca da problemática levantada, a qual mais tarde poderá vir a ser aprimorada por meio da verificação prática dos argumentos levantados.

Nesta senda, o trabalho será dividido em três partes principais: introdutoriamente, será relatado como se deu o surgimento da internet, vindo posteriormente a tratar do fenômeno contemporâneo das redes sociais, determinando sua aplicabilidade, extensão e efeitos na sociedade de Direito; na segunda etapa

serão definidos os possíveis mecanismos jurídicos de controle da criminalidade cibernética, estabelecendo uma linha histórico-evolutiva das implementações legais brasileiras, além de abordar o tema da responsabilidade civil enquanto instrumento alternativo à reprimenda penal; na terceira e última parte serão analisados os métodos investigativos dos delitos informáticos, validando a utilização destes e a eficácia da legislação digital vigente através de breves estudos de caso, e vindo a definir, por fim, propostas de melhorias a serem implementadas neste âmbito no amparo às relações virtuais considerado o cenário atual.

2 DILEMAS DE UMA SOCIEDADE EM REDE NO BRASIL E NO MUNDO

2.1 Origem e evolução da rede mundial de computadores (*internet*)

É no apogeu da Guerra Fria que a narrativa tem início, numa atmosfera tomada pelo medo de ataques iminentes e pelas incertezas do futuro, que a partir de estratégias ousadas desenvolvidas por uma das subdivisões do Departamento de Defesa dos Estados Unidos da década de 1960, a Agência de Projetos de Pesquisas Avançadas (ARPA), surge o advento da internet. O fenômeno da conexão em uma rede mundial de computadores foi inicialmente criado para fins de segurança nacional, descrito por Castells (1999) como uma “tática de guerrilha”, a qual objetivava estabelecer um sistema de comunicação entre os centros de pesquisa que fosse eficiente, confiável e que não precisasse ser controlado a partir de nenhum centro físico que o poder inimigo pudesse tomar ou destruir.

Inicialmente denominada ARPANET, a rede de comunicação tinha seu acesso restrito aos militares, chegando ao público em geral tempos depois, por volta da década de 1970, pois temia-se o mau uso da tecnologia por civis e pelos países não alinhados (CASTELLS, 1999). A partir de então foi “[...] apropriada por indivíduos e grupos no mundo inteiro e com todos os tipos de objetivos, bem diferentes das preocupações de uma extinta Guerra Fria” (CASTELLS, 1999, p.44), tonando-se a base de uma macroestrutura de conexão em constante e célere expansão, capaz de estabelecer contato com os mais remotos cantos do globo.

No Brasil, a internet começou a ser difundida no final dos anos 1980, mas nessa época ainda era uma conexão limitada e possível apenas para fins estatais,

acadêmicos e científicos. Oficialmente, a primeira conexão estabelecida no país se deu entre o Laboratório Nacional De Computação Científica do Rio de Janeiro (LNCC) e a Universidade de Maryland dos Estados Unidos (GUIZZO, 1999).

Acreditava-se na década de 1990 que a internet seria um meio de comunicação engessado e impopular, sendo utilizado em sua maioria entre empresas, bancos e o Estado de modo geral, ou na academia para fins educacionais, ficando a grande parcela da população sem acesso a maioria dos recursos que nela existiam. Entretanto, a expansão da rede no Brasil deu-se de maneira veloz, evoluindo tanto quanto as nações mundo afora, e em menos de uma década já era possível utilizá-la para fins antes inimagináveis, como por exemplo, compras online, e-mails instantâneos e até mesmo para o Imposto de Renda, o qual passou a ser possível declarar de forma online (GUIZZO, 1999).

Em última análise, cabe enfatizar que o surgimento deste aparato tecnológico na segunda metade do século passado não deve ser atribuído a um evento específico:

> O microprocessador possibilitou o microcomputador; os avanços em telecomunicações possibilitaram que os microcomputadores funcionassem em rede, aumentando assim seu poder e flexibilidade. As aplicações dessas tecnologias na indústria eletrônica ampliaram o potencial das novas tecnologias de fabricação e design na produção de semicondutores. Novos softwares foram estimulados pelo crescente mercado de microcomputadores que, por sua vez, explodiu com base nas novas aplicações e tecnologias de fácil utilização, nascidas da mente dos inventores de software. A ligação de computadores em rede expandiu-se com o uso de programas que viabilizaram uma teia mundial voltada para o usuário. E assim por diante (CASTELLS, 1999, pp.97-98).

Conforme mencionado pelo sociólogo Manuel Castells (1999), pesquisador da sociedade da informação, cujos ensaios apesar de precursores no tema têm-se mantido bastante atuais, o que ocorrera nada mais foi que uma cadeia de feitos autônomos realizados em notável confluência e harmonia que contribuíram com o desenvolvimento deste sistema tal qual se conhece hoje.

2.2 Paradigmas da pós-modernidade: difusão das redes sociais no Brasil e no mundo

Gilles Lipovetsky em seu livro “A Era do Vazio” de 1983, caracteriza o pós-modernismo como um período de extremo consumismo, de tendências individualistas,

mas de fácil adaptação, e de recorrente ceticismo quanto à imposição de concepções únicas e universais. É nesta lógica que se inserem as redes sociais: o isolamento do mundo físico causado pelo uso crescente da internet leva à constante necessidade de o sujeito estar a todo tempo se comunicando através dos meios virtuais, sempre conectado, numa tentativa de adequação do novo estilo de vida às necessidades básicas da humanidade (GERMANO; NOGUEIRA, 2017).

Por óbvio, a evolução das sociedades não ocorre do dia para a noite, é um processo lento e constante, e todo avanço alcançado é automaticamente refletido na cultura de cada povo. A conexão em rede possibilitou, pela primeira vez na história da humanidade, um intercâmbio cultural com origens históricas diversas, acessível a todos os públicos; um local onde se constroem relações interculturais de respeito, reconhecimento e solidariedade, conforme foi observado por Gadea (apud SCHERER-WARREN, 2021). Há, portanto, um deslocamento das fronteiras tradicionais para o plano mundial, conforme menciona Sarah Abdel-Moneim (2002), conectando as iniciativas locais com as globais e vice-versa, construídas em torno de impactos e visões alternativas.

Capazes de difundir dados de maneira mais ampla e rápida, as redes sociais passaram a desempenhar um papel vital na sociedade da informação, suscitando o empoderamento de coletivos e de movimentos sociais frente aos outros poderes instituídos, na medida em que atuam como elemento informativo, organizativo e articulador. São ambientes cujas configurações se definem pelas adesões por uma causa ou por afinidades políticas ou culturais, tornando-se um dos principais territórios para as discussões ideológicas contemporâneas, impulsionando a democratização das relações e diminuindo a centralização de influências convencionais (SCHERER-WARREN, 2021).

Entretanto, como todo bônus tem seu ônus, os sites de redes sociais para além das transformações positivas trouxeram consigo novas formas de manifestação da violência. Isso ocorre devido às características deste novo sistema que permitem a replicabilidade das informações, a facilitação da busca e localização, a possibilidade de permanência e a “escalabilidade”, ou seja, a capacidade de continuar funcionando apesar de contextos alterados e expandindo-se conforme a demanda (BOYD, 2010).

2.3 Globalização e a crise do rígido pensamento jurídico

O ponto central das problemáticas jurídicas está diretamente relacionado com as questões culturais de sua época; assim é avaliado o impacto da revolução tecnológica da pós-modernidade no meio jurídico pelo pesquisador Eduardo Carlos Bianca Bittar (2005). A dimensão cultural foi intensamente afetada por profundas modificações de crenças, valores, hábitos, estilos de vida, etc., de modo que os antigos padrões já não servem mais como parâmetros no processo de restabelecimento dos consensos de uniformidade. Conclui-se, portanto, que "[...] está-se diante da mudança de uma época, de uma transição intertemporal, fator de polêmicas, rejeições, ansiedades e clamor social", ou seja, uma crise (BITTAR, 2005, p.136).

Os primeiros indícios de inadequação aos habituais paradigmas do Estado de Direito legalista e da dogmática jurídica começaram a surgir ainda durante o século XIX, onde longos atos burocráticos e imensidões de textos normativos começavam a mostrar-se pouco eficientes na regulamentação das relações nos novos modelos de sociedades que surgiam. A partir da década de 1970 já era possível notar um crescimento abrupto das taxas de criminalidade, movimentos de trabalhadores, greves, pobreza, diferenças sociais, guerrilhas civis; tratava-se de uma reação em cadeia ao processo evolutivo da geração (BITTAR, 2005).

Habermas esquematizou este cenário da seguinte forma:

> Tendo como ponto de origem o sistema econômico, uma crise econômica de caráter sistêmico; tendo como ponto de origem o sistema político, uma crise de racionalidade de caráter sistêmico e uma crise de legitimação (identidade); tendo como ponto de origem o sistema sócio-cultural, uma crise de motivação (HABERMAS, 1999, p.62).

A validade universal e objetiva, a legalidade, a ordem baseada na igualdade formal e a "impositividade" enquanto valores essenciais do ordenamento jurídico concebidos nos séculos anteriores "[...] deixa(m) de ser princípio(s) de efetividade do Estado Democrático de Direito e passa(m) a ser medida(s) de contenção ideológica das mazelas formais do sistema jurídico" (BITTAR, 2005, p.145).

Neste cenário de transformações torna-se inconcebível executar o Direito fundado em valores estáveis e consensuais. A incongruência da lógica formal dos

ideais regulamentadores frente a realidade da crise coletiva enseja na vulnerabilidade do plano da justiça social, sendo crucial a atualização dos valores, das concepções e dos paradigmas da própria sociedade (BITTAR, 2005).

3 O DESEMPENHO DO ORDENAMENTO JURÍDICO BRASILEIRO NA REPRIMENDA DOS ATOS ILÍCITOS COMETIDOS NAS REDES SOCIAIS

3.1 Diferenciação entre delitos informáticos e criminalidade na internet: conceituação e classificação geral

Independentemente de toda e qualquer revolução pela qual tenha passado a humanidade, fato é que a criminalidade se caracterizou como um fator quase que intrínseco às sociedades, por mais antigas ou isoladas que fossem; o delinquente sempre existiu, e sempre utilizou os meios necessários em cada época para atingir seus objetivos (MAILLO; PRADO, 2019).

"É inegável que onde há relevância econômica deve haver relevância jurídica [...]" (JESUS; MILAGRE, 2016, p 48), e é a partir deste prisma que o Direito se faz fundamental no controle das redes digitais de informações, haja vista que todos os setores das sociedades caminham no sentido de estabelecerem suas bases no ambiente abstrato da Internet. Neste contexto, começou-se a ser cobrada na seara jurídica brasileira a criação de uma legislação específica que cuidasse de crimes eletrônicos (JESUS; MILAGRE, 2016).

Conforme precisamente colocam Jesus e Milagre (2016), antes de qualquer tomada de decisão desta natureza faz-se necessário analisar se "[...] a internet é um meio novo de execuções de crimes 'velhos' ou é, por si mesma, uma geradora de novos delitos". Segundo os pesquisadores, tal questionamento é auto responsivo, uma vez que é evidente o surgimento de novos crimes relacionados exclusivamente à rede mundial de computadores, assim como também têm acontecido crimes já há muito conhecidos pelas sociedades onde a internet é utilizada apenas como um dos meios para sua execução (JESUS; MILAGRE, 2016).

Daí a necessidade de distinção entre os conceitos de criminalidade na internet e de delitos informáticos propriamente ditos. Rodríguez Mourullo, Alonso e Lascuraín (apud JESUS; MILAGRE, 2016, p. 49) propõem que os delitos informáticos se

caracterizam por terem como objeto de ataque um elemento puramente virtual, como dados ou sistemas informáticos, enquanto que a criminalidade na internet consiste na instrumentalização do meio virtual para a prática de delitos diversos.

Neste mesmo sentido leciona Marcelo Crespo (2011, p. 63):

> A simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser – repita-se – com precisão técnica, considerada um crime informático. Ocorre, todavia, que não só autores, mas também as mídias em geral, convencionaram denominar crimes informáticos qualquer delito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito.

Contudo, ainda segundo o autor, apesar de teoricamente haver tal distinção técnica, em decorrência da popularidade social e acadêmica que o termo “crime informático” ganhou na definição de todo e qualquer delito ocorrido na internet, torna-se praticamente impossível não aderir a ele neste sentido. De acordo com esta corrente de pensamento representada pelo uso de uma nomenclatura única, de modo a garantir certa ordem nas disposições doutrinárias, os pesquisadores brasileiros passaram a dividir os tipos de crimes informáticos em grupos, ocorrendo entre uma tese e outra apenas pequenas variações que não chegam a alterar o sentido macro dos termos (CRESPO, 2011).

Viana e Machado (2013) explicam que os delitos cibernéticos podem ser classificados em 4 (quatro) classes: primeiramente, os próprios, onde a informática (ou a integridade dos dados informáticos) é o bem jurídico agredido, como por exemplo a implantação de vírus em aparelhos eletrônicos a fim de corromper dados pessoais e computacionais; segundo, os impróprios, nos quais o comportamento do agente ofende outros bens jurídicos diversos da informática, utilizando os dispositivos eletrônicos como meros instrumentos para a realização do crime, tais como a pornografia infantil, a ameaça, a injúria, etc; terceiro, os mistos, que atingem simultaneamente mais de um bem protegidos por lei, sendo um deles obrigatoriamente a informática, considerando-os, portanto, crimes complexos, por abarcarem tipos penais distintos em uma mesma conduta; e, por fim, os mediatos ou indiretos, caracterizados primariamente pela violação da informática enquanto bem jurídico, esta praticada para a ocorrência de um delito não-informático consumado ao final, como no caso de furto de dinheiro de contas bancárias através da captura de dados pessoais pelo computador.

Esta classificação é defendida também por Jesus e Milagre (2016), os quais acrescentam que o crime informático pode ser um crime-meio ou um crime-fim, este último demandando tipificação penal específica, consistindo, para tanto, nos chamados crimes próprios. A exemplo, têm-se a edição das Leis n° 12.735/2012 e n° 12.737/2012.

Já Teixeira (2014) divide os crimes informáticos em apenas 3 (três) grupos: primeiros, os puros, onde o agente intenta diretamente contra dados informáticos; segundo, os comuns, em que são utilizados aparelhos eletrônicos com internet apenas como ferramenta para o cometimento de um delito distinto dos informáticos; e terceiro, os mistos, nos quais é praticado um crime contra a informática com o único objetivo de se consumar um outro crime principal contra um bem jurídico diverso.

3.2 A regulamentação de atos ilícitos civis ocorridos nas redes sociais no Brasil

O Direito Civil da informática tem o objetivo de determinar os direitos e deveres dos usuários das tecnologias de informação, a fim de regular as relações privadas provenientes deste meio (JESUS; MILAGRE, 2016). Neste sentido, podemos citar o Marco Civil da Internet, um projeto de lei que, após um longo processo de análise legislativa, foi aprovado em 23 de abril de 2014 (TEFFÉ; MORAES, 2017).

Segundo diversos autores, o Marco Civil da Internet, ou Lei nº 12.965/2014, é considerado como a uma espécie de Constituição do ciberespaço (JESUS; MILAGRE, 2016), uma vez que tratou de esculpir primariamente os direitos e liberdades civis no território virtual, tendo como base os princípios fundamentais da Constituição Federal, ao invés de optar por uma regulamentação criminal, repressiva e punitiva (LEITE; LEMOS, 2014).

Esta lei estabelece como princípios básicos norteadores da internet brasileira a privacidade, a neutralidade da rede e a liberdade de expressão, todos interligados entre si. “Enquanto a neutralidade da rede reforça a liberdade de expressão, a privacidade representa seu limite” (TEFFÉ; MORAES, 2017, p. 112).

Neste diapasão, depreende-se da popularização das redes sociais o quão fácil tem-se tornado para qualquer indivíduo se valer de um dispositivo eletrônico para criar contas pessoais ou realizar postagens (LOPES; SCHIRMER, 2019). Apesar de revolucionar a forma como as pessoas se comunicam, tal facilidade acaba

contribuindo com a violação de diversos direitos de terceiros. Cabe salientar que a rede social nada mais é que um modelo de negócio, estruturado na comercialização de espaços para a publicidade, de produtos e até dos próprios perfis, cadastros e dados pessoais, havendo, portanto, uma relação de remuneração indireta entre seus usuários e os provedores dos aplicativos (TEFFÉ; MORAES, 2017).

A partir da configuração desta relação de consumo, diversos processos judiciais pleiteando reparação de danos causados em redes sociais passaram a lotar os Tribunais de Justiça (LADICO, 2014). O entendimento majoritário da doutrina e da jurisprudência brasileira, análogo às disposições contidas entre os artigos 19 e 21 do Marco Civil da Internet, estabelece a possibilidade da responsabilização civil subjetiva do provedor de aplicações de internet oriunda de conteúdos de autoria de terceiros apenas quando, após notificado judicialmente sobre a existência de conteúdo criminoso na rede e exigido nos termos da lei, este não realizar as providências necessárias que estejam ao seu alcance para fazer cessar os danos provenientes de tais violações (LEITE; LEMOS, 2014). Neste sentido, cita-se acórdão proferido pelo STJ, no qual a Relatora Min. Nancy Andrighi determina os limites da responsabilidade civil do provedor de aplicações:

> DIREITO CIVIL E DO CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA. [...] 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa *in omittendo.* [...] (BRASIL, 2011, p. 379).

Ademais, conforme reconhece o Marco Civil da Internet em seu artigo 18, não se deve confundir os provedores de aplicações com os provedores de conexão com a internet, estes últimos que justamente por conta da natureza de serviços prestados não possuem qualquer controle sobre a divulgação dos conteúdos nas redes, e, portanto, não estão sujeitos à responsabilização civil por quaisquer danos gerados por usuários (LEITE; LEMOS, 2014).

Porém, como toda regra possui suas exceções, eis que a principal delas no que diz respeito à responsabilização civil dos provedores de conteúdo encontra guarida no art. 21 do MCI (Marco Civil da Internet), o qual estabelece que a disponibilização de conteúdo por usuários que viole a intimidade de outrem, decorrente da divulgação de materiais contendo cenas de nudez ou de atos sexuais sem autorização de seus participantes, quando após o recebimento de notificação judicial não tornar indisponível tais conteúdos, não haverá que se falar mais em responsabilidade civil subjetiva, mas sim, em responsabilidade subsidiária por parte do provedor (TEFFÉ; MORAES, 2017). Este dispositivo tem sido objeto de incessantes críticas por parte da doutrina, que sustenta a necessidade de atribuição da responsabilidade civil subjetiva, e não subsidiária, quando da omissão do provedor também nesses casos de exposição de conteúdo privado (SCHREIBER, 2015).

Dentre outras inovações trazidas pela Lei nº 12.965 de 2014, no âmbito das investigações dos ilícitos, tem-se que, nos termos do inciso I do art. 10, apenas mediante ordem judicial os provedores serão obrigados a disponibilizar informações que permitam a identificação de algum usuário ou remover materiais danosos (proteção aos dados pessoais e às comunicações privadas). Fala-se também da guarda de dados e registros de acesso dos usuários, que deverá ser de pelo menos 1 (um) ano pelos provedores de conexão, consoante art. 13 da lei, e de 6 (seis) meses pelos provedores de aplicações, conforme o art. 15 do mesmo dispositivo legal, asseverando, para tanto, em seus arts. 14 e 16, a necessidade dos utilizadores das redes terem conhecimento sobre estas diligências (PEREIRA, 2021).

A mais atual norma brasileira que trata sobre a manutenção de direitos e deveres no ambiente virtual – bem como no meio físico –, é a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados (LGPD), em vigor desde agosto de 2020. Baseada na Regulamentação Geral de Proteção de Dados (GDPR) da União Europeia, ela tem como objetivo regulamentar a coleta e o tratamentos de dados dos

entes públicos e privados, preservando, sobretudo, as informações e o direito à privacidade das pessoas naturais (IOTTI, 2022). Em suma, a LGPD empoderou a pessoa física, uma vez que instituiu que qualquer cidadão pode ter acesso a seus dados que, porventura, se encontrem em uso por alguma organização. (MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS, 2019).

Além de versar sobre direitos fundamentais resguardados pela Constituição Federal, a Lei nº 13.709/2018 estabelece em seu artigo 6º um rol de princípios fundamentais ao processamento de dados. Primeiramente, artigo de lei indica como norteador do tratamento das informações o princípio da Finalidade, o qual determina que todo o processo deve ocorrer de maneira legítima, específica e explícita; em seguida menciona o princípio da Adequação, que por sua vez exige que o tratamento dos dados seja cumprido de acordo com as finalidades previamente estipuladas aos titulares; ademais, o princípio da Necessidade, onde são definidos limites de processamento ao mínimo necessário para se alcançar o objetivo designado; o princípio do Livre Acesso, com garantia de consulta facilitada e gratuita ao titular das informações acerca das atividades nas quais possam estar envolvidas seus dados; o princípio da Qualidade dos Dados; o princípio da Transparência; o princípio da Segurança, que visa proteger os dados pessoais de acessos não autorizados; o princípio da Prevenção, onde são adotadas medidas preventivas à ocorrência de danos durante o processamento; o princípio da Não Discriminação; e, por último, o princípio da Responsabilização e Prestação de Contas (BRASIL, 2018).

No que tange aos deveres civis dos agentes encarregados pelo tratamento dos dados, o art. 42 da LGPD é claro ao estabelecer a possibilidade de responsabilização por danos morais ou materiais eventualmente causados aos respectivos titulares das informações manejadas. A legislação especifica ainda que o dever de reparação dos danos ocorrerá de forma solidária entre o controlador e o operador de dados, podendo este último vir a responder pessoalmente com seu próprio patrimônio por indenizações devidas aos titulares (IOTTI, 2022).

Ainda, a Lei nº 13.709/2018 estipula em seu artigo 52 a aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dado (ANPD) nos casos de processamento inadequado das informações de terceiros, variando entre uma simples advertência, com indicação de prazo para adoção de medidas corretivas, até a imposição de multas proporcionais ao nível do dano causado (IOTTI, 2022)

Filgueira e Oliveira Júnior (2022) ressaltam a importância desta lei aos usuários do ciberespaço, a qual veio firmar meios mais seguros para a navegação digital, trazendo maior segurança jurídica principalmente às pessoas físicas, estas que geralmente figuram os polos mais vulneráveis nas relações de consumo. Assim colocam os autores:

> A Lei Geral de Proteção de Dados alterou o formato como as empresas e os órgãos públicos devem resguardar os dados pessoais dos indivíduos que estão vinculados ao empreendimento, dentre eles os dados dos empregados, dados dos clientes, dos prestadores de serviços, entre outros (FILGUEIRA; OLIVEIRA JÚNIOR, 2022, p.10).

Reconheceu-se, portanto, a necessidade de proteção dos dados pessoais destes usuários que são tão fundamentais para o desenvolvimento das atividades empresariais.

3.3 A regulamentação de atos ilícitos criminais ocorridos nas redes sociais no Brasil

Diz-se do Direito Penal da informática como “[...] um complexo de normas, regulamentos e entendimentos jurídicos concebidos no escopo de repreender fatos criminosos que atentem contra bens informáticos” (JESUS; MILAGRE, 2016, p. 51). Neste sentido, cita-se, a partir de então, as normas jurídicas regulamentadoras das condutas sociais no âmbito das redes sociais virtuais.

Umas das primeiras legislações desta natureza a serem promulgadas no Brasil foi a Lei nº 9.983, de 14 de julho de 2000, de autoria do Poder Executivo. Embora tenha sido criada inicialmente para proteger os sistemas da Previdência Social, passou logo em seguida a vigorar sobre todo o tráfego cibernético realizado pela Administração Pública no geral, trazendo alterações ao Código Penal no que tange a divulgação de dados sigilosos e alterações indevidas nos sistemas virtuais dos entes federativos (JESUS; MILAGRE, 2016).

Outro Projeto de Lei que merece menção foi de nº 84/1999, de autoria de Luiz Piauhylino, deputado federal por Pernambuco na época, que veio a converter-se na atual Lei nº 12.735/2012, após tramitar por 13 (treze) anos nas casas legislativas. Atualmente chamada de “Lei Azeredo” por ter tido com um dos relatores principais e defensor atuante de sua aprovação o político brasileiro Eduardo Azeredo, chegou a

ser qualificada no início de sua proposta como uma espécie de “AI-5 digital” (JESUS; MILAGRE, 2016), por conter uma redação demasiadamente ampla e rígida, chegando a criminalizar condutas socialmente comuns aos usuários nas redes, flertando com os perigos de uma censura velada (PEREIRA, 2021).

Assim discorrem Leite e Lemos acerca deste polêmico Projeto de Lei:

> Por exemplo, criminalizava práticas como transferir as músicas de um iPod de volta para o computador. Ou, ainda, criminalizava práticas como desbloquear um celular para ser usado por operadores diferentes. Ambas punidas com até quatro anos de reclusão. E esses são apenas dois exemplos pontuais. Se aprovada como proposta, aquela lei significaria um engessamento da possibilidade de inovação no país. Seria uma lei que nos engessaria para sempre como consumidores de produtos tecnológicos, criminalizando diversas etapas necessárias para a pesquisa, inovação e produção de novos serviços tecnológicos (LEITE; LEMOS, 2014, p. 04).

Como efeito, após forte rejeição da sociedade, o PL nº 84/1999 teve cerca de 14 (quatorze) propostas de artigos suprimidos, consolidando-se com apenas 4 (quatro) ao final. Apesar de não inserir tipo penal novo ao ordenamento jurídico, a Lei nª 12.735/2012 viabilizou a criação e aperfeiçoamento de órgãos voltados ao combate e investigação de delitos ocorridos nas redes de computadores, além de acrescentar à Lei nª 7.716/1989 – a qual regulamenta sobre os crimes de preconceito de raça e cor – a possibilidade de suspensão de publicações eletrônicas (ou em qualquer outro meio) de natureza nazista ou afim (JESUS; MILAGRE, 2016).

Foi também no ano de 2012 que veio a ser aprovada a principal norma penal que versa sobre crimes informáticos presente no ordenamento jurídico brasileiro até então: a Lei n° 12.737/2012, ou, como é popularmente conhecida, "Lei Carolina Dieckmann", em referência ao famoso caso da atriz que teve suas fotos íntimas vazadas na internet. Em que pese sua tramitação em tempo recorde, a referida legislação estabeleceu-se como uma espécie de marco legal para os crimes desta natureza ao tratar de temas fundamentais do ramo, como a liberdade individual no meio digital, o direito à intimidade e a segurança das informações pessoais (JESUS; MILAGRE, 2016).

A Lei de Crimes Informáticos n° 12.737/2012 incorporou os artigos 154-A e 154-B no Código Penal Brasileiro, onde passou a tipificar a “[...] invasão de dispositivo informático alheio, conectado ou não à rede de computadores, por meio de violação indevida de mecanismo de segurança [...]” como crime (SOUSA, 2021, p. 44).

Ademais, incluiu disposições acerca da interrupção ou perturbação de serviço informático, telemático, ou de informação de utilidade pública, determinando a quem nestes incorrer as mesmas sanções do tipo penal descrito no art. 266 do CP, além de equiparar o cartão de crédito ou débito à documentos particulares, no que tange ao crime de falsificação previsto no art. 298 do mesmo dispositivo legal (SOUSA, 2021).

Destarte, passou a jurisprudência a equiparar a invasão de dispositivo informático ao crime de interceptação de comunicação, o qual encontra previsão no artigo 10º da Lei nº 9.296/1996, visando ampliar a aplicação do que se entende por obtenção ilegal de informações de terceiros. Tendo em vista que a interceptação pressupõe apenas a captação de dados de comunicações que estejam em curso, tinha-se uma tipificação extremamente frágil, deixando a cargo da descrição de uma única conduta a tutela dos usuários dos meios informáticos (SOUSA, 2021).

Eis um dos julgados realizado pelo Tribunal de Justiça de Santa Catarina neste contexto:

> CRIME DE INTERCEPTAÇÃO DE COMUNICAÇÃO (LEI N. 9.296/96, ART. 10) - INVASÃO A PROVEDOR DE INTERNET E COMPUTADORES DE SEUS USUÁRIOS - DOMÍNIO TOTAL SOBRE AS MÁQUINAS - TIPICIDADE - RECURSO NÃO PROVIDO. Configura o crime do art. 10 da Lei n. 9.296/96, a conduta de quem "invade" provedor de internet, apropriando-se dos logins e senhas de seus usuários e, assim, "invadindo" seus computadores, aos quais tinha livre e desimpedido acesso, podendo, inclusive, apagar arquivos de sistema, como, de fato, o fez (SANTA CATARINA, 2007, sp).

Importante crítica levantada pelos pesquisadores Jesus e Milagre (2016) foi o fato do delito do art. 154-A, *caput*, do Código Penal, ter sido tratado de início como crime de menor potencial ofensivo de competência dos Juizados Especiais Federais (art. 61 da Lei nº 9.099/1995), demonstrando os autores ser insuficiente o procedimento simplificado para apuração de delitos desta natureza. Entretanto, após implementação da Lei nº 14.155, de 27 de maio de 2021, foram modificadas as penas para os tipos previsto no artigo supracitado do Código Penal, tornando-as mais graves, bem como as dos crimes referidos nos arts. 155 e 171, acrescentando-lhe os §§ 4º-B e 4º-C, e §§ 2º-A e 2º-B, respectivamente.

Outra pertinente reflexão realizada pelos autores diz respeito à descrição relativamente genérica dos delitos implementados pela Lei 12.737/2012:

> [...]nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos

> de mera conduta, cuja simples prática – independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente – já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade de risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características (JESUS; MILAGRE, 2016, p. 74).

Ou seja, partindo deste pressuposto, a tentativa de enquadrar isoladamente meras condutas de forma tão ampla no rol de delitos penais, não levando em consideração a intenção do agente, tampouco os possíveis efeitos decorrentes do ato, poderiam vir a abarcar situações que por sua trivialidade não mereciam ensejar na repressão penal.

Tema de relevante clamor social, os crimes de natureza sexual cometidos na internet, mormente nas redes sociais, são objeto de diversos debates na legislação brasileira. Crimes como a pornografia infantil e a pedofilia – que não é caracterizada como um tipo penal em si, mas como uma conduta praticada por pedófilo - no ambiente digital são exemplos que ganharam notoriedade devido à alta incidência após a popularização das redes, dada a conveniência do anonimato, estando descritos na Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), do artigo 241 ao 241-E. As penas máximas incidentes a estes tipos de crimes são de 3 (três) à 8 (oito) anos de reclusão (SOUSA, 2021).

Necessário se faz ressaltar que a analogia tem sido um recurso basilar nos tribunais brasileiros na lide para com os crimes virtuais cometidos nas redes, uma vez que geralmente tratam-se de condutas já tipificadas na legislação, inovando apenas no meio utilizado a sua prática, qual seja, o ciberespaço (FILGUEIRA; OLIVEIRA JÚNIOR, 2022).

4 ANÁLISE DE CASOS CONCRETOS IMPACTANTES DE DELITOS NAS REDES SOCIAIS NO BRASIL

4.1 Aspectos gerais da investigação cibernética

Embora soe trivial enfatizar o árduo caminho a ser percorrido pelo sistema jurídico para manter-se apto ante a revolução tecnológica da contemporaneidade,

inevitável se faz citar a precariedade do suporte de tecnologia e segurança da informação nestas esferas, especialmente quando se trata de investigação criminal virtual. José Antônio Milagre é um dos especialistas em Direito Digital e investigação cibernética forense mais atuante no ramo acadêmico atualmente, o qual, em parceria com o também jurista Damásio de Jesus em sua obra conjunta "Crimes Cibernéticos" de 2016, propôs uma sistematização dos métodos legislativos e traçou o panorama estrutural de como pode ocorrer a persecução aos agentes infratores nas redes. (JESUS; MILAGRE, 2016).

Segundo os pesquisadores, todos acessos realizados às redes geram dados de conexão, os quais sempre são armazenados pelos sistemas de fornecimento de aplicações e conexão à internet, ainda que o criminoso tente fazê-lo de forma anônima, ocorrendo da seguinte forma:

> Quando alguém se conecta na Internet, para boas ou más finalidades, o faz através de um ISP (Internet Service Provider), ou provedor de acesso à Internet. Este provedor atribui ao usuário um endereço IP (Internet Protocol), em uma determinada faixa de data e horário – comumente enquanto durar a conexão à Internet. Tal atribuição pode ficar registrada no provedor de conexão (registros de conexão associados a dados cadastrais). O usuário, por sua vez, ao interagir com serviços na Internet (hospedagem, blogs, emails, chats, discos virtuais, redes sociais, mensageiros, serviços de vídeos etc.), tem seus dados registrados por estas aplicações, o que se chama de “registro de acesso a aplicações na Internet”, que contém várias informações sobre o uso do serviço web por tal usuário (data, hora, IP, fuso horário associado ao uso de determinada aplicação) (JESUS; MILAGRE, 2016, pp. 183-184).

Considerando que na grande maioria dos crimes digitais a vítima é apenas utilizadora dos serviços, não possuindo acesso à administração do ativo informático utilizado para a prática do crime, faz-se necessária a ajuda dos terceiros que detém este domínio para que seja apurada a responsabilidade do delito. Todavia, tais registros só podem ser fornecidos mediante ordem judicial (JESUS; MILAGRE, 2016).

Assim, toda investigação cibernética visa inicialmente localizar o IP *(Internet Protocol)*, o qual deverá ser fornecido pelos provedores de aplicações, para descobrir-se através deste qual provedor de acesso à internet foi utilizado pelo agente criminoso, “[...] e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa” (JESUS; MILAGRE, 2016, p. 184).

Mesmo nos casos em que o agente criminoso não seja o titular da conta de Internet, este último pode acabar respondendo por negligência da segurança da sua rede, ao permitir que terceiros a acessassem de maneira indiscriminada. Uma situação ainda mais grave é quando um destes provedores não está no Brasil, onde o recurso mais comum de contato com autoridades e fornecedores de serviços no exterior, obedecendo aos ditames processuais de produção de provas lícitas, é a morosa “carta rogatória” (JESUS; MILAGRE, 2016).

Por ser o Brasil signatário do MLAT (*Mutual Legal Assistance Treaty*), há ainda a possibilidade de uso do chamado DRCI (Departamento de Recuperação de Ativos e Cooperação Internacional) do Ministério da Justiça, no qual é possível ser feita uma intermediação mais direta entre os órgãos judiciais dos países envolvidos. Entretanto, tal procedimento pode ser igualmente vagaroso, e, como os provedores de aplicações excluem rapidamente os dados de acesso dos usuários, a aquisição das informações necessárias pode nunca acontecer, ficando o crime eletrônico sem apuração pela ausência de provas (JESUS; MILAGRE, 2016).

No ordenamento jurídico brasileiro ainda não há lei específica que trate da estrutura investigativa nos crimes cibernéticos, fato este que de acordo com Jesus e Milagre (2016) torna infrutíferas as legislações penais específicas já existentes, pois estas não atuam efetivamente na redução dos ilícitos descritos. A única exceção é a Lei nº 12.735/2012 (Lei Azeredo), a qual chega a prever a possibilidade de criação de setores e equipes especializadas no combate à ação delituosa nas redes por parte de órgãos específicos da polícia judiciária.

A realidade não muda muito no que tange ao tratamento da interceptação telemática, um recurso que é muito útil na investigação dos delitos virtuais. Este instrumento encontra-se previsto na Lei nº 9.296/1996, o qual tem seu uso exclusivo para a formação das provas em investigação criminal e em instrução processual penal, mediante ordem do juízo competente, quando não for possível a obtenção destas por outros meios; sendo aplicada apenas nos casos em que a pena para a infração cometida seja a de reclusão, e devendo ocorrer impreterivelmente sob segredo de justiça (JESUS; MILAGRE, 2016).

A carência de especialistas em informática e segurança da informação nos setores jurídicos brasileiros, conforme especificam Jesus e Milagre (2016), culmina na criação irrazoável de tipos penais, uma vez que no nosso ordenamento os legisladores

tendem à optarem por uma regulamentação mais punitiva, como já citado anteriormente. Diante disso, os autores sugeriram uma metodologia específica para se legislar sobre os crimes digitais, a qual denominaram de “TCC – Técnica, Comportamento e Crime” (JESUS; MILAGRE, 2016, p.26).

De acordo com a proposta apresentada, ao se dispor sobre estes delitos deve-se primeiramente analisar as condutas incriminâveis, ou seja, o comportamento do agente e suas intenções, e não as técnicas cibernéticas utilizadas por ele para efetivar o ilícito (JESUS; MILAGRE, 2016). A ideia parte do pressuposto de que “[...] nem toda a técnica se enquadra em um comportamento incriminável [...]” (JESUS; MILAGRE, 2016, p. 28), tal como especificado a seguir:

> • Técnica: método, procedimento, software ou processo informático utilizado e que pode caracterizar um comportamento. Uma técnica pode ser executada manualmente ou por meio de subtécnicas, métodos automatizados ou ferramentas. A exemplo, um agente que obtém acesso a dados de um repositório pode estar utilizando a técnica de *sql injection*;
> • Comportamento: uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, em face de redes de computadores, dispositivos informáticos ou sistemas informatizados. No mesmo exemplo citado acima, por meio da técnica *sql injection*, o agente praticou o comportamento “invasão de sistema informático;
> • Crime: um ou vários comportamentos, que utiliza uma ou mais técnicas, que ofende um ou mais bens ou objetos jurídicos protegidos pelo Direito. Mantendo o mesmo exemplo, a “invasão de sistema informático” pode ser ou não considerada crime, dependendo do país em que é praticada (JESUS; MILAGRE, 2016, pp. 26-27).

Assim, uma única técnica pode servir de meio para a prática de uma ou mais condutas relevantes para o Direito Penal, bem como uma conduta ilícita pode ser realizada através de diversas técnicas diferentes. Contudo, pede-se cautela na análise destes tipos de crime, pois apesar de muitas técnicas quando praticadas isoladamente não representarem atos incriminâveis, em determinadas situações podem ser utilizadas por crackers com a única finalidade de descaracterizarem o tipo penal pretendido, ao desviarem a conduta do agente daquela descrita na lei (JESUS; MILAGRE, 2016).

Conclui-se, por fim, que essencial mesmo é a aquisição de conhecimentos específicos do ramo da computação por parte do operador do Direito Digital, para que este tenha a perícia de distinguir se determinadas técnicas utilizadas no meio correspondem, de fato, a um comportamento criminoso (JESUS; MILAGRE, 2016).

4.2 Principais casos de delitos nas redes sociais no Brasil

Dado o contexto examinador da presente lide, imprescindível se faz mencionar alguns casos reais de delitos cometidos nas redes sociais que foram exaustivamente examinados pelo Poder Judiciário brasileiro.

Um dos primeiros pleitos judiciais desta natureza envolveu o piloto de Fórmula 1 Rubens Barrichello, que por volta de 2006 ingressou com uma ação em face do *Google* requerendo a exclusão de determinado conteúdo lesivo à sua imagem e honra da rede social *Orkut*, nas denominadas “comunidades” de perfis criados por terceiros, e solicitando indenização pelos danos morais. Tratou-se, neste caso, de uma tentativa de responsabilização dos provedores de conteúdo por condutas ilícitas de usuários do serviço, além da demora em corrigir a situação. O Tribunal de Justiça do Estado de São Paulo deu provimento ao pedido de responsabilização do provedor de hospedagem, e estipulando uma indenização em torno de R$200.000,00 (duzentos mil reais), devida mesmo depois da retirada do conteúdo ofensivo (BRASIL, 2014).

Porém, no Superior Tribunal de Justiça o relator sustentou hipótese parcialmente contrária, alegando o seguinte:

> 4. Impossibilidade de se impor ao provedor a obrigação de exercer um controle prévio acerca do conteúdo das informações postadas no site por seus usuários, pois constituiria uma modalidade de censura prévia, o que não é admissível em nosso sistema jurídico (BRASIL, 2014, p. 1).

Ponderou, contudo, que o valor indenizatório devido seria apenas o equivalente ao período posterior ao prazo das 24 (vinte e quatro) horas iniciais em que o provedor houvesse tomando conhecimento, de fato, da existência de dados ilícitos no site por ele administrado, sem que providência alguma houvesse tomado. Ao final, portanto, manteve-se a indenização nos moldes delineados (BRASIL, 2014).

Outro caso de notável repercussão foi o que envolveu a modelo Daniella Cicarelli e seu namorado, Renato Malzoni, também no ano de 2006. Ocorre que ambos tiveram imagens de momentos íntimos captados sem seus devidos consentimentos, durante período de lazer, em praia na Espanha. As cenas capturadas ilegalmente foram publicadas em um site de visibilidade internacional, o *YouTube*. Diante da situação, o casal ajuizou uma ação na Comarca de São Paulo visando proibir a transmissão das imagens (ESTADO DE SÃO PAULO, 2008).

O Tribunal de Justiça do Estado de São Paulo deu provimento total à ação, culminando na imposição de multa diária ao *YouTube* no valor de R$250.000,00 (duzentos e cinquenta mil reais) pelo não bloqueio dos vídeos íntimos que estavam em circulação. O provedor de conteúdos que, apesar de ser sediado em país estrangeiro, possui escritórios representantes no Brasil, alegou não possuir real controle sobre os conteúdos circulantes, e que entraria em contato com a matriz do exterior. Mais de dez anos depois deste fato marcante e episódios envolvendo exposição não autorizada de imagens em sites ainda são verdadeiros obstáculos para os operadores do Direito brasileiro (ESTADO DE SÃO PAULO, 2008).

Já em junho de 2015, a família do cantor Cristiano Araújo ingressou com uma ação em face do *Google* e do *Facebook* após imagens de um acidente sofrido por ele, o qual culminou no óbito dos envolvidos, circularem nas redes. Tratavam-se de fotos e vídeos do procedimento de autópsia e preparação de corpo, bem como registros feitos no local do acidente expondo a imagem das vítimas. Foi então, ajuizada uma ação com pedido de liminar requerendo a imediata suspensão da veiculação das imagens. Na decisão, o magistrado afirmou que nestas situações os provedores de aplicações são solidariamente responsáveis com os terceiros usuários dos serviços que realizaram pessoalmente as ofensivas publicações, sendo dever destes prestadores de serviços fazer cessar tais ações ilícitas que violam o sentimento de luto vivido pelos familiares das vítimas (PAIVA, 2015).

Após a intimação da parte ré, esta acabou por não cumprir a ordem, sendo então condenada ao pagamento de multa. Em contrapartida, em 29 de outubro de 2015, a 4ª Câmara Cível do Tribunal de Justiça do Estado de Goiás deu parcial provimento a um agravo impetrado pelo *Google* e reconheceu a “inexequibilidade da ordem liminar” imposta à empresa, em decorrência do não cumprimento de uma das exigências fundamentais para a justa delimitação da responsabilidade do provedor: a demonstração por parte do demandante da localização correta do conteúdo a ser removido. Deste modo, o *Google* foi desobrigado de eliminar do seu sistema qualquer conteúdo referente ao caso. Trata-se, assim, da inequívoca vinculação dos termos do art. 19, *caput*, e § 1º, do Marco Civil da Internet, para a real configuração da responsabilidade do provedor de conteúdo (CURY, 2015).

Por sua vez, em 2017 o Tribunal de Justiça do Piauí realizou uma decisão inédita sobre o Art. 213 do Código Penal, determinando a prisão de um indivíduo por

estupro virtual. O réu utilizava do meio digital para ameaçar vítimas a lhes enviar fotos íntimas na internet, exigindo em troca da não divulgação novas imagens íntimas delas. A este comportamento foi dado o nome de “sextorsão” (ALENCAR, 2017).

Esse neologismo deriva da aglutinação das palavras “sexo” e “extorsão”, e caracteriza-se como uma “[...] forma de exploração sexual que se dá pelo constrangimento de uma pessoa à prática sexual ou pornográfica, em troca da preservação em sigilo de imagem ou vídeo da vítima em nudez total ou parcial, ou durante relações sexuais, previamente guardadas” (ALENCAR, 2017, sp). O julgado foi amplamente debatido por especialista do Direito no país, colocando-se em pauta a possibilidade de estupro sem a conjunção carnal de fato. Os nomes das partes e o número do processo não foram publicados por estar tramitando em segredo de justiça.

4.3 Propostas de melhoria do processamento jurídico de atos ilícitos civis e criminais no ordenamento brasileiro

Uma característica de grande importância no sistema jurídico brasileiro é o princípio constitucional da reserva legal, previsto no artigo 5ª, inc. XXXIX, da Carta Magna, o qual determina que "não há crime sem lei anterior que o defina” (BRASIL, 1988). A necessidade constante de enquadramento legal, de modo que se têm a lei como fonte principal do Direito, sempre foi motivo de debate entre os especialistas, sobretudo no que tange às tentativas vãs de emparelhamento do processo legislativo com os avanços tecnológicos da contemporaneidade, uma vez que este ocorre de maneira consideravelmente mais rápida que aquele (JESUS; MILAGRE, 2016).

A grande tônica acerca deste tema é se o legislativo deve mesmo criar novas leis penais específicas ou apenas adaptar as que já estão em vigência. De acordo com o parecer dos especialistas Jesus e Milagre (2016, p. 63) “[...] no Brasil, o legislador criminal pátrio caminha no sentido das alterações do Código Penal e do Código de Processo Penal. ” Os autores advertem ainda sobre o modo de concepção e tratamento das situações jurídicas no Direito Digital por parte do legislador, que equivocadamente tenta criminalizar técnicas informáticas ao invés da conduta praticada, “[...] técnicas estas que são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas” (JESUS; MILAGRE, 2016, p. 26).

Assim, um dos aspectos a serem tratados nada mais é do que o método utilizado pelo legislativo para a criação de leis no âmbito informático; deve-se cuidar para que não seja concebida uma "[...] ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado" (JESUS; MILAGRE, 2016, p. 26). Contudo, todos os fatos na esfera jurídica devem ser analisados com parcimônia para que excessos não ocorram, o que indica que nem sempre será necessário (nem possível) esperar por uma atualização do legislativo acontecer. Sendo admissível o enquadramento de determinada conduta antissocial a algum dispositivo legal em vigor, é evidente que a alusão ao direito comparado e às situações já submetidas ao crivo jurídico seja a melhor opção (LOPES, 2015).

Neste sentido, Alexandre Jean Daoun (2011, p. 2) sugere a utilização mínima do Direito Penal, o qual deve ser guardado apenas para situações absolutamente extremas, condenando, inclusive, a criação de legislação específica para os crimes virtuais, sob a justificativa de que a grande maioria das relações que se mantêm nesse ambiente já são disciplinadas pela legislação penal vigente. Daí surge outra crítica importante a ser considerada: a aplicação dos outros ramos do Direito na repressão de situações praticadas no meio informático das redes sociais, como a responsabilização civil através de indenizações, em oposição à condenação com privação da liberdade ou restrição de outros direitos.

Jesus e Milagre (2016) igualmente acreditam que as sanções tipicamente aderidas pela legislação penal brasileira sejam inviáveis enquanto instrumento reparador dos crimes cibernéticos:

> No que tange à prisão, em nossa ótica esta não se revela a medida mais adequada a lidar com criminosos desta natureza. Em verdade, pela nova Lei das prisões (Lei n. 12.403, de 4-5-2011), torna-se difícil que um cracker possa ser preso preventivamente. Já diante da condenação, entendemos que a tais meliantes podem ser aplicadas penas envolvendo prestação de serviços de segurança da informação e blindagem de sistemas (JESUS; MILAGRE, 2016, p. 196).

Sob outra ótica, inútil será a tipificação ou a criação de leis se não houver uma estrutura investigativa eficiente para que se alcance o agente infrator, e nisto incluem-se a cooperação internacional, a melhoria do aparelhamento policial e o aperfeiçoamento profissional dos que operam nessas áreas (ROZA, 2007, apud JESUS; MILAGRE, 2016). Do mesmo modo, tornou-se a prova eletrônica uma das principais barreiras para o sucesso da persecução criminal, visto que para serem

aceitas juridicamente necessitam passar por rigorosa perícia técnica a fim de atestar sua confiabilidade, e isto demanda a aquisição de conhecimentos específicos por parte das autoridades competentes (JESUS; MILAGRE, 2016).

A problemática da jurisdição nos processos investigativos também é uma pauta importante a ser debatida, considerando que muitos serviços utilizados por brasileiros são de empresas sediadas em solo estrangeiro. A colaboração internacional visa conjugar esforços no combate aos crimes eletrônicos, e nesta senda pode-se citar a realização da Convenção de Budapeste, uma documentação de Direito Internacional Público firmada em 23 de novembro de 2001 pelos países signatários do Conselho da Europa, que fixou diretrizes às políticas nacionais e propôs a harmonização das legislações frente ao eficiente combate ao *cibercrime*. Mesmo contando com posterior adesão de países como Austrália, Japão e Estados Unidos, o Brasil, todavia, não aderiu ao acordo (JESUS; MILAGRE, 2016).

Através de uma uniformização mínima das leis em escala global, assim como uma padronização dos registros e logs dos sites e sistemas de aplicações, o objetivo que se pretende alcançar é a eficaz repreensão do crime cibernético independente da nacionalidade dos envolvidos e do local onde ocorreu a ação (ou omissão) e o resultado (JESUS; MILAGRE, 2016).

No tocante à organização investigativa, o que se tem atualmente no cenário nacional são as delegacias especializadas no combate aos crimes informáticos, mas que ainda se limitam a atuarem em centros urbanos específicos. Desenvolver um arcabouço jurídico progressista para proteção do cidadão e seus dados, ampliar a atuação do Brasil em ações conjuntas com outros países voltadas ao enfrentamento da criminalidade nas redes, a fim de fortalecer as táticas investigativas, e investir maciçamente em educação digital para os operadores da lei são, portanto, fundamentais para que o Estado de Direito seja capaz de tutelar sua sociedade. (JESUS; MILAGRE, 2016).

5 CONSIDERAÇÕES FINAIS

A Revolução Digital transformou o modo de agir e pensar da sociedade, na medida em que foi reorganizando as estruturas de poder. A globalização proporcionou ônus e bônus, cada qual a sua maneira; se por um lado gerou benefícios para a

resolução das demandas diárias, por outro, contribuiu com a expansão dos índices de criminalidade digital.

As redes sociais foram criadas com o intuito de facilitar a comunicação interpessoal. Por meio desta ferramenta as pessoas relacionam-se em tempo real, compartilhando momentos de sua existência. Ocorre que ao criar um perfil nas redes sociais o indivíduo disponibiliza uma série de dados relativos à sua personalidade, características pessoais, preferências e gostos, os quais ficam atrelados ao sistema, ocasionando o uso indevido desses dados por parte alguns usuários mal-intencionados. Estes se valem desses recursos que as redes disponibilizam para inserir mensagens, fotos ou vídeos ofensivos à honra, privacidade, intimidade ou imagem das pessoas, para realizar fraudes e aplicar golpes, causando danos aos usuários de boa-fé.

Diante desse cenário, justifica-se o tratamento legal da relação estabelecida entre o indivíduo e o provedor de conteúdo das redes sociais, uma vez que estes são os responsáveis por propiciar esse ambiente virtual interativo e por manter online todos os comentários e dados inseridos na plataforma por seus usuários. O Marco Civil da Internet (Lei n° 12.965/2014) surgiu, então, como referência principal na regulamentação desta relação, determinando a liberdade de expressão, a privacidade e a neutralidade da rede como princípios norteadores para a disciplina do uso da internet no Brasil.

Foram analisadas ainda as demais leis específicas brasileiras voltadas para coibir os crimes virtuais, quais sejam: Lei nº 12.735/2012 (Lei Azeredo), Lei n° 12.737/2012 (Lei Carolina Dieckmann), e Lei nº 13.709/2018 (Lei Geral de Proteção de Dados). Além de refletir acerca dos benefícios que essas regulamentações trouxeram, foi levantado um questionamento pertinente sobre a real eficácia delas no ordenamento brasileiro, onde se pôs em pauta sua capacidade de promover segurança jurídica e proteção aos usuários das redes sociais e da internet como um todo.

Embora parte dos doutrinadores defendam a necessidade de criação de mais leis penais específicas, observou-se que o legislador caminha no sentido de atualizar as regulamentações que já existem, entendendo que estas já são suficientes para lidar com a demanda dos crimes virtuais. De fato, se faz necessária a evolução da legislação brasileira, onde esta passe a disponibilizar soluções viáveis e mais ágeis,

dada a velocidade com que os avanços tecnológicos acontecem, entretanto, após verificação do parecer de alguns especialistas, foi possível concluir que o grande desafio, na verdade, se dá no processo da elaboração normativa sobre o tema.

Outro desafio constatado foi em relação à crescente transnacionalidade dos crimes cibernéticos, onde a cooperação internacional mostrou-se essencial dadas as características da rede, que possibilita que agente e vítima estejam em países distintos, ou mesmo quando se trata dos provedores de aplicações, os quais em sua grande maioria têm sede no exterior. Uma das soluções levantadas sobre esta problemática foi a uniformização mínima das leis, bem como a efetiva comunicação judicial e policial e uma padronização dos registros e logs, sendo assim possível repreender o crime cibernético, pouco importando a nacionalidade dos envolvidos ou o local da ação.

Conhecer a fundo as técnicas de computação tornou-se fundamental para o operador do Direito, tanto para os defensores quanto para as autoridades, a fim de terem o discernimento necessário para que no momento dos fatos não se confunda a técnica informática utilizada com o real comportamento criminoso. Ter tal sensibilidade é fundamental para que se evitem injustiças e para que se faça uma boa defesa em processos envolvendo crimes cibernéticos. Longo ainda é o caminho que o ordenamento jurídico tem a progredir, de modo que acompanhe a constante evolução social e tecnológica, seja a partir da regulamentação das interações on-line ou até no modo como são conduzidas as investigações de condutas inadequadas ou ilícitas.

REFERÊNCIAS

ABDEL-MONEIM, Sarah. G. O ciborgue zapatista: tecendo a poética virtual de resistência no Chiapas cibernético. **Estudos Feministas**, Florianópolis: UFSC, v.7, n.1-2, p.39-64, 2002. Disponível em: https://www.scielo.br/j/ref/a/ygGdRcZ9VXQWxx8t77x844v/?lang=pt. Acesso em: 02 dez. 2022.

ALENCAR, Telsírio. Juiz que decretou a 1ª prisão por estupro virtual fala sobre o crime. **Portal Pauta Judicial,** 07 de ago. 2017. Disponível em: https://www.pautajudicial.com.br/noticia/juiz-que-decretou-a-1a-prisao-por-estupro-virtual-fala-sobre-o-crime.html. Acesso em: 02 dez. 2022.

BITTAR, Eduardo C. B. **O Direito na Pós-Modernidade.** Rio de Janeiro: Forense Universitária, 2005.

BOYD, Danah. Social network sites as networked publics: affordances, dynamics, and implications. *In:* PAPACHARISSI, Zizi (org.). **Networked self:** Identity, community, and culture on social network sites. New York: Routledge, 2010. p.39-58. Disponível em: https://www.danah.org/papers/2010/SNSasNetworkedPublics.pdf. Acesso em: 02 dez. 2022.

BRASIL. **Constituição da República Federativa do Brasil (1988).** Brasília. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 27 jan. 2023.

_____. **Decreto-lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)**. Brasília. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de

1940 - Código Penal; e dá outras providências. Brasília. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).** Brasília. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 7.716, de 5 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor**.** Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L7716compilado.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 8.069, de 13 de julho de 1990. (Estatuto da Criança e do Adolescente).** Brasília. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/L8069.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 02 dez. 2022.

_____. **Lei nº 9.983, de 14 de julho de 2000**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Brasília. 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9983.htm. Acesso em: 02 dez. 2022.

_____. Superior Tribunal de Justiça (STJ) – 3 Turma. **Recurso Especial nº 1193764/SP**. Configuração e relação de consumo configurada na prestação de

serviços de provedor de conteúdo. Relator(a): Min. Nancy Andrighi, 14 de dezembro de 2010. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/866337543/inteiro-teor-866337553. Acesso em: 02 dez. 2022.

_____**.** Superior Tribunal de Justiça (STJ) – 3 Turma. **Recurso Especial nº 1.337.990/SP**. Caracterização de responsabilidade civil solidária do provedor de conteúdo por crime contra a honra motivado por terceiro usuário da rede. Relator: Min. Paulo De Tarso Sanseverino, 21 de agosto de 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/865054209/inteiro-teor-865054218. Acesso em: 02 dez. 2022.

CASTELLS, Manuel. **A Sociedade em Rede.** 8 ed. São Paulo: Paz e Terra,1999.

CRESPO, Marcelo X. F. **Crimes Digitais.** São Paulo: Saraiva, 2011.

CURY, Lilian. Representantes de Cristiano Araújo devem informar *Google* sobre conteúdo ofensivo. **Tribunal de Justiça do Estado de Goiás** - Centro de Comunicação Social, 04 de nov. 2015. Disponível em: https://www.tjgo.jus.br/index.php/institucional/centro-de-comunicacao-social/124-destaque1/17719-representantes-de-cristiano-araujo-devem-informar-google-sobre-conteudo-ofensivo. Acesso em: 02 dez. 2022.

DAOUN, Alexandre Jean. Crimes informáticos. *In:* BLUM, Renato M. S. O. (coord). **Direito Eletrônico:** A Internet e os Tribunais. Bauru: Edipro, 2001.

ESTADO DE SANTA CATARINA. Tribunal de Justiça de Santa Catarina (2ª Câm. Crimi.). **Apelação criminal nº 2007.006842- 9/SC**. Equiparação do crime de invasão de dispositivo informático ao crime de interceptação de comunicação (Lei nº 9.296, de 24 de julho de 1996). Relator: Irineu João da Silva, 22 de maio de 2007. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sc/5655203. Acesso em: 02 dez. 2022.

ESTADO DE SÃO PAULO. Tribunal de Justiça de São Paulo (4ª Câm. Dir. Priv.). **Apelação Cível nº 556.090.4/4-00**. Caracterização de responsabilidade civil solidária do provedor de conteúdo por crime de invasão e divulgação de conteúdo privado motivado por terceiro usuário da rede. Relator: Des. Ênio Santarelli Zuliani, 12 de jun de 2008. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/6917167/inteiro-teor-110007246. Acesso em: 02 dez. 2022.

FILGUEIRA, Danielle P.; OLIVEIRA JÚNIOR, Vicente C. de O. **Crimes Digitais:** a eficácia do ordenamento jurídico brasileiro em combater os crimes praticados no

ambiente virtual, 2022. 16 f. Trabalho de conclusão de curso (Graduação em Direito) - Rede Ânima Educação (Universidade Potiguar – UnP), 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/22631. Acesso em: 02 dez. 2022.

GERMANO, Idilva M. P.; NOGUEIRA, Maria C. G. M. A difusão das redes sociais digitais e as novas expressões do eu. **Revista de Psicologia**, Fortaleza, v.8, n.2, pp. 53-62, jul./dez. 2017. Disponível em: http://www.periodicos.ufc.br/psicologiaufc/article/view/19276. Acesso em: 02 dez. 2022.

GUIZZO, Érico. **Internet:** O que é, o que oferece, como conectar-se. São Paulo: Ática, 1999.

HABERMAS, Jürgen. **A Crise de Legitimação do Capitalismo Tardio**. 3 ed. Trad. Vamireh Chacon. Rio de Janeiro: Tempo Brasileiro, 1999.

IOTTI, Márcio H. A lei geral de proteção de dados e os reflexos no direito brasileiro. **Revista de Direito Civil**, v. 4, n. 1, pp. 38-50, jan./jun. 2022. Disponível em: https://revistas.anchieta.br/index.php/RevistaDirCivil/article/view/1899/1664. Acesso em: 02 dez. 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

LADICO, Dircilene da S. **Dano moral na internet e sua repercussão aos direitos personalíssimos:** a honra, a imagem e a dignidade humana. CONPEDI, 2014. Disponível em: http://publicadireito.com.br/artigos/?cod=a5e9eeab9a92ab47. Acesso em: 02 dez. 2022.

LEITE, George S.; LEMOS, Ronaldo (coords.). **Marco Civil na Internet.** São Paulo: Atlas, 2014.

LIPOVETSKY, Gilles. **A Era do Vazio:** ensaios sobre o individualismo contemporâneo (1983). Trad. T. M. Deutsch. Barueri: Manole, 2005, 200p.

LOPES, Alana F. **A Responsabilidade Civil das Redes Sociais:** 2015. 41 f. Trabalho de conclusão de curso (Graduação em Direito) - Faculdades Integradas De Caratinga/MG (FIC), 2015. Disponível em: https://dspace.doctum.edu.br/xmlui/handle/123456789/830?show=full. Acesso em: 27 jan. 2023.

LOPES, Diogo D.; SCHIRMER, Candisse. Dano oriundo de redes sociais e sua responsabilização civil. **Revista de Direito Faculdade Dom Alberto**, 2019, v. 08, n. 01, p. 01-17. Disponível em: https://revista.domalberto.edu.br/revistadedireitodomalberto/article/view/637/620. Acesso em: 02 dez. 2022.

MAILLO, Alfonso S.; PRADO, Luiz R. **Criminologia.** 4 ed. São Paulo: Forense, 2019.

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS. **Guia para a Lei Geral de Proteção de Dados**. 2019. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 02 dez. 2022.

PAIVA, Daniel. *Google* e *Facebook* terão de retirar imagens da autópsia de Cristiano Araújo. **Tribunal de Justiça do Estado de Goiás:** Centro de Comunicação Social, 26 de jun. 2015. Disponível em: https://www.tjgo.jus.br/index.php/institucional/centro-de-comunicacao-social/147-destaque2/16191-google-e-facebook-terao-de-retirar-imagens-da-autopsia-de-cristiano-araujo. Acesso em: 27 jan. 2023.

PEREIRA, Geandressa T. **Responsabilidade Civil na Internet:** 2021. 48 f. Trabalho de conclusão de curso (Graduação em Direito) - Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUI, 2021. Disponível em: https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/7423. Acesso em: 02 dez. 2022.

SCHERER-WARREN, Ilse. Redes sociais: trajetórias e fronteiras. *In:* DIAS, Leila C.; SILVEIRA, Rogério L. L.; (org.). **Redes, Sociedades e Territórios.** 3 ed. Santa Cruz do Sul: EDUNISC, 2021. p.31-52. Disponível em: https://livrandante.com.br/livros/leila-christina-dias-rogerio-leandro-lima-da-silveira-orgs-redes-sociedades-e-territorios/?doing_wp_cron=1677013203.4463419914245605468750. Acesso em: 02 dez. 2022.

SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: Newton De Lucca; Adalberto Simão Filho; Cíntia Rosa Pereira de Lima. **Direito & Internet III** – Tomo II: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 277-305.

SOUSA, Victor H. A. de. **Crimes Eletrônicos Tipificados na Lei Brasileira Face ao Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018):** 2021. 59 f. Trabalho de conclusão de curso (Graduação em Direito) - Unidade Acadêmica Especial de Ciências Sociais Aplicadas da Universidade Federal de Goiás, 2021. Disponível em: https://repositorio.bc.ufg.br/handle/ri/20363. Acesso em: 02 dez. 2022.

TEFFÉ, Chiara S. de; MORAES, Maria C. B. de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar - Revista De Ciências Jurídicas**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272. Acesso em: 02 dez. 2022.

TEIXEIRA, Tarcísio. **Curso de Direito e Processo Eletrônico:** doutrina, jurisprudência e prática. São Paulo: Saraiva, 2014.

VIANA, Tulio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013.