http://journal.unoeste.br/index.php/cs/index
DOI: 10.5747/cs.2019.v3.n4.s080
ISSN on-line 2526-7035

Colloquium Socialis

Submetido: 02/11/2019 Revisado: 13/12/2019 Aceito: 19/12/2019

O ADVENTO DA INTERNET E SEUS DESAFIOS NO CAMPO JURÍDICO BRASILEIRO: BREVE ANÁLISE DOS DISPOSITIVOS LEGAIS SOBRE O MUNDO DIGITAL

Francislaine de Almeida Coimbra Strasser[1], Myllena Gonçalves de Oliveira[1]

[1]Docente em Direito na Universidade do Oeste Paulista – UNOESTE. E-mail: fran_coimbra_@hotmail.com. [2]Graduando em Direito na Universidade do Oeste Paulista - UNOESTE. E-mail: myllenagoncalves.ol@gmail.com

RESUMO

O presente estudo tem por escopo analisar os desafios instalados pelo advento do mundo digital e alguns de seus desdobramentos no campo jurídico brasileiro. Dentre as diversas mudanças sociais ocasionadas pela inserção da informática na vida dos indivíduos, algumas das que possuem maior impacto são as alterações das atividades econômicas, comerciais, comunicativas, relações interpessoais e até mesmo criminais. Desse modo, faz-se necessário a análise do desenvolvimento histórico da internet no país e das principais normas legais formuladas para abordar especificamente o âmbito digital, dentre elas a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), passando por suas disposições principais, finalidade e eficácia. Para a apreciação do exposto acima, emprega-se no presente trabalho o método hipotético-dedutivo e pesquisa bibliográfica e legislativa.

Palavras-chave: Direito Digital; Marco Civil da Internet; Lei Geral de Proteção de Dados Pessoais; Direito Penal; Privacidade.

THE ADVENT OF THE INTERNET AND ITS CHALLENGES IN THE BRAZILIAN LEGAL FIELD: BRIEF ANALYSIS OF LEGAL DEVICES ABOUT THE DIGITAL WORLD

ABSTRACT

The present work has as scope to analyze the challenges installed by the advent of the digital world and some of its developments in the Brazilian legal field. Among the many social changes performed due to the insertion of the Internet in peoples' lives, some of the ones which have bigger impact are the modification of economic, commercial, communicative and even criminal activities, as well as interpersonal relationships. Thus, it's necessary to analyze internet's historical development in the country and the main laws designed to specifically address the digital sphere, among them are the Internet Civil Landmark Law and the General Law of Personal Data Protection (GLDP), going through their main provisions, purpose and efficiency. In order to appreciate the above, the present work uses hypothetical-deductive method and bibliographical and legislative research.

Keywords: Digital Law; Internet Civil Landmark Law; General Law of Personal Data Protection; Criminal Law; Privacy.

INTRODUÇÃO

O fenômeno da internet moderna é um tema de constante pesquisa nas mais diversas áreas do mundo científico.

Se analisada pelo ponto de vista do tempo histórico, a internet moderna, desenvolvida em meados da década de 1980 oriunda da tecnologia militar americana (ZANELLATO, 2002, p. 171), pode ser considerada ainda um recém-nascido, contrastando com sua magnitude de alcance e interferência na vida humana.

Sabe-se que a internet somada a rede mundial de computadores (*World Wide Web*) afetaram a sociedade de forma tão intensa, a ponto de redefinir alguns dos aspectos essenciais do ser humano e da sociedade, como a forma de aprender, de consumir, de interagir entre si, de socializar e fazer amigos, de se comunicar e, até mesmo, de punir.

O campo jurídico, assim como outros campos da sociedade, foi impactado por esse fenômeno.

Houve dentre as principais modificações, a inovação e digitalização de partes do processo jurídico, a facilitação de acesso a informações de relevância jurídica pelos operadores do direito – desde doutrinas até jurisprudência internacional e o desenvolvimento de ferramentas que almejam aumentar a eficiência e produtividade do campo jurídico.

Não obstante, o mundo digital trouxe também desafios para os juristas contemporâneos.

Abriu-se um novo espaço para a criação de novos delitos, os chamados "crimes cibernéticos" e com eles levantou-se a necessidade de estabelecer uma resposta jurídica que trouxesse segurança aos cidadãos.

Em outros casos, existe a omissão do legislador que não adequa, de fato, os dispositivos já existentes, principalmente o Código Penal, às condutas digitais (tipicidade), impossibilitando o enquadramento dessas em outras condutas similares no *Codex* devido ao instituto da analogia *in malam partem*.

Isto é, as falhas existentes tanto na tipificação de 'novos crimes' quanto no enquadramento das condutas digitais aos já disciplinados, instauram uma insegurança de bens jurídicos sensíveis, inviável em tempos atuais em que o mundo digital é praticamente inseparável do mundo cotidiano.

Quanto a aplicabilidade da legislação existente em âmbito internacional, a falta de participação do país em tratados internacionais sobre o tema, diminui a possibilidade de real responsabilização de infrator estrangeiro. Haja vista que inexiste a harmonização das leis sobre o tema e estas, somadas a tipificação ineficiente ou a ausência delas, dificultam a execução de institutos já complexos como o da extradição.

Assim, neste estudo analisa-se algumas das principais características do mundo digital e os desafios que estas impõem sobre o mundo jurídico brasileiro, bem como a legislação específica vigente, como forma de melhor compreender a natureza desses desafios jurídicos e confrontá-los com as soluções e/ou instrumentos legais desenvolvidos até o momento.

METODOLOGIA

Foi realizada pesquisa bibliográfica de doutrinadores especializados no tema e na legislação brasileira, buscando delimitar os maiores desafios da temática no âmbito jurídico e compará-los com o aparato legal vigente, analisando sua eficácia.

Trata-se de pesquisa qualitativa dos institutos legais, utilizando de método hipotético-dedutivo para análise da aplicação destes em situações análogas as possíveis de ocorrência em casos concretos.

RESULTADOS

A legislação vigente se mostra incompleta e ineficaz face as problemáticas advindas do mundo digital. As normas desenvolvidas especificamente para o tema tipificam um pequeno número de crimes cibernéticos e, por vezes, deixam lacunas e/ou ambiguidades no texto que impossibilitam a real eficácia destas.

DISCUSSÃO

Instantaneidade X Morosidade

Embora seja produto da década de 1980, a internet e a *World Wide Web* (WWW) tiveram real explosão no território brasileiro apenas por volta dos anos 1996-97, com o estabelecimento da internet comercial brasileira que fornecia acesso a esta para pessoa física, levando o mundo digital a população brasileira digitalmente incluída a época (CARVALHO, 2006, p. 144-145).

Atualmente, o Brasil é um dos países mais conectados com um percentual de 74,9% da população conectada à internet no ano de 2017 (IBGE, 2018, p.5).

Dessa forma, apesar de sua implantação tardia a nível nacional, a internet se expandiu, desenvolveu e se estabeleceu no país com velocidade extrema. A velocidade é, de fato, uma das características essenciais da internet, ao lado de sua presença mundial, que fazem dela um fenômeno com vasto potencial.

Entretanto, o fator preocupante é a antinomia que existe entre o ambiente digital e a tecnologia, poia ao mesmo tempo que possuem

forças extremas e de rápida manifestação para o desenvolvimento e melhoramento de institutos sociais, como a educação, a saúde a mobilidade urbana e até mesmo o direito, acabam destruindo outros, como a privacidade, a propriedade privada (intelectual) e até mesmo a segurança jurídica de uma sociedade, caso não haja uma legislação eficiente e centrada no tema.

Tanto é que a sociologia explica que o Direito, por mais que se empenhe em estar de acordo com as necessidades da sociedade em que incide, sempre estará atrás dela por depender dessa mesma sociedade para nortear suas legislações e ordenamento jurídico, principalmente quando esta sociedade é totalmente digitalizada e conectada.

A questão da rapidez também afeta a segurança de forma acentuada, haja visto que os "cyber-delitos" são cometidos na mesma proporção de tempo usual do cenário digital, ou seja, de forma quase instantânea e os processos legais se desdobram com a morosidade habitual do âmbito jurídico brasileiro.

Um levantamento realizado em 2018 pela *Symantec* (empresa especializada no ramo de segurança da internet) evidencia tal discrepância.

Segundo o relatório desta empresa, que mede o impacto humano dos crimes cibernéticos no Brasil, leva-se em média quarenta e três dias para resolver um crime cibernético no país.

Entretanto, vale ressaltar que o documento supramencionado traz que do total de casos mundiais, um terço deles não são solucionados, ou são solucionados parcialmente (SYMANTEC, 2018, p. 14-15).

Mundial X Nacional

Outra característica fundamentalmente digital é sua universalidade.

Hodiernamente, a presença de dispositivos eletrônicos conectados à rede é um evento com extensão mundial.

Isso se dá devido a vários fatores como: 1) a informação ter se tornado de grande valor ao ponto de ser considerada como bem jurídico (MARTINS; MARTINS, 2001, p. 43); 2) o acesso a fontes de informação passou a ser fonte de poder social, político e econômico, criando uma nova classe na hierarquia e relações de poder (ZANELLATO, 2002, p. 177); 3) o acesso a rede ser considerado direito básico humano pela ONU; 4) o papel da tecnologia como catalisadora de mudanças estruturais nas sociedades de todo mundo (WALD, 2001, p. 14), e outros.

Deste modo, a tecnologia e, por consequência, a internet, tornaram-se uma necessidade humana, seja elo valor econômico a ela agregado, o que garantiu a expansão a nível mundial, além do constante desenvolvimento e aperfeiçoamento, devido aos investimentos dos países e empresas privadas.

É nesse ambiente naturalmente internacional que nasce o segundo maior desafio dos juristas e legisladores de hoje: a questão territorial das condutas lícitas e ilícitas no ambiente virtual.

Para elucidar, o autor de um crime digital pode estar no país A, enquanto sua vítima está no país B. Ou ainda, o autor pode encaminhar seu ataque na vítima do país B utilizando servidores e/ou computadores nos países C e D.

Dessa forma, um crime cibernético nem sempre acontece em um mesmo território, mas sim em parte dele, além de seus resultados, poderem atingir outros territórios (BRENNER, 2006).

Patricia Peck Pinheiro leciona a respeito desse problema para o Direito Digital, nesse sentido:

> "O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais. [...]. Em suma, no Direito Digital, temos de ter uma existência e um entendimento global. A territorialidade é muito importante nesse aspecto. Que valores devemos proteger em relações de indivíduos de origens distintas? O Direito sempre interfere nas relações humanas, seja em territórios distintos ou não, onde, de algum

> modo, deve-se proteger o que acontece nessas relações. Para melhor esboçar a questão, vamos tomar como referência o Direito Internacional, pelo qual se estabeleceu que, para identificar a norma a ser aplicada, diante da extrapolação dos limites territoriais dos ordenamentos, deve-se averiguar a origem do ato e onde este tem ou teve seus efeitos, para que se possa aplicar o Direito do país que deu origem ou em que ocorreram os efeitos do ato. Aqui entra um dilema importante, que não se aplica no mundo real: na Internet, muitas vezes não é possível reconhecer facilmente de onde o interlocutor está interagindo. ” (PINHEIRO, 2016, p.84-85)

No ordenamento jurídico brasileiro, existem certos princípios que são utilizados para determinar qual ordenamento jurídico será aplicado a um caso concreto. Pode-se citar o princípio do local em que a conduta se realizou ou exerceu seus efeitos, o da localidade do réu, o do endereço eletrônico, entre outros.

Ademais, a Lei nº 12.965/2014 (Marco Civil da Internet) determina a aplicação da lei nacional nos casos em que as consequências dos atos ilícitos de uma relação jurídica internacional se dão em território brasileiro (*lex damni*) e nos casos em que umas das partes envolvidas seja domiciliada no Brasil (*lex domicilii*) (PINHEIRO, 2016, p. 86-87). Todavia, a previsão da supremacia da lei nacional nessas relações jurídicas internacionais feita por lei interna não garante sua efetividade no âmbito internacional.

Compreendendo os empecilhos que a territorialidade incide sobre o processo, julgamento, regulamentação e prevenção das condutas ilícitas na rede, o Conselho da Europa reuniu seus países membros e realizou a *Cybercrime Convention*, conhecida como Convenção de Budapeste, com o objetivo de harmonizar as legislações nacionais sobre o tema (CONCIL OF EUROPE, 2001).

Com relação ao foco do encontro, determinou-se as seguintes temáticas para elaboração de leis: violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de rede como prioridade na harmonização internacional.

O tratado foi assinado em 2001 e entrou em vigor três anos depois. Em 2013, o Conselho convidou países não membros para assinar e ratificar o tratado. Entretanto, o Brasil não foi convidado para fazer parte dele (CONCIL OF EUROPE, 2001).

Privacidade X Redes Sociais

Uma das instituições sociais mais citadas em estudos sobre Direito Digital é a privacidade do usuário na rede. Esse bem jurídico tutelado pela Lei Magna brasileira de 1988 em seu art. 5º, inc. X, dispõe que:

> “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”. (BRASIL, 1988).

Desse modo, fica tutelado a faculdade da intimidade e vida privada do indivíduo como direitos fundamentais e cláusulas pétreas.

Alexandre de Moraes (2002) assevera que quando são publicados assuntos sem finalidade jornalística, mas apenas como instrumento de entretenimento ou diversão, violam não só o direito fundamental da intimidade e vida privada, como também o direito fundamental da dignidade humana.

Não há dúvida, portanto, quanto a extensão dos direitos fundamentais à esfera digital da sociedade, principalmente após a publicações de normas recentes como o Marco Civil da Internet (Lei nº 12.965/14) que, em seu artigo 3º, inc. II, coloca a proteção à privacidade como um dos princípios regentes da disciplina do uso da ferramenta virtual e a Lei Geral de Proteção aos Dados Pessoais – LGPD (Lei nº 13.709/18), que disciplina como objetivo da norma “proteger os direitos fundamentais de liberdade e de privacidade” (BRASIL, 2018), já deixando claro em seu art. 1º., o reconhecimento da importância da questão aos olhos do legislador brasileiro.

Ainda assim, como citado alhures, o avanço normativo brasileiro não acompanha o avanço da tecnologia. Desse modo, um fato que já era de difícil controle fica ainda mais complexo com o desenvolvimento das redes sociais, que permitem publicitar as relações e acontecimentos diários da vida de uma pessoa. Aplicativos como o *Facebook, Instagram, Snapchat* e o *WhatsApp* somados a popularização da internet móvel e de aparelhos desenhados para o desempenho desses aplicativos e dessa nova rede, transformaram a forma de se comunicar digitalmente.

Sobre esse contexto, um indivíduo tem a sua disposição ferramentas que lhe permitem compartilhar sua vida ao vivo, seja por meio das *lives*, da publicação de fotos e vídeos ou de mensagens trocadas em chat 'privado' dentro desses aplicativos, tornando mais difícil de delimitar a vida privada, notadamente com o surgimento da prática do *"print"*.

O *screenshot,* mais conhecido como *'print'*, consiste em fazer uma captura da tela de um dispositivo eletrônico, produzindo uma imagem digital do que está sendo exibido na tela no momento da captura (SELETRONIC, 2018).

É relevante lembrar que o uso de capturas de tela já é aceito no Judiciário como prova -principalmente na área trabalhista e cível familiar- através de ata notarial, possuindo jurisprudência relativamente rica.

Para elucidar, analisar-se-á a seguinte situação hipotética: um indivíduo A, em conversa com um amigo B por meio de mensagens em chat privado do aplicativo *WhatsApp*, reclama de sua colega de serviço C e produz ofensas a esta, utilizando, inclusive, fotos publicadas por C em sua conta privada no aplicativo *Instagram* (onde só tem acesso ao conteúdo publicado quem o dono da conta aceitar como 'seguidor'), para fazer algumas dessas ofensas. Minutos após a conversa, o indivíduo A se depara com o conteúdo de suas mensagens com B publicadas no aplicativo *Facebook*, na página pessoal de B em modo público (quando qualquer pessoa que utiliza o aplicativo pode ver as postagens, seja ela "amiga" do autor do post ou não) em forma de *prints* retirados da conversa, onde é possível identificar A como o autor das ofensas a C.

Nessa situação hipotética existem informações privadas de dois indivíduos distintos sendo publicadas e publicitadas sem sua autorização.

Não obstante, cabe a indagação se um conteúdo publicado em redes sociais, seja em modo de exibição público ou seletivo pode ser considerado como parte da vida privada ou da intimidade de uma pessoa.

Ademais, se a questão da publicação em rede social com visualização restrita pode ser considerada como consentimento (implícito) do seu titular para a publicitação dessas informações privadas.

Liliana Minardi Paesani elucida a questão da privacidade e algumas de suas possibilidades de limitação, afirmando que:

> "[...] o direito à privacidade constitui um limite natural ao direito à informação. Em contrapartida, está privada de tutela a divulgação da notícia, quando consentida pela pessoa. Admite-se, porém, o consentimento implícito, quando a pessoa demonstra interesse em divulgar aspectos da própria vida privada.". (PAESANI, 2014, p. 34).

Já Sandri coloca que "[...] a simples obtenção de informações pessoais de outrem, sem o seu consentimento, pode ocasionar a violação da sua intimidade [...]". (SANDRI, 2019, p. 212). Corroborando seu pensamento está Sampaio, apontando que, independente da informação pessoal estar ou não no domínio fático de seu titular, este:

> "[...] continua a exercer um 'controle' sobre sua destinação. Vale dizer que não poderão ser usadas, armazenadas, processadas, tratadas, comunicadas, transmitidas, divulgadas ou publicadas – sem que tenha sido inequivocamente dada a autorização para tanto. (SAMPAIO, 1998, p.374)

Seguindo os posicionamentos de Sandri e Sampaio, é possível enquadrar os atos do indivíduo A, da situação hipotética citada alhures, como infrações a intimidade e vida privada de C, assim como, a conduta de B como infrações aos

mesmos bens jurídicos citados de ambos A e C. Pois, se um cidadão possui controle, seja ele relativo ou não, sobre suas informações pessoais, o fato dessas informações se apresentarem como conteúdo de conversas íntimas ou de conteúdo de redes sociais que possuam visualização seletiva, não retira destas a característica de dados pessoais que foram publicados sem sua autorização, sendo assim, tutelados constitucionalmente.

Nas palavras de Paesani:

> [...] A privacidade adquiriu novo significado e nova extensão e corresponde ao direito reconhecido ao indivíduo de exercer o controle sobre o uso dos próprios dados pessoais inseridos num arquivo eletrônico. (PAESANI, 2014, p. 43).

Assim, é assegurado a vítima apenas o direito a indenização, o que por si só gera um sentimento de impunidade na internet quanto a conduta das pessoas físicas, disseminando a ideia do meio como "território sem lei" para os cidadãos (considerando o homem médio) que praticam atos, como os supostos na sessão, diariamente.

Da criminalização de condutas ilícitas no âmbito virtual

A) Direito Estadunidense

Para os legisladores americanos, com os atos ilícitos na esfera virtual, surgiu e ainda surge a necessidade de se separar os crimes tradicionais dos crimes virtuais.

Brenner, assinala a necessidade de se adotar leis específicas para os crimes virtuais pois, mesmo que sejam condutas próximas das já previstas em código (como é o caso do *hacking* e do *tresspass*1), estas não se encaixam confortavelmente nas categorias de ofensa existentes.

No caso de novas condutas ainda não previstas, a autora justifica a necessidade de legislação própria justamente por essas condutas criminosas não se encontrarem no ordenamento jurídico atual (BRENNER, 2004, p. 115-116).

B) Direito Holandês

No cenário jurídico holandês, as leis mais importantes sobre o tema foram o *Computer Crime Act (Wet computercriminaliteit)* de 1993 e o *Computer Crime Act II (Wet computercriminaliteit II)*, formuladas para adaptar o Código Penal e Código de Processo Penal do país à vertente digital, criando um sistema penal "misto" paras os crimes cibernéticos.

As leis referidas disciplinam que para os atos ilícitos de origem no mundo digital são enquadradas certas condutas criminosas digitais, as já previstas nos códigos. Por exemplo, o crime de fraude e falsificação não possuem novas previsões para a sua forma digital, elas são enquadras nas provisões já existentes para suas condutas, presentes nos arts. 326 e 225 do DDC, respectivamente. Em oposição, os crimes de *hacking* e interceptação ilegal foram adicionados aos códigos citados anteriormente (KOOOPS, 2010, p. 4-15).

C) Direito Brasileiro

É fato que o Brasil iniciou seus esforços legislativos quanto a área digital tardiamente. Somente a partir do ano de 2012 é possível notar a publicação de normas especificamente pensadas para tutelar questões desse âmbito, com a promulgação das leis brasileiras nºs 12.735/12, conhecida como Lei Azeredo e a de nº 12.737/2012 conhecida extraoficialmente como Lei Carolina Dieckmann.

Quando se analisa a linha temporal dessas normas específicas, nota-se que *a priori* a preocupação do legislador foi tipificar condutas ilícitas digitais, que a Lei nº 12.737/2012 chama de "delitos informáticos", passando a delimitar os direitos, princípios e deveres básicos dos usuários da internet somente dois anos depois com a Lei nº 12.965/14, conhecida com Marco Civil da Internet.

Por fim, o legislador brasileiro volta suas atenções novamente a esse tema, passados quatro anos da publicação do Marco Civil, publicando as Leis nº 13.709 e nº 13.718, ambas no ano de 2018.

Embora até o momento existam poucos artigos no Código Penal referente ao tema, é possível concluir que o direito nacional percorre um caminho legislativo semelhante ao da legislação holandesa, criando novos artigos que tipificam algumas condutas ilícitas no âmbito da internet e ao mesmo tempo adaptando outras

[1] Similar a violação de domicílio no Brasil, previsto no art. 150 do Código Penal.

que já são previstas em 'crimes tradicionais' como aconteceu com o crime de *hacking* e a falsificação de cartão de crédito, respectivamente.

Da Legislação Brasileira Atual para com o Campo Digital

A) Lei nº 12.735/12

O texto publicado em 30 de novembro de 2012, que ficou conhecido como Lei Azeredo, tinha por objetivo "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticados contra sistemas informatizados e similares" (BRASIL, 2012).

No entanto, após os vetos presidenciais recebidos, a norma tão somente instaurou a criação de órgãos especializados no combate as condutas em meio digital nas forças policiais judiciárias, sem qualquer tipificação (art.4°) e permite ao juiz de direito, a pedido do Ministério Público, autorizar a interdição de mensagens ou páginas na internet que possuam caráter racista, antes mesmo de inquérito policial.

Embora sua importância no contexto histórico-jurídico brasileiro seja manifesta por ser a primeira norma desenhada especificamente para tratar de assuntos do mundo digital, uma vez que seu projeto de lei original é datado em 1999, o texto não trouxe mudanças significativas ao ordenamento já vigente, além de não tipificar as condutas como diz sua ementa.

B) Lei n° 12.737/12

O texto popularmente chamado de Lei Carolina Dieckmann, publicado também em 30 de novembro de 2012, foi a primeira norma brasileira a realmente tipificar e criminalizar uma conduta ilícita digital.

Vale ressaltar que o nome dado, remete ao episódio que se deu em maio mesmo do ano da publicação da lei, em que a atriz citada teve diversas fotos íntimas divulgadas na rede, as quais foram capturadas por meio de sua caixa de e-mail que havia sido hackeada.

Tal episódio deu origem a uma real discussão sobre o tema e destacou a importância e urgência de se possuir dispositivos que previssem tais acontecimentos e os regulamentasse, tutelando os bens jurídicos no meio digital, garantindo a justiça às vítimas e trazendo uma mínima segurança jurídica ao mundo conectado brasileiro.

Em seu artigo 2º, o texto acresce os artigos 154-A e 154-B ao Código Penal, criminalizando a conduta nomeada de "invasão de dispositivo informático" e definindo qualificadores e agravantes desta.

Já no artigo seguinte (artigo 3º da Lei 12737/12), coloca a interrupção de serviço de internet como conduta a ser punível, nos parâmetros do art. 266 do Código Penal, além de prever uma agravante a esta mesma conduta.

Por fim, ainda no mesmo artigo 3º, a lei enquadra a conduta de falsificação de cartão de crédito no art. 298 do Código Penal, como falsificação de documento particular.

Não obstante, apesar dessas disposições legais, a lei ainda continua falhando na eficácia, seja porque condiciona a existência do crime digital, se houver a violação de dispositivos de segurança, seja pelas provas que devem existir, mais especificamente de perícia, o qual na maior parte das vezes não consegue averiguar e confirmar o ocorrido no meio digital.

Nesse sentido, a doutrina elucida:

> "Nota-se que grande parte da ineficácia da lei 12.737/2012 está na previsão que o art. 154-A do Código Penal faz ao retratar que só existirá crime se houver violação de dispositivo de segurança. Ou seja, quando a vítima não possuir antivírus, *firewalls* ou qualquer outro meio que torne seguro seu dispositivo eletrônico e mesmo assim este for violado virtualmente, tal ato não será enquadrado como invasão de dispositivo informático, pois se faz necessário ter ultrapassado algum tipo de mecanismo de segurança. [...] A lei 12.737/2012 também encontra forte barreira em sua aplicabilidade em razão do anonimato que se faz presente no âmbito virtual, pois os delitos de natureza cibernética necessitam de provas, mais especificamente de perícia, uma vez que não há como conseguir testemunha para esse tipo

> de crime." (LOUREIRO *et al*., 2019).

Em suma, considera-se mínima a segurança jurídica trazida, haja vista que, a lei analisada tipifica, de forma incompleta, apenas a conduta de *hacking*, se mostrando como um *band-aid* jurídico emergencial, desenvolvido para sanar o caso público que lhe deu origem.

C) Marco Civil da Internet

A Lei nº 12.965 de 23 de abril de 2014, mais conhecida como Marco Civil da Internet, é resultado da parceria do Ministério da Justiça com outras instituições que buscavam retirar o aspecto de "terra sem lei" da internet brasileira, demarcando princípios e garantias, além de definir direitos, deveres e responsabilidades dos seus usuários.

Debatido o texto base produzido pelo Ministério da Justiça, teve por objetivo pautar o debate e problematizar as principais questões a serem abordadas na posterior elaboração de um projeto de lei.

As discussões foram fomentadas em blogs abertos para esse fim na rede, em seguida, foi elaborada uma minuta de anteprojeto de lei que, então, teve cada um de seus artigos, parágrafos e incisos abertos para comentários (AZEVEDO, 2014).

A possibilidade de discussão popular de um projeto de lei no ambiente virtual representou uma profunda transformação na forma de promover debates, bem como no alcance e nas possibilidades de participação nas discussões.

Os indivíduos puderam exercer a participação democrática na construção de normas a despeito da localidade que se encontravam e sem restrição de horário, uma vez que comentários e sugestões podiam ser feitos a qualquer hora do dia.

Isso reflete uma boa governança, numa democracia substancial, espaço em que as decisões são adequadas e não corrompidas, e "consiste na exigência de um agir governamental baseado na transparência, responsabilização do governante, igualdade, legalidade, não discriminação e participação" (CARVALHO, 2016, p. 761).

O conceito de bom governo é um legado de Platão (427 a.C.-347 a.C.), na Grécia Antiga, que idealizou um Estado cuja preocupação centralizava-se no bem-estar do cidadão e na ideia de justiça, ou seja, um Estado perfeito.

Em sua obra A República, o filósofo enfrenta questionamentos acerca da essência da justiça. Adotando a técnica do diálogo, ele respondia à medida que os participantes iam traçando com objetividade a forma como a justiça se configurava na sociedade.

Adaptado à realidade do século XXI, o bom governo permanece com suas bases fincadas num sistema de democracia real e concreta, com ampla participação do povo nos rumos políticos de uma nação. A completa participação social justifica-se por incluir no centro de decisões os reais destinatários das políticas adotadas, entendimento segundo o qual a boa governança só se efetiva quando as práticas governamentais correspondem aos anseios sociais, num contexto de proatividade cidadã, em que o povo opina, assume encargos, beneficia-se e responsabiliza-se pelas escolhas políticas.

Assim, o Marco Civil da Internet é um instrumento legal pioneiro não só em relação a seu conteúdo e objetivos, como também no seu processo de deliberação e formulação, que trouxe o aspecto democrático, característica clássica do mundo virtual, ao desenvolvimento da lei.

Todavia, o caráter pioneiro do texto em questão não eximiu este de críticas por especialistas e doutrinadores. Tomasevicius Filho (2016, p.276) se posiciona criticamente a esse instrumento, e coloca que "não se perceberão mudanças substanciais, uma vez que esta não acrescentou nada à legislação vigente".

Bezerra e Waltz (2014, p. 169) assinalam ainda que "a efetividade de uma legislação para a rede depende que o governo produza, em curto prazo, uma série de regulamentações que instituirão os detalhes de como serão tratados temas centrais do novo arcabouço jurídico.".

É fato que o Marco Civil em si é um avanço necessário sobre a normatização do espaço da internet brasileira e que estabeleceu respostas às dúvidas comuns dos usuários nacionais, além de refutar algumas de suas inquietações em relação a liberdade e democracia da rede no Brasil.

Dentre essas normas, pode-se destacar: 1) o art. 2° e 8º, caput, que asseguram a liberdade de expressão dentro do ambiente digital, refutando a ideia da censura poder se

reestabelecer no país; 2) a definição da impossibilidade de se responsabilizar civilmente os provedores de internet por danos de terceiros, descrita no art.18; 3) a preocupação com a segurança dos dados, registros e privacidade dos usuários presentes nos arts. 10 a 17 da Lei; 4) a previsão sobre a atuação do Poder Público diante do desenvolvimento da internet, nos arts. 24 e 25; 5) a implantação da rede como instrumento promocional de cidadania, descrita nos arts. 26 e 27, entre outros.

Não obstante, a Lei nº 12.965 /2014 é ineficaz quanto a vários outros delitos virtuais, seja por não os prever (em caso de novos delitos advindos da cultura digital), os prever parcialmente (delitos já previstos, porém sem parecer sobre a utilização do meio digital como instrumento ou ambiente de prática da conduta delituosa) ou por ignorar fatores legais essenciais na aplicação de uma norma. É o que ocorre com delitos como *catfish* e *grooming*, que não são previstos atualmente ou delitos como a calúnia, difamação e falsidade ideológica, que são parcialmente previstos.

Quanto a desconsideração de aspectos legais essenciais, têm-se a questão da não extradição por certos países e da inexistência jurisdicional do Brasil em dadas situações, o que se observa no artigo 11 do Marco Civil e nos arts. 154-A e 154-B do Código Penal Brasileiro, instaurados pela Lei n.º 12.737/12.

De acordo com o citado artigo 11, qualquer operação de coleta, guarda e tratamento de registros e dados pessoais ou de comunicação realizada por provedores ou aplicações de internet deverão respeitar a legislação brasileira. No §1º do mesmo artigo reforça que o disposto em seu c*aput* se aplica a dados coletados no país ou ao conteúdo das comunicações que possuem pelo menos um dos seus terminais em território nacional. Em seguida, o conteúdo do §2º destaca que o *caput* é aplicável mesmo para pessoas jurídicas sediadas no exterior, se estas prestarem serviços ao público brasileiro ou caso uma das integrantes de seu grupo econômico possua estabelecimento no Brasil.

Todavia, esses dispositivos também não possuem a eficácia esperada, pois o ato da coleta, guarda, dentre outros, podem não ocorrer no território brasileiro, mas sim no país sede das empresas provedoras ou ainda via servidor localizado em outro território que a empresa provedora possua instalações.

Outra situação é o ato ilícito ser realizado por empresa que não possua sede ou integrantes no Brasil, mas que presta serviços à comunidade virtual brasileira. Nesse caso, o Brasil não possui jurisdição sobre a empresa.

Já sobre o que concerne aos artigos 154-A e 154-B do Código Penal, que discorrem sobre o crime de *hacking*, a eficácia, que já é baixa quando se trata de infrator e vítimas dentro do território brasileiro, devido a dificuldades estruturais e de recursos humanos qualificados nas etapas investigativa e de perícia, é praticamente nula quando o infrator não está em território brasileiro.

Isto se dá devido ao fato do ato da invasão poder não ter se dado no território nacional e mesmo que, de fato, ocorra dentro do país, existe a possibilidade de não extradição desse infrator, dependendo de sua pátria-mãe, dos tratados de extradição firmados com o Brasil e das divergências legislativas e punitivas sobre os crimes cibernéticos – que é um obstáculo ainda maior com a não participação do Brasil na Convenção de Budapeste.

O exposto da sessão não deixa dúvidas quanto à importância histórica e social do Marco Civil, mas evidencia a alta ineficácia da lei caso não exista a implantação de instrumentos aliados e complementares a este.

D) Lei nº 13.709/18

A lei publicada em 14 de agosto de 2018, nomeada de Lei Geral de Proteção aos Dados Pessoais (LGPD), pode ser considerada o primeiro grande instrumento legal complementar da Lei nº 12.965/14 (Marco Civil), que dispõe como coloca o texto de seu art. 1º:

> "[...] sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.". (BRASIL, 2018).

Já no primeiro artigo do capítulo de disposições preliminares, o legislador deixa claro a fundamentação da tutela dos dados pessoais

digitais nos direitos fundamentais constitucionais, os explicitando um a um no artigo seguinte.

Dentre os fundamentos descritos no art. 2º, vale ressaltar a preocupação em determinar os limites dos direitos individuais e os direitos das entidades que realizam o tratamento dos dados, objetivando harmonizá-los, sem o detrimento tanto da função econômica das entidades, do desenvolvimento do mundo informático e dos direitos dos titulares dos dados.

O art. 3º delimita especificamente da questão territorial dos dispostos em seu texto, dispondo que:

> "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independente do meio, do país de sua sede ou do país onde estejam localizados os dados [...].". (BRASIL, 2018).

Em seguida, dispõe nos incisos do artigo em questão, os requisitos para a aplicação da lei nacional, determinando assim que "ainda que o controle transacional não seja da União, o mero fato de os participantes da ação serem originários da União permite que o regulamento seja aplicado." (PINHEIRO, 2018. p.56).

Entretanto, ainda se percebe a ineficácia do instrumento quanto extraterritorialidade da norma, nas situações onde a entidades responsáveis pelo tratamento não se situam no Brasil, como Tomasevicius Filho (2016, p.276-277) observa ainda na Lei do Marco Civil da Internet, mostrando que embora mais clara, a norma ainda não soluciona certas falhas das normatizações que esta complementa.

Uma observação de suma importância é sobre o art. 4ª da LGPD, que delimita as situações que não possuem tutela dessa norma, trazendo no texto de seu inc. I que o tratamento de dados "realizado por pessoa natural para fins exclusivamente particulares e não econômicos" caracteriza uma das situações que a Lei analisada não incide sobre. O disposto no inciso assinala o foco do dispositivo em regulamentar a atividades relacionadas ao fornecimento de bens e serviços. (PRINHEIRO, 2018, p. 57).

Assim, a situação hipotética apresentada no título "PRIVACIDADE X REDES SOCIAIS" deste estudo não seria tutelada nas premissas deste dispositivo, todavia, este não esclarece sobre qual área do ordenamento jurídico e/ou quais instrumentos legais tutelariam os direitos do titular dos dados quando estes são utilizados por terceiros naturais sem fundo econômico.

Nos dois últimos artigos do capítulo das disposições preliminares da norma (arts. 5º e 6º), o legislador se preocupa em explicar os conceitos de termos específicos utilizados no texto do instrumento (esclarecendo, por exemplo, o que a Lei considera dados pessoais, dados pessoais sensíveis, titular, tratamento e etc., visando diminuir a possibilidade de ambiguidade e/ou dualidade de interpretação dos dispostos ali) e demarcar os princípios que devem ser observados nas atividades de tratamento de dados, como a boa-fé, a transparência, a finalidade e outros.

Nos capítulos seguintes do instrumento, o legislador discorre sobre a forma como o tratamento deve se dar, adentrando nos aspectos: 1) dos requisitos, onde, por exemplo, detalha as situações onde é possível a realização do tratamento, assim como, detalha sobre o consentimento do titular, onde este é necessário e onde pode ser escusado e 2) do tratamento de dados pessoais sensíveis e de menores, traçando diretrizes para este processo; no aspecto dos direitos do titular, do tratamento de dados realizado por poder público, da transferência dos dados em escala internacional, dos agentes de tratamento, da segurança e sigilo durante o processo de tratamento, das sanções administrativas cabíveis aos que infringirem a norma e da Autoridade Nacional de Proteção de Dados (ANPD) e seu conselho.

Cabe afirmar, assim, que a Lei Geral de Proteção de Dados Pessoais (LGPD) se configura como um dos principais instrumentos jurídico-normativos complementares à Lei do Marco Civil da Internet, que reafirma a extensão e incidência dos direitos fundamentais no campo digital. Contudo, embora disponha sobre uma atividade essencial neste meio, que é o tratamento de dados pessoais por terceiros e pela ordem pública, esta ainda carrega as falhas de eficácia na sua aplicabilidade extraterritorial, consequência da característica mundial da rede que limita a eficácia das normas nacionais sobre o tema, a risco de torná-las obsoletas.

E) Lei n° 13.718/18

O dispositivo mais recente que incide sobre o direito digital é a Lei nº 13.718 de 24 de setembro de 2018, que modifica o Código Penal brasileiro para, entre outros objetivos, tipificar o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, acrescendo ao mesmo código o art. 218-C, que dispõe:

> "Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir**, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática -,** fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.". (BRASIL, 2018, grifo nosso).

Embora o dispositivo acrescente e estabeleça outros artigos e providencias ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o presente trabalho focará no artigo citado acima por sua clara natureza digital. A pena prevista para quem praticar a(s) conduta(s) descritas no artigo em questão é de pena privativa de liberdade, com período de um a cinco anos, isto é, se o fato não constituir crime mais grave.

O artigo analisado é a primeira tipificação de crime digital desde o ano de 2012 e embora, regulamente apenas algumas das diversas condutas ilícitas existentes na rede, não deixa de ser de grande importância, haja vista que aborda uma prática delituosa cada vez mais comum no meio, que é a divulgação de vídeos e/ou imagens íntimas sem consentimento da vítima. A prática ganhou atenção por vitimizar, comumente celebridades e pessoas públicas.

Nesses casos, a conduta prevista é, em maioria, praticada por terceiro, que invade algum dispositivo da vítima e divulga o conteúdo ilícito e íntimo. Nessa situação, o ato de divulgar esse conteúdo é um desdobramento do crime de *hacking* prevista no art. 154-A do Código Penal. Tal fato mostra a variedade de condutas ilícitas possíveis na rede e relação existente entre elas.

Outra ocorrência numerosa tutelada no texto do artigo 218-C, é a divulgação de material que contenha registro de cena de estupro ou cena de estupro de vulnerável.

Em um caso recente, uma jovem de vinte e dois anos foi dopada por um conhecido durante uma festa e foi vítima de um estupro coletivo. Entretanto, a vítima só teve conhecimento do caso dias depois, por meio de um vídeo do ato que havia sido publicado na internet. (ISTOÉ, 2019). Em outra situação, um homem foi preso por estupro de vulnerável envolvendo um adolescente de treze anos de idade. A prisão foi realizada após a mãe da vítima descobrir o vídeo do acontecimento em um grupo de *WhatsApp* e denunciou o autor do crime, que, inclusive, foi quem compartilhou o vídeo (G1, 2019).

Nestes cenários, a rede funciona como palco para o criminoso, que não satisfeito com o crime inicial, divulga, publica e/ou compartilha registro do ato para satisfazer sua lascívia e/ou a de outros além de humilhar a vítima publicamente.

Todavia, o segundo caso concreto mencionado traz uma outra situação comumente intrínseca a divulgação feita pelo autor do crime em redes sociais, que é o (re)compartilhamento desses materiais por terceiros nas mesmas plataformas originais ou em outras.

É extremamente usual a visualização de materiais ilícitos em grupos redes sociais, em especial no *Whatsapp*, que possui caráter mais privado e de difícil, senão, impossível controle de conteúdo divulgado. Fica clara a possibilidade de enquadramento do terceiro (re)compartilhador no art. 218-C, uma vez que este está publicando em meio telemático um registro de estupro ou de cena de sexo, nudez ou pornografia, sem o consentimento da vítima.

Além disso, no § 1º do artigo citado acima, o ordenamento prevê uma agravante ao crime descrito, aumentando a pena de um terço a dois terços nos casos em que "[...] o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com fim de vingança ou humilhação. " (BRASIL, 2018). Isto é, nessa agravante está tipificada o crime de *revenge porn* (pornografia de vingança, em tradução livre), ato em que a divulgação de material ilícito é feita por ex-parceiro(a) da

vítima, com intuito de humilhá-la e/ou se vingar do término da relação ou de outra situação.

Por fim, cabe reconhecer o respeito do legislador à liberdade de expressão, ao direito ao acesso à informação e à liberdade de imprensa, sem renunciar ao respeito à vítima, na formulação da excludente de ilicitude descrita no § 2º do art. 218-C, colocando:

> "Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica **com a adoção de recurso que impossibilite a identificação da vítima**, ressalvada sua prévia autorização, caso seja maior de dezoito anos.". (BRASIL, 2018, grifo nosso).

Assim, necessário avançar no campo penal, em relação a tipificação dos crimes digitais, realizado pela seguinte lei, principalmente se tratando de condutas que ferem um bem jurídico sensível como a dignidade sexual, que vitimizam, em sua maioria, minorias sociais - em especial as mulheres - e os incapazes.

CONSIDERAÇÕES FINAIS

Com o exposto conclui-se que o mundo jurídico ainda se encontra longe de alcançar o seu objetivo de disciplinar o mundo digital, embora já possua instrumentos que visam estender a esse novo e amplo espaço as diretrizes legais existentes e necessárias a qualquer sociedade, inclusive para o espaço informatizado.

Embora seja de suma importância os avanços jurídicos até então realizados, seja no cenário jurídico brasileiro ou internacional, é igualmente importante a conscientização dos legisladores sobre a necessidade de desenvolver instrumentos internacionais que harmonizem e aproximem as legislações particulares de cada território, levando em conta a essência mundial da internet e a relativa ineficácia legal de leis puramente nacionais que visam a normatização de relações e atividades realizadas no meio, para que exista, de fato, uma segurança jurídica dos indivíduos.

Quanto a prevenção e criminalização de condutas ilícitas no meio virtual, o ordenamento jurídico brasileiro ainda necessita de maior estruturação para abordar estas condutas, tipificá-las e criminalizá-las em novas diretrizes e/ou enquadrá-las efetivamente naquelas que já existem.

Uma vez que o Código Penal brasileiro não permite a analogia *in malam partem*, impossibilitando, nos casos concretos, o livre enquadramento de condutas ilícitas digitais em condutas 'tradicionais' sem a devida regulamentação legal, explicita a necessidade do esforço dos legisladores em adequar os instrumentos legais ao mundo digital.

É de igual necessidade a formulação de um parecer legal das condutas ilícitas de terceiros naturais, as quais não são tuteladas devidamente nos dispositivos atuais, aplicando o aspecto de controle e organização social, que o direito possui, nas relações informatizadas e possibilitando a real responsabilização dos infratores.

REFERÊNCIAS

AZEVEDO, A. **Marco civil da internet no Brasil.** Rio de janeiro: Alta Books, 2014.

BEZERRA, A. C.; WALTZ, I. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. **Revista Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, v.16, n.2, p.161-175, mai. 2014. Disponível em: https://jornaisdesergipe.ufs.br/index.php/eptic/issue/view/210. Acesso em: 14 ago. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 21 ago. 2019

BRASIL. **Decreto-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. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-

2014/2012/Lei/L12735.htm. Acesso em: 19 ago. 2019.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 ago. 2019.

BRASIL. **Lei Nº 12.737, de 30 de novembro de 201**2. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 ago. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 ago. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD) Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 ago. 2019.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: Acesso em: Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm. Acesso em: 22 ago. 2019.

BRASIL. **Lei Nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 23 ago. 2019.

BRENNER, S. W. Cybercrime jurisdiction. **Crime, law and social change**, v. 46, n. 4-5, p. 189-206, 2006. Disponível em: https://www.researchgate.net/publication/228796695_Cybercrime_jurisdiction. Acesso em: 15 ago. 2019. https://doi.org/10.1007/s10611-007-9063-7

BRENNER, S. W. US cybercrime law: Defining offenses. **Information Systems Frontiers**, v. 6, n. 2, p. 115-132, 2004. Disponível em: https://link.springer.com/article/10.1023%2FB%3AISFI.0000025780.94350.79. Acesso em: 15 ago. 2019. https://doi.org/10.1023/B:ISFI.0000025780.94350.79

CARVALHO. A. R. **Curso de direitos humanos.** 3. ed. São Paulo: Saraiva, 2016.

CONCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185.** 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 21 out. 2019.

G1. **Homem que estuprou adolescente e publicou vídeo no WhatsApp é preso em Olinda, diz polícia**. 2019. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2018/09/24/homem-que-estuprou-adolescente-e-publicou-video-do-crime-no-whatsapp-e-preso-em-olinda-diz-policia.ghtml. Acesso em: 30 ago. 2019.

IBGE. **Pesquisa nacional por amostra de domicílios contínua** - PNAD contínua. Divulgação anual. 2018. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 13 ago. 2019.

ISTOÉ. **Jovem sofre estupro coletivo e descobre caso por vídeo na internet**. 2019. Disponível em: https://istoe.com.br/jovem-de-22-anos-sofre-

estupro-coletivo-e-descobre-caso-por-video-na-internet/. Acesso em: 30 ago. 2019

JUNIOR, T. S. F. A liberdade como autonomia recíproca de acesso à informação. *In*: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (org.). **Direito e Internet**. São Paulo: Revista dos Tribunais, 2001. p. 241-247.

KOOPS, B. J. Cybercrime legislation in the Netherlands. *In*: BJ Koops, **Netherlands Reports To The Eighteenth International Congress Of Comparative Law**. 2010. p. 595-633. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1633958. Acesso em: 12 ago. 2019.

LOTUFO, R. Responsabilidade civil na internet. *In*: GRECO, M. A.; MARTINS, I. G. S. (org.). **Direito e Internet**. São Paulo: Revista dos Tribunais, 2001. p. 211-240.

LOUREIRO, A. J. C.; COHEN, A. C. L.; ALVES, G. C. **Análise da Lei Carolina Dieckmann e sua (in)eficácia no ordenamento jurídico brasileiro.** Portal Jurídico Investidura, Florianópolis/SC, 01 Fev. 2019. Disponível em: www.investidura.com.br/biblioteca-juridica/artigos/direito-penal/337191-analise-da-lei-carolina-dieckmann-e-sua-ineficacia-no-ordenamento-juridico-brasileiro. Acesso em: 23 Out. 2019.

MARTINS, I. G. S.; MARTINS, R. V. G. S. Privacidade na comunicação eletrônica. *In*: GRECO, M. A.; MARTINS, I. G. S. (org.). **Direito e Internet**. São Paulo: Revista dos Tribunais, 2001. p. 41-53.

MORAES, A. **Direitos Humanos Fundamentais**: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 4. ed. São Paulo: Atlas, 2002.

PAESANI, L. M. **Direito e Internet:** Liberdade de Informação. Privacidade e Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2014.

PINHEIRO, P. P. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

PINHEIRO, P. P. **Proteção de dados pessoais** – comentários à Lei nº 13.709/2018. São Paulo: Saraiva Educação. 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/4!/4/4@0.00:6.73. Acesso em: 01 set. 2019.

SAMPAIO, J. A. L. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SANDRI, J. S. O poder das redes sociais na internet e a tutela da vida privada. *In*: CASTILHO, Ricardo. **As Faces do Poder.** Rio de Janeiro: Lumen Juris, 2019. p. 267-288.

SELETRONIC. **O que é screenshot?**. 2018. Disponível em: https://seletronic.com.br/o-que-e-screenshot/. Acesso em: 27 ago. 2019.

SYMANTEC CORPORATION. **Relatório de Crimes Cibernéticos NORTON: O impacto humano.** Divulgação anual. 2018. Disponível em: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf. Acesso em: 15 ago. 2019.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estud. Av.**, São Paulo, v. 30, n. 86, p. 269-285, abr. 2016. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso. Acesso em: 16 ago. 2019. http://dx.doi.org/10.1590/S0103-40142016.00100017.

WALD, A. Um novo direito para a nova economia: os contratos eletrônicos e o código civil. *In*: GRECO, M. A.; MARTINS, I. G. S. (coord.). **Direito e Internet**. São Paulo: Revista dos Tribunais, 2001. p. 9-30.

ZANELLATO, M. A. Condutas Ilícitas na Sociedade Digital. **ESPM-Caderno Jurídico**, São Paulo, n.4, p. 167–230, jul. 2002.