

**CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE
PRUDENTE**

CURSO DE DIREITO

A QUEBRA DO SIGILO TELEFÔNICO NO WHATSAPP

Maria Fernanda de Toledo Pennacchi Tibiriçá Amaral

Presidente Prudente/SP

2018

**CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE
PRUDENTE**

CURSO DE DIREITO

A QUEBRA DO SIGILO TELEFÔNICO NO WHATSAPP

Maria Fernanda de Toledo Pennacchi Tibiriçá Amaral

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção de grau de Bacharel em Direito, sob orientação do Prof. Wilton Boigues Corbalan Tebar.

Presidente Prudente/SP

2018

A QUEBRA DO SIGILO TELEFÔNICO NO WHATSAPP

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

Prof. Wilton Boigues Corbalan Tebar

Prof. Mário Coimbra

Prof. Rodrigo Lemos Arteiro

Presidente Prudente,
03 de dezembro de 2018.

“Para tudo há uma ocasião certa; há um tempo certo para cada propósito debaixo do céu: há tempo de nascer e tempo de morrer, tempo de plantar e tempo de arrancar o que se plantou.”

Eclesiastes 3: 1-2

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por me capacitar e sustentar ao longo dessa jornada. Ao meu orientador Prof. Wilton Boigues Corbalan Tebar, pela paciência, didática, atenção e suporte, por estar sempre disponível a ceder seus conhecimentos e colaborar para o desenvolvimento desse trabalho.

A minha família em especial meu pai, Prof. Dr. Sérgio Tibiriçá Amaral que desde pequena me incentivou a ler e foi fundamental para a confecção desse trabalho monográfico. Aos meus amigos que não nominarei para não ser traída pelo esquecimento. Aos colegas de classe que também estiveram escrevendo, pelo apoio e compreensão.

Um agradecimento especial a minha amiga Beatriz Rebes, que foi uma grande surpresa dessa faculdade, obrigada por sempre estar comigo e por me levar para mais perto do Pai.

A todos os advogados e colaboradores do Escritório Pinheiro e D'arce Pinheiro Advogados Associados, pelo vasto conhecimento a mim oportunizado durante meu estágio e contribuição para meu crescimento profissional, sou eternamente grata.

Sou grata as escreventes Vanessa e Eliana, que me proporcionaram aprender mais sobre o Juizado Especial Cível, bem como Mariellen, Taiane e ao Dr. Michel Feres.

A todos os meus professores, não só os que tive na faculdade mas todos que me acompanharam desde a pré-escola, por transmitirem com paixão, empenho e sabedoria seus conhecimentos sobre os mais diversos temas: os ensinamentos e lições de vida foram fundamentais para minha formação pessoal e profissional.

RESUMO

O presente trabalho tem intuito de explicar como ocorre a quebra do sigilo telefônico no Whatsapp, mostrando que, na verdade, se trata da quebra de dados telefônicos. A quebra do sigilo telefônico só é autorizado por meio de decisão judicial em processo criminal. O estudo visa estender essa autorização aos processos cíveis. Demais disso, procura-se desenvolver uma ferramenta que realize o bloqueio do aplicativo apenas para o usuário que violou o direito. No mais, aborda-se os direitos da personalidade, liberdade de expressão, direito à informação, direito ao esquecimento. Além disso, abordou-se o surgimento da Internet e as consequências para a sociedade, a criação de normas capazes de acompanhar o desenvolvimento da tecnologia e o uso de princípios para a solução dos casos concretos. Utilizou-se, no presente estudo, o método indutivo.

Palavras chave: Quebra do Sigilo Telefônico. Whatsapp. Quebra de Dados Telemáticos. Direitos da Personalidade. Direito ao Esquecimento.

ABSTRACT

The present article has the task to explain how occurs the breach of confidentiality communication in whatsapp, showing, in deed, it's about the breach of datas, o communicantionconfidentialy is only authorized by judicial decision in criminal process. The study intent to extend that authorization to civil process. Foring to develop a toll that make a block of the app only for the user who violate the law. Approach the right of personality, liberty of expression, right of information, oblivion right. The emergence of the internet and the consequences for the society, the creation of rights able to achieve the development of technology and the use of principles to solve the real cases. Use of inductive method.

Key Words: Breach of Telephone Secrecy. Whatsapp. Breach of Telematic Data. Personality Rights. Right to Oblivion.

LISTA DE ABREVIATURA E SILAS

Art.....	Artigo
Arpanet.....	Advanced Research Projects Agent Network
BBB.....	Big Brother Brasil
CF	Constituição Federal
CC	Código Civil
CDA.....	Communication DecenseAct
CP.....	Código Penal
CPC.....	Código de Processo Civil
CPP.....	Código de Processo Penal
DUDH.....	Declaração Universal de Direitos do Homem
FCT.....	Federal Trade Center
HC.....	Habeas Corpus
IBGE.....	Instituto Brasileiro de Geografia e Estatística
IP.....	Internet Protocol
RHC.....	Recurso em Habeas Corpus
SERASA.....	Centralização de Serviços de Banco
SPC.....	Serviço de Proteção ao Crédito
STF.....	Supremo Tribunal Federal
STJ.....	Superior Tribunal de Justiça
ONG	Organização Não-Governamental
ONU.....	Organização das Nações Unidas
UNCITRAL.....	Comissão das Nações Unidas para Direito Comercial Internacional

SUMÁRIO

1 INTRODUÇÃO.....	10
2 INTIMIDADE NA CONSTITUIÇÃO FEDERAL.....	12
2.1 Os Alcances dessa Proteção.....	12
2.2 O Direito à Informação e a Liberdade de Expressão.....	15
2.3 A Internet como Direito Fundamental.....	17
2.4 A Quebra do Sigilo Telefônico.....	20
2.5 A Quebra de Dado Telefônico e Telemáticos.....	22
3 O DIREITO DIGITAL.....	25
3.1 O Surgimento da Internet e suas Implicações Jurídicas.....	27
3.2 A Figura do Whatsapp.....	29
3.3 A Responsabilidade Civil pelo Conteúdo Transmitido na Rede.....	32
3.4 O Marco Civil da Internet.....	34
3.5 A Nova Lei de Proteção aos Dados.....	36
3.6 O Direito Ao Esquecimento.....	37
3.7 Vedação ao Anonimato no Direito Brasileiro.....	40
4 A ONU E AS DISCUSSÕES SOBRE PROGRAMA DE CONTROLE DOS ESTADOS.....	41
5 CONCLUSÕES.....	52
6 REFERÊNCIAS BIBLIOGRÁFICAS.....	54

1 INTRODUÇÃO

O estudo foi desenvolvido com o objetivo de compreender os fenômenos tecnológicos que surgiram juntamente com a internet e suas implicações jurídicas na vida prática da chamada Sociedade da Informação, que nasceu com a rede mundial de computadores, a chamada internet.

O primeiro capítulo trata dos direitos da personalidade (tendo como os mais importantes a intimidade e a privacidade) e as consequências das violações causadas por meio da internet. Dentro de um recorte temático, a liberdade de expressão deve ser priorizada, contudo, sem deixar de lado os direitos da personalidade, que são os limites, visto que a plataforma mundial permite vários programas, postagens e conteúdos, bem como variadas formas de comunicação. O capítulo foi dividido em sub-tópicos para facilitar a compreensão do leitor. Aborda-se nesta apreciação acadêmica, a quebra do sigilo telefônico, da quebra de dados telefônicos onde se insere o Whatsapp que em realidade se trata da quebra de dados telemáticos.

No segundo capítulo narrou-se a respeito do surgimento da Internet e suas evoluções tecnológicas no decorrer dos anos até se chegar a figura do Whatsapp. Destacou-se as responsabilidades de cada indivíduo pela disseminação dos mais distintos conteúdos, em especial as *fake news*. Trouxemos a legislação pátria no tocante ao tema, com o Marco Civil da Internet e a recente Lei de Proteção de Dados para a utilização da rede mundial de computadores nas diferentes esferas de utilização que vão desde compra e venda até redes sociais, passando para outros tipos de informação e comunicação, incluindo sigilo de dados judiciais e bancários, por exemplo. Ainda, buscou-se mostrar que surge um Direito ao Esquecimento que se trata um instituto novo que garante aos usuários que conteúdos a seu respeito sejam removidos da rede, por meio do *habeas data*.

Por fim, discorreu-se sobre o entendimento da Organização das Nações Unidas sobre o que é Internet e quais são os direitos dela decorrentes. A ONU afirma se tratar de um direito humano fundamental, pelo qual, todas as pessoas estão livres para usar a rede como bem entenderem. A pesquisa é bibliográfica em livros, revistas, artigos eletrônicos nacionais e estrangeira, mas também há uma visita aos julgamentos efetivados no Brasil, bem como casos ocorridos em outros países.

Por se tratar de uma temática bastante nova dentro da chamada Sociedade de Informação, a jurisprudência também foi pesquisada, a fim de conhecer os problemas atinentes aos direitos exercitados dentro do referido aplicativo e as possibilidades legais de autorização da busca de informações e de outros tipos de conteúdos que se encontrem no telefone.

O trabalho foi estruturado sob o método dedutivo, pela revisitação da teoria sobre o tema e apresentação de novas premissas a serem confirmadas ao longo do trabalho. O método histórico também foi utilizado para que melhor se compreendesse a evolução tecnológica do direito digital.

2 INTIMIDADE NA CONSTITUIÇÃO FEDERAL

Os Direitos da Personalidade, como os direitos humanos ou fundamentais, tiveram grande importância na Constituição Federal em contraponto com a Liberdade de Expressão e de Informação, após anos de regime militar, no qual existia uma censura institucional. O legislador constituinte buscou garantir todos os direitos relativos à manifestação do pensamento que eram, teoricamente, possíveis ao cidadão, esquecendo-se, porém, que dessa forma legitimaria a sua violação dentro de um regime de liberdade. Neste capítulo abordaremos a temática do ponto de vista constitucional, além das formas de responsabilização dos ofensores, pois embora exista uma liberdade que proíbe uma censura prévia, há necessidade de respeitar os direitos da personalidade, garantir direito de resposta e ainda conhecer o autor das informações, com a vedação ao anonimato.

Tanto que o legislador constituinte criou um capítulo para cuidar da Comunicação Social e ainda colocou os direitos de intimidade, privacidade, honra e imagem no rol de direitos e garantias individuais, que inclusive são “cláusulas pétreas”, assegurando a indenização por dano moral e material, bem como assegurando o direito de resposta. Portanto, são direitos que devem coexistir numa democracia e vai caber ao Poder Judiciário dirimir os conflitos que possam surgir entre os titulares desses direitos em especial na Sociedade de Informação, que democratizou não apenas o acesso à toda a sorte de conteúdo, mas possibilita a criação de site, páginas e ainda a utilização das redes sociais para divulgação.

2.1 O Alcance e os Fundamentos Desta Proteção

A Constituição Federal de 1988 ficou conhecida como a “Constituição Cidadã”, nas palavras do deputado constituinte Ulisses Guimarães, que como jurista e professor de Direito Constitucional, procurou não apenas assegurar os direitos, mas garantir instrumentos judiciais na busca da efetivação. A Lei Maior recebeu dessa denominação devido ao seu formato extremamente garantista e também em razão de contar com um extenso rol de direitos e garantias individuais e coletivas, pois podem ser encontrados nos tratados de direitos humanos ratificados pelo País, que são meramente exemplificativos. Certamente, a Lei Maior foi um reflexo das repressões sofridas durante o regime militar, que foi marcada pela censura dos

veículos de comunicação e total controle dos conteúdos. Por isso, o legislador originário pátrio resolveu por bem garantir a população uma série de direitos considerados fundamentais, entre os quais uma proteção contra o Estado.

Para Paulo Lôbo¹, os chamados direitos da personalidade são aqueles considerados essenciais à pessoa humana e aptos a resguardar a dignidade desta, preservando-a de atentados provocados por outros indivíduos. Por isso, esses direitos da personalidade não consistem apenas em direitos de assegurar e defender direitos, mas de proteger bens como a integridade da pessoa, sua maneira de agir e viver, suas qualidades e atributos, bem como seus defeitos. A defesa é abrangente, pois garante ao ser humano tudo aquilo que lhe é próprio na sua vida: opção sexual, vida familiar, crença, cultura, talento, vocação, intimidade, imagem, identidade, entre outros.

O intuito do legislador foi excelente, mas o que preocupa é a prática, pois esses direitos garantidos na Constituição tem difícil aplicabilidade. Especialmente quando tratamos do direito à intimidade, que com as tecnologias de informação, redes sociais, internet e Whatsapp sofreram mudanças.

No artigo 5º inciso X “são invioláveis a intimidade, a vida privada, a honra e a imagem de pessoas, assegurado o direito a indenização pelo dano material e moral decorrente de sua violação.”

Precisamos compreender do que trata esses institutos protegidos, embora o recorte acadêmico aborde apenas os dois: intimidade e privacidade. Intimidade se refere a vida pessoal do indivíduo com seus amigos e familiares, dentro de sua casa, num ambiente íntimo. Uma coisa é certa: a intimidade é um direito diferente dos direitos à vida privada, à honra e à imagem das pessoas, quando a doutrina os reputava, como manifestação daquela.²

Nessa toada, precisamos saber quem tem esse direito, ou seja, quem são os destinatários dos direitos da personalidade. Pessoas famosas tem direito a intimidade? Evidente que sim, pois podem se relacionar livremente com quem quiserem no âmbito doméstico. Contudo, esse direito é mitigado.

Pessoas que estão constantemente na mídia, acabam por ter esse direito mitigado, os fãs e os chamados “paparazzis” estão sempre seguindo-os para

¹LÔBO, Paulo. **Direito Civil: parte geral**. São Paulo: Saraiva, 2015, p. 93.

² Bittar, Carlos Alberto. **Os direitos da personalidade**. São Paulo: Saraiva, 2014. p.64-65.

saberem com quem se relacionam, os lugares que frequentam. Muitas vezes, eles tem sua intimidade violada.

Há duas correntes doutrinárias que nos ajudam na interpretação: o Regime de Exclusão, que nos permite diminuir o direito de intimidade. A outra parte da doutrina defende A Necessidade de Ponderação que argumenta que nem a intimidade nem a liberdade de expressão são absolutas.

Mas, por outro lado, a casos nos quais as pessoas abrem mão dos direitos da personalidade, como nos programas de televisão como BBB, no qual os participantes se sujeitam a uma vigilância e monitoramento, abrindo mão quando participam dos reality shows. Os participantes negociam direitos em tese irrenunciáveis, distinguindo-se esta da renúncia momentânea e específica quanto ao objeto, transitória quanto ao tempo e revogável a qualquer momento.³

Pessoas que possuem esse direito mitigado, são elas: pessoas cuja atividade afeta o interesse público, por exemplo políticos; pessoa que estão constantemente na mídia, os artistas; fatos que sejam de interesse popular, catástrofes naturais.

Para expor a vida privada de determinada pessoa, é necessário que a notícia seja verdadeira, e tenha relevância pública. Caso de políticos, jogadores de futebol, artistas, cantores e etc.

A Constituição garante a proteção à intimidade, bem como o Código Civil no artigo 12 institui a proteção preventiva, por meio de cautelar ou ordinária para cessar a ameaça ao direito. Há também a modalidade repressiva, onde se resolve por meio de ação de perdas e danos, quando a violação já ocorreu, mas também por ação no Poder Judiciário.

O legislador constituinte, devido ao passado histórico do país, traz a liberdade de expressão como direito fundamental, afim de garantir a imprensa, e aos cidadãos a possibilidade de expressarem-se livremente. É preferível que haja a violação do que se limite a liberdade de expressão.

É preferível que haja a violação do que se limite a liberdade de expressão previamente, embora isso possa acontecer em casos bastante especiais por ordem do Poder Judiciário.

³ Venosa, Silvio Salvo. **Direito Civil: parte geral**. São Paulo: 6 ed.2006. p. 174.

Há conflitos que geram grande repercussão nacional, e até internacional, como foi o caso do ex participante do programa Big Brother Brasil que ficou conhecido como “Daniel Estuprador” ele foi indevidamente acusado de estupro e posteriormente foi absolvido, contudo, até hoje encontramos fotos do rapaz vinculadas ao episódio, inclusive em sites internacionais.

É garantido o direito de retratação, onde uma informação equivocada pode ser respondida pela pessoa que se sentir violada, no mesmo meio que foi vinculado. No entanto, uma vez divulgada, não há mais controle, por mais que a informação seja infundada a pessoa fica relacionada ao fato.

Por isso, há que se discutir o direito ao esquecimento, ou seja a retirada daquelas informações dos meios informativos.

O direito à privacidade está ligado ao núcleo familiar do indivíduo, pressupõe a autonomia do sujeito, visto que, restrições não são toleradas. Para justificar a exposição da privacidade da pessoa, é necessário que haja relevância, no entanto é cabível indenização por danos morais e materiais.

Lembramos que a pessoa jurídica pode ter sua imagem violada, e por isso o Superior Tribunal de Justiça editou a súmula nº 227 que permite a incidência de dano moral a pessoa jurídica.

Além da legislação brasileira, o Brasil é signatário do Pacto de San Jose da Costa Rica, que estabelece a proteção aos direitos da personalidade em nível regional e tratados das Nações Unidas que asseguram esses mesmos direitos em nível global.

2.2 O Direito à Informação e a Liberdade de Expressão

O Direito à informação se divide em: direito de informar, de se informar e de ser informado. O direito de informar garante o fluxo livre informações sem a interferência estatal, mas há ainda nas lições de Vidal Serrano Nunes Júnior e Luiz Alberto David Araujo⁴ o direito positivo de informar, chamado de “direito de antena”, que garante os meios como o fornecidos aos partidos políticos na propaganda eleitoral gratuita e na propaganda política partidária. A diferença entre elas é que a

⁴Araujo, Luiz Alberto David. Nunes Júnior, Vidal Serrano, **Curso de Direito Constitucional**. São Paulo: Verbatim, 22ª edição, 2018. p.34

primeira divulga os candidatos e visa assegurar os votos, enquanto que a propaganda política partidária tem como principal objetivo a divulgação da plataforma do partido.

No direito de se informar, o indivíduo busca informações de seu interesse através de pesquisas, um instituto interessante relacionado a esse direito é o *habeas data* (banco de dados público que permite à população ter acesso a informações a seu respeito). O direito de ser informado é exclusivo do Estado que tem o dever de informar a população sobre matéria de interesse público. No entanto, os órgãos que exercem funções públicas também devem informar pelo princípio da transparência, como as empresas paraestatais, por exemplo.

Após a ditadura militar a liberdade de expressão ganhou grande relevância, foram muitos anos de censura até finalmente o povo poder se expressar livremente. A internet impulsionou o exercício desse direito.

É certo que a Constituição protege a liberdade de expressão, contudo deve ser feita de forma ética, legal e responsável. O consumidor ao fazer uma reclamação de determinada empresa na Internet precisa ser coerente, em caso de difamação irá responder por eventuais danos por ele ocasionados.

O ordenamento brasileiro tem prezado pela liberdade de expressão em detrimento dos direitos da personalidade. Nos casos de violação, resolver-se-á por perdas e danos na esfera judicial.

A liberdade de Imprensa é destinada aos profissionais de imprensa, jornalista, radialistas e comunicadores, enquanto que a liberdade de expressão é mais ampla e pertence à todas pessoas, pelos mais diversos meios ou veículos, como música, poesia, teatro, literatura e outros.

A internet intensificou e garantiu a liberdade de expressão, na rede as pessoas podem compartilhar seus pensamentos e ideias, contudo enfrentamos uma questão importante que é o anonimato.

O anonimato é vedado pela Constituição Federal. Porém através da internet é muito difícil identificar o autor de determinadas postagens, por vezes é possível localizar o IP mas impossível saber com precisão quem foi o autor da postagem.

Além disso, por traz do anonimato se escondem pessoas que usam a rede para praticar crimes cibernéticos, desde fraude, roubo de dados, *cyberbullyng*,

pedofilia entre outros. Muitas vezes o usuário abusa da chamada liberdade de expressão para cometer insultos e praticar delitos.

É certo que no Brasil é preferível que se cometa o delito do que seja cerceada a liberdade de expressão, pois tudo se resolve em perdas e danos. No entanto, essa política é nociva, pois sabendo disso os criminosos se aproveitam de um direito constitucional para prática de crimes.

2.3 A Internet como Direito Fundamental

De acordo com Organização das Nações Unidas, por meio da Resolução A/HRC/32/L.20, de 26 de junho de 2016, formulada pelo Conselho de Segurança da ONU foi aprovado por 55 países membros, a internet é considerada um direito fundamental e o seu bloqueio é um crime contra a humanidade.

Um dos objetivos da Resolução é contribuir para o desenvolvimento sustentável e disseminação da informação e comunicação e tecnologia para o avanço do progresso humano.

A privacidade é um tema debatido exaustivamente, principalmente após o vazamento de dados confidenciais do caso de espionagem do site Wikileaks, cujo o proprietário, Edward Snowden, se encontra exilado na embaixada do Equador em Londres há 4 anos. Esse caso trouxe à tona a preocupação com a privacidade nas redes sociais.

O principal problema hoje é quanto ao controle dos dados divulgados na rede, pois muitos crimes são cometidos anonimamente o que é expressamente vedado pela Constituição brasileira.

A Organização das Nações Unidas condena os países que bloqueiam a internet de seus cidadãos pois trata-se de um direito humano fundamental. Recentemente o governo francês de Manoel Macron proibiu o uso de celulares nas escolas públicas francesas, contudo essa medida não é passível de condenação pela ONU, pois visa o desenvolvimentos dos alunos e sua atenção em sala de aula.

Segundo a jurisprudência estadunidense, no Caso US Telecom Association vs. Federal Communications Commission⁵, fica proibida aos provedores

⁵ Case US Telecom Association vs. Federal Communication Commission Disponível em: <https://casetext.com/case/us-telecom-assn-v-fed-commcns-commn->

de internet banda larga e móvel, a restrição de conteúdo a sites legais nem aplicativos de mensagens, vídeos como o Whatsapp.

No Brasil, os Tribunais tem caminhado no mesmo sentido, inclusive condenando empresas de telefonia móvel por bloquear os serviços de internet móvel dos usuários quando acabava a franquia contratada. Como alternativa, foi sugerido que se diminuísse a velocidade da internet.

Ainda tratando da jurisprudência pátria, é possível observar sentenças que bloquearam o uso do aplicativo Whatsapp em todo o Brasil, devido a investigações de cunho criminal.

Ao julgar dois mandados de segurança, o desembargador Raimundo Nonato da Costa Alencar, entendeu que a decisão do juiz de primeiro grau foi desproporcional e irrazoável porque atinge um número indeterminado de pessoas, as quais não cometeram qualquer ilícito.

Buscamos encontrar meios adequados para punir os responsáveis. O caso em testilha, trata de uma determinação de bloqueio do aplicativo em razão de uma investigação criminal de tráfico de drogas. Contudo, o Tribunal concedeu a liminar afim de suspender o bloqueio do aplicativo.

Uma maneira de solucionar a situação seria desenvolver um mecanismo capaz de bloquear o acesso ao aplicativo apenas dos envolvidos na situação, sem prejudicar toda a coletividade.

Outro caso envolvendo a jurisprudência estadunidense refere-se a: 18 cidadãos apresentaram uma queixa contra a empresa Carrier IQ que era provedora do software usado por eles, porém os dados foram interceptados pela Ré.

“Os autores alegam que os dados interceptados pelo software Carrier IQ incluem: (1) URLs (incluindo aquelas que contêm strings de consulta com informações incorporadas, como termos de pesquisa, nomes de usuário, senhas e informações de localização geográfica com base em GPS); (2) informação de localização GPS; (3) mensagens de texto SMS; (4) números de telefone discados e recebidos; (5) o teclado do usuário pressiona / pressionamentos de tecla; e (6) compras e usos de aplicativos. *Identidade*. ¶ 65. Essas informações são interceptadas como parte das “chamadas” do software Carrier IQ no sistema operacional do dispositivo para “métricas” *Id. Identidade*. Em seguida, armazena as informações no Móvel memória RAM do dispositivo em uma base contínua.”⁶

[3?q=whatsapp%20and%20blocking&p=1&tab=keyword&jxs=&sort=relevance&type=case](https://casetext.com/case/in-re-carrier-iq-inc-3?q=whatsapp%20and%20blocking&p=1&tab=keyword&jxs=&sort=relevance&type=case) Acesso em: 07 de agosto de 2018.

⁶*In re Carrier Iq, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015). Disponível em: <https://casetext.com/case/in-re-carrier-iq-inc->

Esta interceptação de dados representa um sério risco ao consumidor, pois quando se tem conhecimento de que os dados foram interceptados talvez seja tarde demais, porque os dados podem ser usados para fins ilícitos.

Recentemente, o Facebook foi investigado pela FTC – *Federal Trade Commission* – Comissão do Comércio. O que ocorria era que ao criar um perfil na rede social você concordava com os termos de uso, e nele constava uma cláusula que autorizava a concessão de dados pessoais dos usuários para sites e aplicativos parceiros do Facebook.

Em meados de 2015, o pesquisador Aleksander Kogan realizou um teste de personalidade que foi realizado por cerca de 270 mil usuários, acessando assim 50 milhões de dados. Até aqui, não havia nenhuma violação as políticas de privacidade dos usuários, pois ele é parceiro do Facebook.

Entretanto, Kogan liberou esses dados para a Cambridge Analytics, empresa britânica de análise de dados, que está diretamente ligada a campanha de Donald Trump para a Casa Branca, os dados obtidos por Kogan foram usados para criar estratégias de comunicação e influência nas redes sociais.⁷

Apesar de o entendimento quanto a natureza jurídica de direito fundamental, estamos longe de garantir a efetivação desse direito. Há diversas políticas públicas de WI-FI grátis em praças e parques públicos, no entanto é necessário que o usuário tenha um aparelho celular ou notebook o que dificulta o acesso à internet.

É preciso alcançar determinadas populações que se encontram afastadas e se quer possuem energia elétrica, esgoto encanado, acesso à saúde e educação, quem dirá à Internet.

Na Sibéria, um dos lugares mais ermos e remotos do mundo, a população Nanet, povo indígena natural da Sibéria, possui acesso à Internet, apesar das temperaturas congelantes, devido a uma empresa de energia que fazia pesquisa na área foram instaladas torres de transmissão de sinal telefônico, por isso, o povo Nanet goza desse direito fundamental, desde que possuam aparelho eletrônico.

[10?q=mobile%20app%20&p=1&tab=keyword&jxs=&sort=relevance&type=case](https://www.ftc.gov/press-release/2015/08/10?q=mobile%20app%20&p=1&tab=keyword&jxs=&sort=relevance&type=case) Acesso em: 07 de agosto de 2018.

⁷ Crise no Facebook: vazamento de dados para a Cambridge Analytics. Disponível em: <https://marketingdeconteudo.com/facebook-vazamento-de-dados/> Acesso em 07 de agosto de 2018.

Há uma série de medidas que devem ser adotadas para efetivação do acesso à internet. Entre elas, a instalação de torres de transmissão de sinal, em locais remotos do país como o Norte e Nordeste, que são as áreas que tem o menor percentual de acesso à Internet nos lares.

Há países em que acesso à Internet é extremamente restrito, como por exemplo China, Coréia do Norte e Cuba. Na China, a rede social Facebook é bloqueada, eles possuem seus próprios canais de comunicação que são fiscalizados pelo governo. Na Coréia do Norte a população civil sequer tem acesso a Rede. Em Cuba recentemente foi liberado o acesso à Internet, contudo é bem restrito e passa por “vistoria” do Governo a fim de garantir que não haja reclamações sobre o regime comunista vigente.

A Comissão Interamericana de Direitos Humanos com sede em Washington-DC, Estados Unidos da América tem como principal meio de acesso as informações a respeito de Cuba através da plataforma Twitter.

É de competência da Comissão a elaboração de Recomendações sobre a situação humanitária nos países membros da OEA. A maioria dos países acatam essas recomendações obedecendo as imposições da Comissão. Contudo, não é o caso de Cuba que não assinou nem ratificou o Pacto de San Jose da Costa Rica.

2.4 A Quebra do Sigilo Telefônico

A Constituição brasileira, em seu artigo 5º, XII, aduz: é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Observa-se que é preciso três requisitos para que haja a interceptação telefônica, quais sejam, ordem judicial, advinda de juiz competente, para fins de investigação criminal ou instrução processual penal e nas hipóteses da lei. Os direitos fundamentais não são absolutos e por isso, presentes os requisitos da Lei Maior nasce a possibilidade de mitigação da privacidade e da intimidade autorizadas pelo Poder Judiciário.

O fato da interceptação somente ser autorizada em processo penal no Poder Judiciário, não impede que seja utilizada como prova emprestada no processo civil, administrativo, disciplinar, político-administrativo.

É importante definirmos em que consiste a quebra do sigilo telefônico, é a captação e gravação de uma conversa telefônica no momento em que ela se verifica, por uma terceira pessoa e sem a cognição dos interlocutores.

A proteção que garante a inviolabilidade de correspondência e comunicações em geral, também assiste o armazenamento e transmissão de informações decorrentes da informática. Como é o caso do Whatsapp, que é um aplicativo que surgiu com a internet e ganhou uma utilização como veículo de fácil e rápida comunicação digital.

Além disso, há que distinguir a proteção aos dados telefônicos. Nele está incluso o sigilo bancário e fiscal. Essas informações são uma modalidade de correspondência, o seu sigilo somente será quebrada nas hipóteses legais, como por exemplo em uma Comissão Parlamentar de Inquérito ou por ordem judicial.

O Ministro Celso de Mello no julgamento do *habeas corpus* 90.050-6/RJ, STF, 2ª turma, decisão 10-6-2008, afirmou:

A transgressão, pelo Poder Público, ainda que em sede de fiscalização tributária, das restrições e das garantias constitucionalmente estabelecidas em favor do contribuintes (e de terceiro) culmina por gerar ilicitude da prova eventualmente obtida no curso das diligências estatais, o que provoca, como direta consequência desse gesto de infidelidade às limitações impostas pela Lei Fundamental, a própria inadmissibilidade processual dos elementos probatórios assim coligidos⁸

Fica claro que a quebra de dados configura um violação ao direito à privacidade e à intimidade, que são direitos fundamentais e fazem parte de uma esfera que o Estado precisa de justificativa para invadir. A intimidade não deve ser violado, pois a publicidade de dados pode ferir a dignidade do ser humano, revelando dados que fazem parte de um direito protegido pela Lei Maior e também pelos tratados internacionais de direitos humanos no âmbito da Organização das Nações Unidas e da Organização dos Estados Americanos. Publicada de forma incorreta e sem a devida autorização do Poder Judiciário, há uma grave violação dos direitos da personalidade, uma vez que tal intromissão dos direitos do indivíduo só

⁸HC 90.050-6/RJ – STF 2ª turma. Relator: Ministro Celso de Mello. Brasília, 10 de junho de 2008.

pode acontecer em casos muito especiais e dentro de limites estabelecidos pela Constituição e pelos tratados de Direitos Humanos que o Brasil é signatário.

Contudo, é preferível que se permitam essas violações aos direitos da personalidade ao cerceamento da liberdade de expressão, visto que, é possível resolver em perdas e danos.

2.5 A Quebra de Dados Telefônicos e Telemáticos

A quebra de dados telefônicos é classificada em três aspectos, quais sejam: dados públicos que são acessíveis a população em geral, dados sigilosos de primeiro grau, que são acessados por requisição da autoridade administrativa competente, e dados sigilosos de segundo grau que exigem uma ordem judicial.

O capítulo da comunicação social prevê normas sobre essa questão, bem como outros dispositivos na Lei Maior e também nos tratados de direitos humanos em nível de Nações Unidas e Organização dos Estados Americanos.

O Código de Processo Penal dispõe sobre o assunto:

Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.⁹

Portanto o objetivo do referido dispositivo é proteger a vida humana diante da ocorrência do grave crime que é o tráfico humano.

Já quanto aos dados telefônicos quando apreendidos em prisão em flagrante ou por busca e apreensão domiciliar, o delegado de polícia pode usufruir do poder requisitório para acessar os dados.

Quanto aos dados telemáticos (combinação de telecomunicação e informática) há uma polêmica em torno do assunto, pois o Marco Civil da Internet foi mais restritivo. Segundo a Constituição a autoridade poderia acessar os dados sem ordem judicial, contudo a legislação complementar estabeleceu uma cláusula de reserva de jurisdição para mensagens eletrônicas e registros de conexão à internet.

⁹ Artigo 13-B do Código de Processo Penal.

Os dados obtidos através da busca e apreensão domiciliar, o próprio mandado judicial soluciona o problema, garantindo o acesso as informações. Quanto aos decorrentes de prisão em flagrante a doutrina diverge¹⁰.

Uma parte entende que é dispensável a autorização judicial pois é dever da polícia investigar o acusado, além do mais ele poderia apagar os dados comprometendo e a investigação, o acesso pela polícia não torna o dado público pois permanece no sigilo da investigação.

Outra corrente defende que é imprescindível a autorização judicial pois ao acessar o e-mail, Whatsapp, SMS, e sites visitados pelo indivíduo pois envolvem o direito probatório de terceira dimensão. O e-mail exige autorização judicial conforme dispõe o Marco Civil da Internet. Assim, por analogia, e por se tratar de mecanismos similares, compreendemos que o mesmo se aplica ao Whatsapp.

É preciso compreender o que se entende por direito probatório de terceira dimensão, refere-se a meios probatórios invasivos e que dispõe de alta tecnologia que não está à disposição da população em geral, e admitem encontrar resultados que não seriam possíveis pelos meios convencionais.

Assim, concluímos que todas as vezes que as autoridades utilizarem meios tecnológicos inacessíveis ao público em geral é necessário que expeça-se uma autorização judicial para que haja a interceptação.

No julgamento do RHC 31.531/RO o Superior Tribunal de Justiça entendeu que é nulo o acesso aos dados telefônicos e as conversas de Whatsapp sem ordem judicial porque viola o direito à intimidade e privacidade do indivíduo. O Ministro Néfi Cordeiro em seu voto afirmou:

“Nas conversas mantidas pelo programa Whatsapp, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva interceptação inautorizada de comunicações. É situação similar às conversas mantidas por e-mail, onde para o acesso tem-se igualmente exigido a prévia ordem judicial.”¹¹

Hoje o aparelho celular não se destina apenas a receber ligações telefônicas mas também acesso a mensagens eletrônicas, e-mail, e outros aplicativos que possibilitam a troca de dados.

¹⁰ MORAES, Alexandre de. **Direito Constitucional**. 29. Ed. – São Paulo: Atlas, 2013.

¹¹ BRASIL. Superior Tribunal de Justiça. Processual Penal. *Habeas Corpus*. Tráfico de drogas. Recurso em *Habeas Corpus* nº 31.531/RO da 6ª turma do Superior Tribunal de Justiça do estado de Rondônia, Brasília, DF, 19 de abril de 2016. RT vol. 970 p. 461

No crime de sequestro, entretanto, é perfeitamente possível o acesso aos dados telefônicos e telemáticos pois a gravidade do delito exige uma ação rápida da polícia que pode ser crucial para a solução do caso. Por se tratar de um crime permanente é perfeitamente admitido pela doutrina essa flexibilização do direito a intimidade e a privacidade.

Questionamos até onde vai o poder investigatório do delegado de polícia, e porque ele suprime os direitos da personalidade em alguns de seus aspectos fundamentais quando confrontados com determinados crimes, como sequestro, tráfico de drogas e pedofilia.

Porque essa supressão geralmente está vinculada ao direito penal. Isto é, nos crimes; no âmbito cível essa máxima não se aplica. Contudo, muitas vezes os reflexos dos crimes na seara cível permitem uma supressão dos direitos da personalidade por se resolverem facilmente por perdas e danos.

Posto isso, trazemos uma nova teoria, de que a quebra do sigilo telefônicos bem como dos dados telemáticos deveriam ser possíveis no juízo cível, levando em conta a gravidade do crime, autorização do juiz e os demais requisitos exigidos pela lei no âmbito penal.

Caso contrário, estaríamos diante de uma injustiça: seria afirmar que o juízo criminal é mais “importante” que o juízo cível. É verdade que a gravidade dos crimes cometidos na esfera penal é maior que na esfera cível. Contudo, isto abriria um precedente sem tamanho para uma insegurança jurídica.

Os delitos ocorrem, e cabe aos operadores do direito trazerem soluções para essas problemáticas. Assim, é perfeitamente admissível a quebra dos dados telefônicos e telemáticos no juízo cível, quando o magistrado compreender necessário para a segurança da investigação e efetiva aplicação da lei.

3 O DIREITO DIGITAL

Neste capítulo abordou-se desde o surgimento da Internet, suas mudanças até o surgimento de aplicativos para smartphones como o Whatsapp, e as reviravoltas tecnológicas proporcionados por ele.

O chamado Direito Digital surge com a rede mundial de computadores, pois a Internet permite um enfoque novo para o direito, que nasce na tentativa de dar respostas dentro do ordenamento jurídico constitucional e do internacional a um fenômeno social que se concretizou nos últimos anos.

Para De La Calle Restrepo¹², a magnitude do fenômeno informático que as tecnologias e os computadores incidiram praticamente em todos os planos da vida moderna, produzindo, inclusive, modificações de raiz no comportamento cultural das sociedades, proporcionando o nascimento de uma nova era.

Para estudo do Direito Digital é preciso conhecer sobre o funcionamento do sistema e também os vários tipos de participantes.

Horácio Fernández Delpech estabelece que os participantes formam grupos, utilizando dos Estados Unidos da América do Norte: a) usuários individuais; b) provedores de conteúdo; c) provedores de serviço e d) provedores de rede¹³. Existem outras possíveis classificações que podem colaborar com esse estudo: 1) provedor de acesso; 2) provedor de conteúdo; 3) provedor hospedeiro ou de *hosting* e 4) usuário.¹⁴

Os usuários denominados de “*users*” pelos norte-americanos são todas as pessoas que por meio de computador, por meio de um provedor de serviços e mediante uma conexão, acessam a página de um site da rede para recolher a informação colocada ali pelos provedores de conteúdo. São pessoas difusamente espalhadas pelo planeta, pois mesmo antes da internet, a informação era considerada um bem ou interesse difuso¹⁵. José de Oliveira Ascensão faz uma

¹² DE LA CALLE RESTREPO, José Miguel. **Autodeterminacion informativa y habeas data em Colombia – Análisis de La Ley 1266**. Bogotá: Temis, 2008. p.22.

¹³ DELPECH, Horacio Fernández. **Internet: sua problemática jurídica**; Buenos Aires: Abeledo-Perrot, 2008 p.19.

¹⁴ AMARAL, Sérgio Tibiriçá. O Direito a Informação na TV, a Convenção das pessoas com deficiência e 9 *closed caption*. In: Dirceu Pereira Siqueira; José Roberto Anselmo. (Org.). **Estudos sobre os Direitos Fundamentais e Inclusão Social**. 1 ed. Birigui: Boreal, 2010, p. 336-352., p 407.

¹⁵ CARVALHO, Luis Gustavo Grandinetti Castanho de. **Direito de informação e liberdade de expressão**. Imprensa: Rio de Janeiro, Renovar, 1999.

abordagem importante sobre os participantes, chamando o usuário de navegante, principalmente quando faz uso dos sites de busca¹⁶.

Os provedores são empresas que prestam um tipo de serviço pelo qual se permite uma conexão com a Internet ou ainda outros serviços, como a hospedagem dos conteúdos. São aqueles que oferecem informação por meio de uma página ou sítio. Os autores, editores e demais titulares das mais diversas manifestações coletam, mantêm e organizam todo o tipo de informações em uma página ou sítio na rede, da qual provem a informação, a fim de que ela possa ser lida por qualquer usuário da internet que ingresse nessa página ou sítio. Os provedores de conteúdo coletam, mantêm, processam e organizam informações para acesso “on-line”.

Os exemplos no Brasil são a Globo.com e a UOL, que colocam à disposição do usuário notícias, vídeos, música, entretenimento, serviço de e-mail e outros. Há conteúdos gratuitos e outros que são restritos aos assinantes.

Carla Rodrigues Araújo Castro diz que os provedores são instituições que se conectam na Internet via um ou mais acessos dedicados e disponibilizam acesso a terceiros a partir de suas instalações¹⁷. Estas empresas podem cobrar ou não por esses serviços ou conteúdo.

Patrícia Peck, por sua vez, afirma que se trata de uma empresa que presta serviços de conexão à Internet e de serviços de valor adicionado como hospedagem, que detém ou utiliza uma determinada tecnologia, linhas de telefone e troncos de telecomunicação próprios ou de terceiros¹⁸.

Necessário diferenciar os demais provedores. Os de conteúdo são páginas ou mesmo sítios que podem ser alcançados pelos usuários como WWW.estadao.com.br. Todavia, há casos de pagamentos prévios ou necessidade de uma chave de acesso (*password*).

O provedor de conteúdo é diferente, portanto, do provedor de serviço, que no idioma inglês são os ISPS (*internet servisse providers*). Essa é a denominação comum para dois tipos de sujeitos que possibilitam a conexão entre o usuário e o provedor: a) provedores de acesso e b) provedores de alojamento ou

¹⁶ ASCENSÃO, José de Oliveira. *Hyperlinks, Frames, Metatags – A Segunda Geração de Referências na Internet* <in> **Estudos Sobre Direito da Internet e da Sociedade da Informação**. São Paulo: Almedina, 2001. p. 208.

¹⁷ CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2001. p. 68.

¹⁸ PECK, Patrícia. **Direito digital**. São Paulo: Saraiva, 2002.p. 52.

armazenamento. Alguns autores afirmam que são ambos provedores de acesso, pois são atividades de meio, uma intermediação entre os usuários e a rede. É um típico contrato de prestação de serviços, pois o provedor oferece serviços de conexão de rede de forma individualizada e intransferível para um ou vários usuários num ou em vários locais. O usuário, por sua vez, se responsabiliza pelos conteúdos dos seus e-mails.

Os provedores de acesso (IAP – Internet Access Providers) oferecem aos seus usuários individuais serviços de conexão com a internet, através de um servidor de grande potência que está conectado à rede, a fim de que o usuário possa alcançar os diferentes sítios. Trata-se de uma atividade meio, ou seja, um serviço de intermediação entre o usuário e a rede. Uma prestação de serviço pela qual o usuário paga pela utilização ou recebe de graça. São uma instituição que se liga à Internet, via um Ponto-de-Presença ou outro provedor, para obter conectividade IP¹⁹ e repassá-la a outros indivíduos e instituições, em caráter comercial ou não²⁰. O provedor de acesso torna possível ao usuário a conexão à rede por meio de telefone ou outro meio.

O Direito Digital busca tratar de boa parte dessa relação na rede, seguindo os princípios da Constituição bem como os Tratados Internacionais.

3.1 O Surgimento da Internet e Suas Implicações Jurídicas

O surgimento da internet se deu durante a guerra fria nos Estados Unidos da América do Norte, na Universidade da Califórnia. Pesquisadores, afim de evitar os ataques nucleares russos, desenvolveram um sistema de telecomunicações que funcionava por redes locais chamadas de LAM, posicionadas estrategicamente e interligadas pela rede de telecomunicação geográfica WAN.

Esse projeto foi chamada de Arpanet (AdvancedResearchProjects Agent Network) e se limitava a prestar serviços as universidades que desenvolviam pesquisas militares e instituições ligadas a elas. Posteriormente outras empresas

¹⁹ Internet Protocol – Protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na rede. TCP/IP é o protocolo para comunicação entre computadores. Tornou-se o padrão de fato para a transmissão por meio de redes, incluindo a Internet.

²⁰ PECK PINHEIRO, Patrícia. Direito Digital, p.369.

apareceram e passaram a fornecer o serviço para universitários, comerciantes e enfim a população mundial em geral.

A partir da década de 90, com o avanço da internet e do direito digital, a facilidade de acesso à conteúdos e informações de outros países, inclusive, se tornou uma realidade. Rapidamente essa tecnologia se espalhou pelo mundo, e atualmente é muito raro, lugares em que não há acesso à internet.

Hoje em dia, há doutrinadores que defendem a internet como um direito fundamental. Contudo, é preciso analisar as implicações que essa afirmação tem no caso concreto. O Estado se torna responsável por disponibilizar vias de acesso à internet, como rede Wi-Fi gratuita e de qualidade.

Com tantos problemas sérios existentes no país, seria plausível falarmos em investimentos que forneçam a população o acesso gratuito à internet? Em muitas cidades encontramos praças com postos para se conectar à rede. Contudo é precipitado dizer que é um direito fundamental. A despeito da Organização das Nações Unidas trazerem o direito à Internet como um direito fundamental, é preciso cautela quanto a temática, devido a necessidade se garantir outros direitos em tese mais importantes dada as carências da população.

Segundo o IBGE há cerca de 116 milhões de brasileiros conectados à internet, 64,7% tem idade superior a 10 anos. O celular é o principal meio de acesso à rede, em 2016, 94,6% dos brasileiros usavam celulares para se conectar.

O Brasil é o quarto país que mais possui pessoas conectadas, contudo se compararmos com o México por exemplo, temos quase o mesmo percentual, contudo a população mexicana é inferior. Portanto, apesar do crescimento, há muito o que se fazer para que as classes menos favorecidas obtenham meios para acessar a internet.

No cenário atual, seria impossível vivermos sem a internet, ele está em quase tudo que fazemos, desde o pagamento no cartão de crédito até o uso do sistema GPS. Por isso, a defesa da internet como direito fundamental do cidadão ganha força.

O direito digital não um novo ramo do direito, é apenas o nome dado as demais áreas do direito que se dedicam a estudar as mudanças que Internet ocasionou. A legislação não consegue acompanhar as mudanças que ocorrem no mundo virtual, portanto, tudo que venha a tratar de direito digital deve ser abordado de forma genérica para que possa sobreviver as transformações.

Os princípios devem prevalecer diante das regras, pois uma regra poderia ser inadequada em determinado momento devido a rápida evolução legislativa.

Nos Estados Unidos da América do Norte, uma prática comum e célere é a Arbitragem, se valendo da normas de Direito Consuetudinário, princípios como: a generalidade, continuidade, publicidade, durabilidade e uniformidade são essenciais para tomada de decisão.

Trata-se de uma solução alternativa de controvérsias, marcada pela rapidez e eficiência, advindas das terras americanas. Patricia Peck Pinheiro, em seu livro Direito Digital, preleciona:

Pelos motivos expostos acima, reiteramos que o Direito Digital não se limita a Internet, sendo a própria evolução do Direito onde a Internet é um novo recurso que deve ser juridicamente atendido, como todas as outras inovações que estejam por vir. Em tal realidade, o maior compromisso do Direito Digital é evitar qualquer tipo de arbitrariedade²¹

A Internet revolucionou a sociedade como um todo, desde as relações comerciais, o surgimento de crimes praticados pela rede e a incógnita do anonimato, tendo implicações relevantes no Direito. Fazendo os princípios se sobreporem as regras quando se trata da temática do Direito Digital. Bem, surge um novo ramo do direito que envolve não apenas os conteúdos postados na rede, mas o próprio funcionamento da rede mundial de computadores, incluindo as redes sociais.

3.2 A Figura do Whatsapp

Os telefones móveis e celulares foram recebendo funções e também ganhando programas com funções diversas, que vão desde fazer filmagens, armazenar imagens, como outros que fornecem mapas e rotas de trânsito. Whatsapp é um aplicativo de mensagem que foi desenvolvido em 2009 por dois veteranos do Yahoo, por Brian Acton e Jan Koum, na cidade de Santa Clara, Califórnia.²²

O aplicativo oferece troca instantânea de mensagens escritas, chamadas de voz, envio de fotos, vídeos e documentos em PDF, tudo isso

²¹ Pinheiro, Patricia Peck. Direito Digital. 2008, p. 34

²² Site oficial do Whatsapp. Disponível em: <https://www.whatsapp.com/about/> Acesso em: 07 de agosto de 2018.

gratuitamente. O aplicativo surgiu para competir no mercado asiático buscando facilitar o processo de comunicação pessoal, inclusive por meio de grupos.

Hoje, a ferramenta é utilizada em nada menos que 120 países, e foi a primeira a atingir a marca de 1 bilhão de usuários. Os números são significativos, e instituem uma nova dimensão na era digital nesse processo comunicativo de pessoa para pessoa e dentro de grupos.

Em 2013, Mark Zuckemberg o criador do Facebook comprou a franquia do Whatsapp, visando aumentar o número de usuários ele fez declarações nas quais garante o máximo sigilo e proteção aos usuários, através de mensagens criptografadas²³

A criptografia é uma forma de proteger documentos, arquivos, sistemas. Consiste em uma chave criptográfica que pode ter de 40, 64, 80, 112, 384 bits e até mais. Quanto maior for a chave mais segura ela é. Nos Estados Unidos a criptografia é considerada uma arma, sendo que sua exportação era proibida. Após uma intensa luta judicial, o engenheiro Philip Zimmermann conseguiu exportar seu software *pretty good privacy*, mas por um programa que utilizava uma chave de 40 bits. Que pode ser facilmente decodificada.

A questão desse sigilo foi discutida em algumas ações judiciais no Brasil. Quando a Justiça do Estado do Piauí investigava um caso de pedofilia, solicitou à empresa que desse acesso as conversas de determinada pessoa, que era suspeita dos abusos com as crianças e adolescentes. Apesar da ordem judicial, a empresa se negou a fornecer os dados. A alegação da direção da empresa foi de que o aplicativo é criptografado e nem mesmo a empresa não tem acesso a esses dados.

A justiça piauiense, por sua vez, determinou o bloqueio do aplicativo em todo território nacional, decisão essa reformado pelo Tribunal de Justiça do Piauí por afrontar a coletividade.

Essa decisão não é um caso isolado, pois em outras investigações criminais a justiça brasileira determinou o bloqueio do aplicativo, inclusive instituindo pena de multa pelo descumprimento.

Atualmente, busca-se formas de acessar os dados do réu sem prejudicar a coletividade. Muitas empresas usam o aplicativo para contatar clientes,

²³ Wikipédia, a enciclopédia livre, Whatsapp. Disponível em: <https://pt.wikipedia.org/wiki/WhatsApp>
Acesso em: 07 de agosto de 2018.

portanto o bloqueio do dispositivo afeta não só a vida particular do indivíduo, mas também uma série de empresas que fazem uso da ferramenta.

Com fulcro no artigo 12 incisos III e IV do Marco Civil da Internet, os juízes baseiam a decisão de suspensão temporária do aplicativo, devido a não colaboração da empresa com as investigações criminais, como uma forma de punição.

Artigo 12: Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Fica claro que a decisão judicial possui base legal no ordenamento pátrio, contudo não parece razoável tal entendimento, uma vez que prejudica toda a coletividade que nada tem a ver com o crime praticado por terceiro.

Senão vejamos alguns julgados nesse sentido: mandado de segurança nº 2015.0001.001592-4 (0013872-87.2014.8.18.0140):

Tratam-se de dois mandados de segurança, com pedido de liminar, impetrados por Global Village Telecom S.A., Empresa Brasileira de Telecomunicações S.A. (Embratel) e Claro S.A. contra ato do Juiz de Direito da Central de Inquérito de Teresina, o qual determinou que os diretores das impetrantes que, no prazo de vinte e quatro hora, **suspendesse em todo território nacional, até o cumprimento da ordem judicial** proferida no processo nº 0013872-87.2014.8.18.0140, o tráfego de dados por meio aos domínios whatsapp.net e whatsapp.com, bem como todos os seus subdomínios e todos os outros domínios que contenham whatsapp.net e whatsapp.com em seus nomes²⁴

Como resta claro, o juiz piauiense entendeu que a investigação criminal no caso de pedofilia sobrepunha o direito à liberdade de expressão dos demais usuários do aplicativo. O tema é bastante polêmico principalmente pelo alcance da medida protetiva.

Contudo não foi esse o entendimento dos desembargadores Raimundo Nonato da Costa Alencar:

²⁴ BRASIL. Tribunal de Justiça do Piauí. Mandado de Segurança nº 0013872-87.2014.8.18.0140. Juiz de direito, Central de Inquérito de Teresina – PI.

Desproporcional e irrazoável (sic), assim, a sanção aplicada pelo magistrado, pois, além de atingir um número inestimável de cidadãos que usufruem do aplicativo, ainda se trata da obrigação que o próprio poder Judiciário pode fazer materializar junto aos responsáveis pelos registros, no caso da empresa Facebook Serviços Online do Brasil Ltda., sem violar direitos de terceiros.²⁵

O tribunal é claro no sentido de que tal decisão fere a liberdade de expressão, além de atingir um número indeterminado de pessoas que nada tem a ver com o crime praticado no Piauí.

O ideal seria o desenvolvimento de uma ferramenta que atingisse apenas o criminoso. No entanto, isso ainda não foi possível. Assim, por diversas vezes, os magistrados tem decidido pela suspensão do aplicativo em face da falta de colaboração da empresa demandada.

Engana-se quem pensa que só o Brasil determinou tais medidas de suspensão do aplicativo. No Reino Unido, o primeiro ministro britânico David Cameron se pronunciou a respeito da falta de colaboração do Facebook nas investigações de terrorismo, “vamos permitir meios de comunicação que são impossíveis de ler? Minha resposta é: Não, não devemos fazer isso”

Na Arábia Saudita houve ameaça de retirada do aplicativo do ar, na época o aplicativo Viber (troca de mensagens de voz pela internet) foi bloqueado no país. Em Bangladesh e no Irã, o Whatsapp teve suas atividades suspensas devido a ameaça de terrorismo.

Na Síria, durante a Primavera Árabe, usava-se o aplicativo para marcar protestos por isso em 2012 o governo do ditador sírio Bashar Al-Assad determinou o bloqueio do dispositivo.

Os países que enfrentam crises como a da chamada “Primavera Árabe” e os que são democráticos como a Arábia Saudita buscam exercer um controle absoluto, enquanto que as democracias buscam estabelecer limites e apurar os responsáveis pelos abusos.

3.3 A Responsabilidade Civil pelo Conteúdo Transmido na Rede

Os primeiros casos de responsabilização civil por divulgação de conteúdos ilícitos dos usuários ocorreu nos Estados Unidos da América do Norte,

²⁵Mandado de Segurança n. 0013872-87.2014.8.18/0140. Desembargador Raimundo Nonato da Costa Alencar. Tribunal de Justiça do Estado do Piauí. 26 de fevereiro de 2015.

isto porque este foi o primeiro país a utilizar a internet como um modelo de informação de massa nas redes sociais e também nos veículos de comunicação. Por conta do número muito grande de usuários, o número de violações também era muito elevado.

Nos Estados Unidos da América do Norte a maioria dos casos trata da tentativa de responsabilização dos fornecedores de serviço de acesso à internet. Os Tribunais estadunidenses têm se posicionado a favor da liberdade de expressão, pela não condenação dos fornecedores de serviços pelos conteúdos divulgados por terceiros, por meio de suas plataformas. O modelo norte-americano é diferente em cada Estado e tem legislação própria, mas há ainda leis federais que são apreciadas pelos Tribunais da União, posto que também há legislação em nível federal sobre a Rede Mundial de Computadores.

Portanto, o vetor é de total liberdade, mas com a responsabilização por parte de quem abusar do direito violando a vida privada e intimidade por meio da rede mundial de computadores.

Finalmente, a promoção e regulação dos conteúdos a nível internacional, dado o caráter transnacional da internet, tem sido uma preocupação constante dos países onde a utilização desta rede informática tem vindo a generalizar-se, razão pela qual já se têm verificado várias iniciativas nesse sentido, com referiremos oportunamente. Esta crescente movimentação com vista à resolução, no âmbito internacional, do que já começa a ser um problema dos conteúdos ilegais e lesivos na internet, parece assumir-se, de fato, como a principal ou até a única forma de combater, de uma forma eficaz, esses conteúdos

A primeira tentativa de controlar o conteúdo divulgado na rede, veio dos Estados Unidos, em 1996, por meio da aprovação do *Communications Decency Act* (CDA). Foi uma reforma nas leis de telecomunicação que condenava a transmissão de materiais obscenos, indecentes, inapropriados para menores de dezoito anos. Nesse caso, permitindo a responsabilização dos fornecedores de acesso.

Muito tempo antes quando não existia a rede mundial, a Suprema Corte dos Estados Unidos da América do Norte, por meio do juiz-presidente Oliver W, Holmes destacou a constitucional possibilidade de restrições à liberdade de

expressão no caso *Schenck*²⁶, análises doutrinárias são feitas com base nos votos sobre expressões provocativas e ofensivas. Portanto, sempre houve limites e o regime buscou sempre garantir a liberdade de ideias e conteúdos.

Porém o CDA foi considerado inconstitucional, por denúncia do Tribunal da Filadélfia, e posterior confirmação da Suprema Corte Norte Americana, por ferir a liberdade de expressão.

“Por ser a maior forma de expressão já desenvolvida, a Internet merece a maior proteção possível contra a intromissão governamental”. Decisão do Tribunal Federal de Apelações dos Estados Unidos da América proferida em junho de 1996.

No sistema Norte Americano, quem deve ser responsabilizado é autor da ofensa a honra, os provedores de internet não podem ser responsabilizados civilmente por atos praticados por terceiros. Seria impossível controlar todo o conteúdo divulgado por seu canal, além do que estaria exercendo uma forma de censura o que totalmente contrário a primeira emenda.

No caso *Jane Doe vs. Bates*, numa sala de bate papo online (*Candyman*) do Yahoo foi publicado conteúdo de pornografia infantil, como fotos, vídeos e etc. A autora alegou que o site tinha consentimento do conteúdo ilegal divulgado em sua página e que foram negligentes ao permitirem esses conteúdos criminosos.

O Congresso decidiu que quem deve ser punido são as pessoas que divulgam os conteúdos ilícitos na Rede, e não as plataformas prestadoras de serviço. O Tribunal do Texas decidiu pela prisão de Mark Bates, autor das postagens, e pela absolvição do portal de notícias Yahoo.

3.4 O Marco Civil da Internet

O Marco Civil da Internet, Lei 12.965/2014, veio para regulamentar os direitos e obrigações dos usuários da rede mundial de computadores no Brasil dentro dos parâmetros da Constituição e dos tratados. Estabelecendo proibições, responsabilidade civil dos usuários e provedores de internet nos casos concretos, bem como algumas situações do dia-a-dia.

²⁶ 249 US 47. Neste caso, o juiz Holmes estabeleceu a tese do “perigo claro e presente”, para justificar uma restrição à liberdade de expressão. Este teste foi alterado pelo mesmo ministro da Corte Suprema na decisão do caso “*Abrahms*”, onde instituiu o princípio do “perigo claro e iminente” para admitir restrições.

Por meio dos seus princípios, como os da intimidade, da privacidade e da liberdade de expressão, estabeleceram-se uma série de condutas que devem ser adotadas pelos usuários, a fim de que o funcionamento ocorra sem violações e problemas para as pessoas, visando que exista respeito à dignidade da pessoa humana usuária da rede e de seus aplicativos.

Por muito tempo, a jurisprudência divergia quanto a responsabilização dos provedores de internet no que tange aos conteúdos ilícitos divulgados por seus usuários aproveitando a hospedagem. A lei 12.965/2014²⁷ trouxe a seguinte redação para o artigo 19:

“Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário”.

Acabando com o impasse jurisprudencial, e determinando que caso os provedores tenham acesso aos dados pessoais dos que tiverem o conteúdo removido da rede, têm o dever de informá-los o motivo garantindo-lhes o contraditório e a ampla defesa. Fica patente a preocupação com a total liberdade de manifestação dos conteúdos, mas restando uma responsabilização no caso de uma ordem do Poder Judiciário não ser obedecida no caso de uma decisão.

Assim, por meio de ordem judicial, pode o usuário ter seu conteúdo removido da plataforma, a exemplo do que acontecia anteriormente no caso dos veículos impressos. No entanto, há outra possibilidade de retirada ou proibição de conteúdos por meio de notificação extrajudicial aos provedores, como caso de imagens e vídeos de nudez e atos sexuais de caráter privado.

Vejamos a explicação de dois autores, André Giachetta e Pamela Meneguetti, Marco Civil da Internet:

O Marco Civil da Internet reafirmou a garantia constitucional à inviolabilidade da intimidade e da vida privada, como princípio e também como direito dos usuários da rede mundial de computadores, como reação aos fatos internacionais relacionados à coleta e utilização não autorizada de dados pessoais e de comunicação de usuários brasileiros, mesmo que prescindível ante as disposições da Constituição Federal de 1988²⁸

²⁷Lei 12.965/2014. Lei do Marco Civil da Internet.

²⁸Giachetta, André e Meneguetti, Pamela, Marco Civil da Internet, p. 390

Fica claro que o Marco Civil privilegiou o princípio à liberdade de expressão, podendo o usuário publicar o conteúdo que lhe convier. Contudo haverá a responsabilização àqueles que violarem a intimidade e privacidade dos demais.

Portanto, o vetor é de total liberdade, mas com a responsabilização por parte de quem abusar do direito violando a vida privada e intimidade por meio da rede mundial de computadores.

3.5 A Nova Lei de Proteção de Dados Pessoais

O legislador brasileiro foi bastante pertinente ao redigir a Lei de Proteção aos dados pessoais (lei 13.709/2018). Esta novidade visa garantir a segurança e o sigilo ao tratamento de dados nos meios eletrônicos.

O artigo 5º, X, da referida lei, define o que é tratamento de dados pessoais:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Para melhor compreender esta lei, é preciso saber que o titular é aquele a quem se referem os dados. O controlador é a pessoa que decide como será o tratamento de dados.

O titular deve autorizar a utilização de seus dados pessoais no momento da contratação do serviço, tendo o direito de saber quais são os dados usados no tratamento pelo controlador.

Os agentes de tratamento de dados tem o dever de aplicar as medidas e técnicas que efetivem a proteção à privacidade, intimidade, honra, imagem, liberdade de expressão e os demais princípios dispostos na lei.

Excetua-se a aplicabilidade do diploma no que tange aos dados pessoais quanto as atividades acadêmicas, jornalísticas, para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão a infrações penais.

Como já foi mencionado, a plataforma Facebook se envolveu em polêmicas no ano passado pois forneceu dados pessoais de seus usuários às

empresas parceiras, foi alvo de investigações visto que não tinha autorização para tanto. Principalmente porque ficou provado que algumas dessas empresas tinham a finalidade de propagar *fake news*, que inclusive influenciaram no resultado das eleições presidenciais Norte Americanas.

No Brasil as *fake news* ficaram populares devido a sua veiculação especialmente pelo Facebook e Whatsapp, é verdade que muitas foram desmentidas, ainda assim, são motivo de discussão pois na essência tratam da corrida presidencial.

Recentemente o aplicativo Facebook foi condenado pelo Tribunal Superior Eleitoral a retirar da Internet 33 notícias falsas relacionadas a candidata a vice presidente da República Manuela D'ávila.²⁹ Interessante que em sua decisão o ministro Sergio Banhos determinou que a empresa fornecesse os dados para identificação dos responsáveis pela divulgação das notícias, IP dos computadores, para que haja a devida responsabilização.

3.6 O Direito ao Esquecimento

Esse instituto jurídico nasceu na Alemanha, no final da década de 70, ele é extremamente recente e talvez por isso o direito brasileiro não o tutele, mas a doutrina e a jurisprudência tem caminhado no sentido de garantir esse direito especial que visa a proteção a vida digna do ser humano. O enunciado 521 da VI Jornada de Direito Civil trata: "A tutela da dignidade da pessoa humana na sociedade de informação inclui o direito ao esquecimento".

Há apenas um Informativo nº 527, do Superior Tribunal de Justiça, divulgado em 09 de outubro de 2013 que dispõe: "o direito ao esquecimento é o direito que uma pessoa possui de não permitir que um fato, ainda que verídico, ocorrido em determinado momento de sua vida, seja exposto ao público em geral, causando-lhe sofrimento ou transtornos".

Direito ao esquecimento consiste em um tipo de resguardo diante da intromissão na vida privada, familiar, social ou na correspondência de um indivíduo, garantindo assim a proteção de dados pessoais. Assim o usuário da Rede mundial

²⁹ TSE manda Facebook retirar do ar 33 links com notícias falsas contra Manuela D'ávila. Disponível em: <http://www.charlesaraujo.com.br/site/2018/10/tse-manda-facebook-tirar-do-ar-33-links-com-noticias-falsas-contr-manuela-davila/> Acesso em: 28 de outubro de 2018.

de Computadores também tem pleno conhecimento das informações divulgadas na rede a seu respeito, bem como a possibilidade de retirá-las.

O remédio constitucional hábil para requerer o direito ao esquecimento é *habeas data*. Durante a ditadura era usado para que as pessoas tivessem acesso às informações obtidas pelo poder judiciário. Era possível a alteração de informações equivocadas pelo *habeas data*, visto que os militares e agentes da repressão trabalhavam com informações que nem sempre eram corretas devido às fontes pouco confiáveis e também as opiniões daqueles que estavam encarregados em fazer as anotações.

Posteriormente, o referido remédio constitucional passou a ser usado para questões ligadas ao Serviço de Proteção ao Crédito (SPC) e também os bancos do SERASA.

Todavia, com a rede mundial de computadores foram surgindo outros bancos de dados, que são as edições dos jornais e revistas disponíveis “*online*”, bem como páginas de conteúdos variados. Com essa possibilidade de armazenamento ilimitado de conteúdos surgem problemas graves, com violações de direitos da personalidade e até mesmo para cometimento de crimes de injúria, calúnia e difamação.

Alguns casos se tornaram marcantes no cenário nacional, como por exemplo o caso determinado na própria Rede de “Daniel Estuprador” ex participante do programa Big Brother Brasil, Daniel Echaniz que foi acusado durante o programa de estuprar outra participante Monique Amin, o programa mostrou que eles praticaram sexo após uma festa, e a moça estava extremamente alcoolizada, posteriormente alegou não se recordar do ocorrido. Judicialmente ficou comprovada a inocência de Daniel, sendo que a suposta vítima confessou que consentiu com a relação em juízo, no entanto até hoje diversos sites, inclusive estrangeiros noticiam o fato condenando o rapaz.

Outro caso polêmico foi da Escola Base, onde os donos da escola foram acusados pelos pais de alguns alunos juntamente com o motorista da van de abusar sexualmente de crianças. Posteriormente ficou comprovada que a criança possuía uma doença que causava a dilatação da vagina. A gravidade da acusação e a comoção e revolta nacional foi tamanha que a escola foi fechada e os donos tiveram sua casa pichada e depredada, assim como a fachada da escola.

Em ambos os casos, os acusados eram inocentes. Ainda assim, foram condenados pela opinião pública, será que eles teriam o direito ao esquecimento e a remoção deste conteúdo da rede?

Acreditamos que sim. Nesse contexto, mencione-se o caso Aída Curi, que foi encontrada morta durante os anos 1950, imaginou ser caso de suicídio porém posteriormente comprovou se tratar de estupro e homicídio. Nos anos 2000, o programa Linha Direta Justiça da TV Globo, resolveu recriar o caso, no entanto a família Curi entrou com recurso no Tribunal de Justiça do Rio de Janeiro para barrar a transmissão do programa.

Sob a alegação de que o crime havia ocorrido a mais de 50 anos, a vítima já falecida e constrangimento e dor aos familiares de Aída, conseguiram impedir a transmissão, o STJ também autorizou o direito ao esquecimento, e aguarda-se o julgamento do Agravo em Recurso Extraordinário nº 833.248 do Supremo Tribunal Federal.

O direito ao esquecimento se relaciona com o direito de resposta, em que a pessoa que tiver uma informação enganosa a seu respeito divulgada em um meio de comunicação, (jornal, TV, rádio e internet) tem o direito de retificar a informação no mesmo programa e horário que a calúnia foi transmitida. Além disso, o direito ao esquecimento possibilita a remoção do conteúdo mentiroso dos meios de comunicação.

O website Youtube, que dá acesso a diversos vídeos, até recentemente quando precisava bloquear algum conteúdo por ordem judicial precisava retirar todo o site do ar. Com a tecnologia, foi desenvolvida uma ferramenta que possibilitou o bloqueio apenas do conteúdo considerado inadequado.

No aplicativo Whatsapp, também acontece isso, é preciso desligar todo o sistema operacional do aplicativo em razão de uma condenação criminal, assim toda a coletividade acaba prejudicada por um crime que não teve responsabilidade.

Por isso, é necessário desenvolver um mecanismo que atinja somente os condenados. Relembre-se que, por vezes, a justiça brasileira determinou o bloqueio do aplicativo em todo o país em razão de sentenças criminais, isso sem observar que há milhares de pessoas que usam do aplicativo para trabalhar, se relacionar e etc.

É certo que as decisões que bloquearam o aplicativo não se sustentaram em segunda instância, ainda assim, é incontável o número de pessoas que sofreram com a determinação judicial.

3.7 A Vedação ao Anonimato no Direito Brasileiro

A Constituição Federal brasileira expressamente veda o anonimato, no seu artigo 5º IV - é livre a manifestação do pensamento, sendo vedado o anonimato. Isto significa que qualquer pessoa pode dizer o que pensa por qualquer meio, desde que se identifique. Essa vedação ganha importância no atual momento da Sociedade de Informação em nível global.

O motivo dessa vedação nos parece óbvio. Ora, se o anonimato fosse legal, seria praticamente impossível punir os responsáveis por crimes de opinião, especialmente os que são cometidos através da internet.

Nos casos em que se sabe quem praticou o crime de opinião já é difícil rastrear o IP que emitiu a informação, imagine sem saber qualquer dado o quão árdua seria esta tarefa.

É imprescindível que crimes de opinião cibernéticos sejam devidamente investigados e punidos. É vero que os crimes contra a honra são de ação penal privada, ou seja, está condicionado a representação do ofendido. Porém, nada impede que o Estado seja responsável pela ação penal, por exemplo quando o ofendido for o próprio Estado/Governo.

No Brasil não é possível o anonimato devido à essa vedação constitucional prevista no artigo 5.o., mas no México, um dos blogs de maior sucesso e grande número de acessos, o Blog Del Narco³⁰, não revela a identidade dos seus autores, por motivos óbvios, mas há conteúdos publicados por traficante, paramilitares e outras pessoas. Na Suécia, a Lei Maior estabelece que o anonimato é um direito constitucional.

O silêncio imposto pela violência do narcotráfico mexicano à imprensa tradicional acabou por fazer surgir na rede mundial de computadores um tipo de alternativa para o debate sobre a violência da chamada “guerra dos cartéis”, bem como os abusos dos policiais. Passados alguns anos, o blogdelnarco publicou

³⁰Disponível em: <http://www.blogdelnarco.com/> Acesso em: 13 de agosto 2018.

centenas de conteúdos ou posts, que mostram um pouco do confronto que matou algumas centenas de pessoas, desde 2006.

4 NAÇÕES UNIDAS E AS DISCUSSÕES DE PROGRAMAS DE CONTROLE DOS ESTADOS

A Organização das Nações Unidas há algum tempo está preocupada com a plataforma mundial de computadores, bem como suas consequências, pois a rede permite, por exemplo, a comunicação entre grupos terroristas e traficantes de drogas, além de questões atinentes aos negócios privados, como compras e pagamentos.

Gerald Herman, secretário da Comissão das Nações Unidas para Direito Comercial Internacional (UNCITRAL), afirma que os fornecedores empresariais terão uma lei específica para protegê-los dos consumidores que, até o momento, estão ditando as regras no mundo do comércio eletrônico e da Internet³¹. No caso de uma legislação terá que levar em conta esse confronto entre intimidade e segurança do Estado, que cresceu depois dos atentados terroristas de 11 de setembro de 2001, bem como interceptações telefônicas. O objetivo é tornar seguro o comércio e também cuidar da licitude do que é vendido e comprado em nível global.

De acordo com a Organização das Nações Unidas, recentemente o acesso à Internet foi consagrado como um direito humano fundamental. Esta medida representa um grande avanço pois através da Rede as pessoas acessam informações e podem exercer a liberdade de expressão.

Entretanto, o acesso à Internet não é completamente difundido no Brasil, desde 2005 quando foram realizadas as primeiras pesquisas sobre acesso à Internet no Brasil apenas 17% dos domicílios possuíam computadores e somente 13% possuíam acesso à internet.³² Em 2017, o IBGE registrou que 70,5% dos domicílios brasileiros possuem acesso à internet.³³

Na Conferência Mundial de Tunes convocada pela ONU em novembro de 2005, surge o chamado “communication rights”, que tem seu antecedente na Carta das Nações Unidas e no artigo 19 da Declaração Universal dos Direitos do

³¹ PAESANI, Liliansa Minardi. **Direito e Internet – Liberdade de informação, privacidade e responsabilidade civil**, p. 78-79.

³² Acesso em: 07 de agosto de 2018. Disponível em: <https://tecnologia.ig.com.br/2018-04-27/acesso-a-internet.html>

³³ Acesso em: 07 de agosto de 2018. Disponível em: <https://tecnologia.ig.com.br/2018-04-27/acesso-a-internet.html>

Homem³⁴. A ideia era criar um tipo de vigilância global, mas esse tema acabou ficando de fora das discussões, bem como interceptações por parte de uma agência, em especial quando existe questões ligadas à segurança pública³⁵. A liberdade de expressão na rede passa a ser acompanhada com a finalidade de garantir a integridade dos Estados, mas na verdade as potências como Rússia, Estados Unidos e China, por exemplo, buscaram cada qual uma solução, muitas vezes sem respeitar os direitos humanos previstos nos tratados.

A China, por exemplo, tem uma censura e proíbe o Facebook, pois não é uma democracia. O país asiático tem partido único, regime socialista e total controle dos meios de comunicação, incluindo as mídias sociais.

A Rússia, por sua vez, também tenta acompanhar os conteúdos e esteve envolvida em alguns escândalos como a eleição do presidente Donald Trump. Portanto, embora a ONU busque confirmar a livre circulação de ideias e opiniões, isso ocorre apenas nos países democráticos.

A liberdade de expressão foi elevada a um direito universal em 1948, quando foi aprovada a primeira Declaração Universal de Direitos Humanos durante a Assembleia das Nações Unidas(DUDH). Mas, as atitudes internas de países não democráticos que são membros, muitas vezes sem legislação, violam os direitos previstos nos dois documentos pioneiros da ONU, pois a Carta também abordava a temática;

Para Loreto Corredoira y Alfonso³⁶, desde a sua aprovação foi consagrada uma doutrina básica compartilhada por todos sobre a universalidade

³⁴ CORREDOIRA Y ALFONSO, Loreto. **Lectura de la Declaración Universal de Derechos Humanos de 1948 em el paradigma de la nueva “Sociedade de la Información. Estudio específico del artículo 19 <in> Libertad em Internet – La red y las libertades de expresión e informacion** (coordinador – Lorenzon CotinoHueso), p. 60.

³⁵ PAESANI, Lilitiana Minardi. **Direito e Internet – Liberdade de informação, privacidade e responsabilidade civil**, p. 55. “A crescente escalada de violência tem possibilitado ao Poder Público a captação de informações e dados privados por meio de métodos eletrônicos sofisticados. Entende a doutrina que, diante dos fins visados, é possível a ação interceptadora, sacrificando-se direitos individuais em prol do bem comum. Essas interferências estão legitimadas pelo sistema jurídico, em função da orientação que cabe ao Estado conceder segurança pública”.

³⁶ CORREDOIRA, Loreto Alfonso y. **Lectura de La Declaración Universal de Derechos Humanos de 1948 em El paradigma de La nueva “Sociedade de la Informaició”. Estudio específico Del artículo 19 <in> Libertad em Internet – La red y las libertades de expresión e información**, p. 57. A autora cita nomes como importantes José Maria Desantes-Guanter, Sanchez-Férriz, González Ballesteros, Escobar de La Serna, Bel Mallen e Cousido.

³⁶ MOLES PLAZA, Ramón J. **Derecho y control em Internet – La regularidad de Internet**, p. 103.

³⁶ A Comissão nasceu em 1946 pela determinação do Conselho Econômico e Social (EGOSOC) com a finalidade de promover os direitos humanos e permaneceu em funcionamento até 2006, quando foi

desses direitos ligados à manifestação do pensamento, levando em conta a proibição de discriminação prevista no artigo 2 da Declaração e também o artigo 19.

Mas há uma grande dificuldade de proteção de direitos relativos à manifestação do pensamento diante do novo território que é a rede mundial, principalmente porque os abusos são frequentes, incluindo o próprio Estado. Por isso, o direito à intimidade, o direito à liberdade de expressão, precisam de algo novo, pois surgem novas ameaças, como o terrorismo e até mesmo uma intervenção do próprio Estado.

A proteção foi sempre associada às limitações e mecanismos de caráter territorial, às vezes com sistemas distintos, que dão respostas aos padrões culturais, religiosos e sempre com valores distintos, fruto da cultura de um povo³⁷. Nesse sentido, haveria necessidade de várias regulações, com controle do Estado, mas também de grupos criminosos e terrorista, além de pornografia infantil. Não haveria uma única regulamentação internacional, mas teriam as nações que promover uma conferência para discutir as temáticas, como terrorismo, espionagem, tráfico de drogas e até mesmo interferências nas eleições.

As temáticas poderiam nesse sentido trazer limites para as comunicações feitas pelos telefones dos particulares. No entanto, as temáticas são tantas que exigiram muita discussão, pois os direitos da personalidade também precisam ser protegidos.

Além disso, os estudos da ONU teriam que reconhecer e integrar a diversidade de sistemas, o pluralismo existente, bem como peculiaridades e localização dos provedores. Na verdade, existe intensa discussão sobre a liberdade de expressão e de informação, bem como limites, mas até o momento, a Organização das Nações Unidas não se ocupou das violações na rede.

Para Manuel Castells existe uma parte significativa da vida cotidiana da pessoas, como o trabalho, o ócio e a interação pessoal, que tem lugar na Rede³⁸. Há ainda uma parte da atividade econômica, social e política que são uma realidade híbrida de interação on-line e interação física, com os aplicativos

criado um órgão substituto denominado Conselho de Direitos Humanos, que é órgão mais abalizado sobre direitos humanos.

³⁷ MOLES PLAZA, Ramón J. **Derecho y control em Internet – La regularidad de Internet**, p. 103.

³⁸ CASTELLS, Manuel. **La Galaxie da Internet – Reflexões sobre a Internet, os negócios e a sociedade**, p. 203 e ss.

bancários por exemplo que permitem pagamentos e transferência de valores. Em muitos casos, uma não existe sem a outra, mas cada Estado tem optado por legislar sem levar em conta o indivíduo.

Dessa forma, a vida no sistema eletrônico sem direitos da personalidade significa que um percentual grande das relações das pessoas ligadas aos direitos da privacidade e intimidade estariam expostas aos vários tipos de vigilância, alguns justificadas pelo Estado e pelos tratados, enquanto que outra sem nenhum tipo de justificativa.

Essa questão fica clara, quando absolutamente nada se discute sobre os sistemas de vigilância que os países costumam negar³⁹, mas que envolvem os sigilos telefônicos e e-mails. A questão pode ser explicada de maneira muito simples: dois membros permanentes do Conselho de Segurança da ONU, que tem poder de veto sobre qualquer assunto, não praticam a liberdade e ao contrário, buscam controlar os conteúdos postados inclusive nas redes sociais. Com isso, uma discussão sobre esses temas fica prejudicada e sempre sujeita ao poder de veto dos membros permanentes.

No ano de 1993, a Comissão da ONU para os Direitos Humanos⁴⁰, que depois foi substituída pelo Conselho de Direitos Humanos⁴¹, criou o escritório do Relator Especial da Organização das Nações Unidas para a Liberdade de Opinião e de Expressão⁴².

Há estudos sobre o tema, visto que este órgão faz documentos anuais para a Comissão desde 1997, sendo que a finalidade é esclarecer os exatos conteúdos dos direitos humanos de liberdade de informação e de expressão⁴³, bem como discutir outras problemáticas, como o papel dos Estados na garantia de direitos. Atualmente essas discussões prosseguem, mas importante afirmar que nasceram ainda no século XX.

³⁹ PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**, p.167.

⁴⁰ A Comissão nasceu em 1946 pela determinação do Conselho Econômico e Social (EGOSOC) com a finalidade de promover os direitos humanos e permaneceu em funcionamento até 2006, quando foi criado um órgão substituto denominado Conselho de Direitos Humanos, que é órgão mais abalizado sobre direitos humanos.

⁴¹ A Resolução da Assembleia Geral da ONU 60/251, de 3 de abril de 2006, está disponível em <http://daccessdds.un.org/doc/UNDOG/GEN/N05/502/66/PDF/N05550266.pdf?OpenElement>.

⁴² Resolução 1993/45, de 5 de março de 1993.

⁴³ MENDEL, Toby. **Liberdade de informação: um estudo comparado**, p. 9.

Após receber suas declarações iniciais sobre a liberdade de expressão em 1997, a Comissão solicitou ao Relator Especial para “refinar sua análise acerca do direito de buscar e receber informações e a discorrer sobre suas observações e recomendações originárias”⁴⁴. Novo Relatório em 1998 abordou o tema e naquele momento: “O direito de buscar, receber e transmitir informações, sobretudo no que tange às informações mantidas pelo Governo em todos os tipos de sistemas de armazenamento e recuperação”⁴⁵.

Há documentos mais recentes, emanados da sede da Organização das Nações Unidas que seguem considerando o caráter fundamental do artigo 19, como regra básica aplicável aos novos meios, ou seja, a rede mundial de computadores, como recomendação aos Estados. Em tese, esses direitos universais deveriam alcançar plenamente a Sociedade de Informação.

Os documentos da ONU no século XXI reafirmam duas características importantes desses direitos em nível internacional, que são a universalidade e a interdependência dos direitos, bem como de que há uma esfera da vida das pessoas que deve ficar a salvo de interferência do Estado ou mesmo das organizações. Os documentos e também os tratados, contudo, ainda não se ocupam da produção dos conteúdos que abordem os sistemas de vigilância, que serve para que o Estado implemente vigilância, controle e violações.

Importante notar que a Declaração Universal dos Direitos do Homem, que marca a terceira dimensão dos direitos humanos, traz como ideal comum de todos os povos e nações, o respeito dos direitos e liberdades que devem ser assegurados por “medidas progressivas de caráter internacional, seu reconhecimento e aplicação universais e efetivos, tanto entre os povos dos Estados-membros como entre os territórios colocados debaixo de sua jurisdição”.

Entre as medidas progressivas de caráter internacional preconizadas, surge a necessidade de várias concertações, ou seja, tratados específicos. A discussão retroage a 18 de janeiro de 1999, quando foi realizada a primeira

⁴⁴ Resolução 1997/27, de 11 de abril de 1997, parágrafo 12(d).

⁴⁵ Relatório do Relator Especial, **Promotion and protection of the right to freedom of opinion and expression**, Doc. da ONU E/CN.4/1998/40, de 28 de janeiro de 1998, parágrafo 14.

conferência da Organização das Nações Unidas para Educação, Ciência e Cultura (UNESCO) sobre a disseminação da pornografia infantil e pedofilia na Internet⁴⁶.

Especialistas das mais diversas áreas, como segurança, de 40 Estados-membros, além de representantes de 75 organizações não-governamentais, analisaram diferentes proposições e estudaram maneiras de defender as crianças e adolescentes na rede mundial.

No tocante a esse tipo de crime surgiu a necessidade uma estrutura legislativa internacional, bem como a cooperação das polícias e Justiças nacionais, o que tem sido feito, especialmente na Europa, mas também no Brasil, contando com a colaboração dos provedores de acesso à rede.

Devido à exploração sexual de crianças e às violações por meio de imagens e vídeos que são crimes previstos na Convenção sobre os Direitos da Criança, a Assembleia Geral das Nações Unidas, a partir de 25 de maio de 2000, instituiu o Protocolo Complementar à Convenção sobre os Direitos da Criança e que cuida, de forma específica, da prostituição, do tráfico de crianças e da pornografia infantil na chamada “*deep web*”. Esses direitos do Protocolo vigoram desde 18 de janeiro de 2002 e os Estados se obrigam a reprimir com sanções penais os atos condenados pelo tratado, bem como colaborar para localizar rede de pedófilos.

Com objetivo de preparar os fundamentos dessa Sociedade de Informação, a ONU realizou em Genebra, na Suíça de 10 a 12 de dezembro de 2003 e em Túnez, de 16 a 18 de novembro de 2005, duas outras conferências sobre o tema, buscando estabelecer limites. O objetivo da primeira fase consistia em preparar, por meio de tratados e declarações, todos os fundamentos para os temas e também os diferentes interesses em jogo. Já a segunda conferência buscou alcançar acordos em matéria de governo de Internet⁴⁷.

Nessa Declaração de Genebra da ONU e na segunda fase realizada em Túnez⁴⁸, os países-membros proclamam: “Reafirmamos como fundamento essencial da Sociedade de Informação, segundo estipulado no artigo 19 da

⁴⁶ PAESANI, Liliana Minardi. **Direito e Internet – Liberdade de informação, privacidade e responsabilidade civil**, p.24.

⁴⁷ www.itu.int/wsis/basic/about-es.html.

⁴⁸ Declaração de Genebra, 2003, Convenção Mundial sobre A Sociedade da Informação: Declaração de Princípios da Segunda Fase da Convenção celebrada em Túnez, em novembro de 2005, conhecida como Compromisso de Túnez, que inclui um Plano de Ação sobre a Sociedade de Informação.

Declaração Universal dos Direitos Humanos, o direito à liberdade de opinião e de expressão(...).”

Há presente nos referidos tratados direitos e garantias de caráter genéricos, com princípios que reconhecem as várias faces do direito de informação e da liberdade de expressão, mas seria necessário outros dispositivos visando assegurar os direitos dos usuários ligados à intimidade e privacidade. Para Corredoira⁴⁹, o documento de Túnez anunciou a existência da *communications rights*, que mais que uma petição de novos direitos, “é uma ação pública em nível internacional de sensibilização sobre os desafios dos direitos de informação numa sociedade globalizada”.

Importante é a aplicação desses marcos dos direitos humanos previstos na Convenção de Túnez, mas buscar aprimoramentos, pois são vários conteúdos de diferentes aspectos. A “Declaração de Princípios” e seu “Plano de Ação” traz em *standers* ou normas, que poderiam ser fortalecidas com outros documentos elaborados por novos tratados das Nações Unidas.

A Declaração de Genebra, que cuidava da infraestrutura da informação, expressão e das comunicações trazia já fundamentos básicos de uma Sociedade da Informação:

21. A conexão é um fator habilitador indispensável na criação da Sociedade de Informação. O acesso universal, equitativo e exequível a infraestrutura e aos serviços da rede mundial de computadores constitui um das linhas mestras da Sociedade de Informação e deve ser um objetivo de todas as partes interessadas que participam da sua criação...⁵⁰

O artigo 23, por sua vez, prevê o cumprimento das obrigações de um serviço universal nas regiões em que as condições tradicionais do mercado não funcionem corretamente, cuidando das questões negociais.

Um princípio básico do direito de informação e da liberdade de expressão é a universalidade, no sentido de que este direito fundamentalmente garanta uma comunicação livre que se exerce em qualquer lugar e por qualquer

⁴⁹ CORREDOIRA, Loreto Alfonso y. **Lectura de La Declaración Universal de Derechos Humanos de 1948 em El paradigma de La nueva “Sociedade de la Información”**. Estudio específico Del artículo 19 <in> Libertad em Internet – La red y las libertades de expresión e información, p. 57.

⁵⁰ Artigo 21 da Convenção de Genebra.

meio de comunicação. No entanto, também é universal o direito à intimidade e a privacidade na rede mundial, que serve como limite.

Esse direito de receber, acessar e divulgar deve ser exercido na rede mundial com as limitações, segundo o artigo 24.2, da DUDH, que estabelece que:

No exercício de seus direitos e liberdades, todas as pessoas estarão sujeitas apenas às limitações determinadas pela lei, exclusivamente com o fim de assegurada o devido reconhecimento e respeito dos direitos e liberdades de outrem, e de satisfazer às justas exigências da moral, da ordem pública e do bem-estar de uma sociedade democrática.⁵¹

A universalidade reclama a igualdade de acesso para buscar conteúdos e divulgar qualquer tipo de informação e expressão, também pretende regular as condições do exercício desses direitos em nível global.

A questão segue sem legislações específicas, sem que as reuniões e conferências realizadas até agora dentro do chamado “Foro para Governança de Internet” tenham alcançado um resultado importante para uma concertação internacional. O foro marcou a primeira reunião para Atenas, no final de 2006, que ocorreu sem muitos avanços, com delimitação dos temas e conteúdos e papel da ONU e dos Estados.

A segunda conferência ocorreu no Rio de Janeiro, de 12 a 15 de novembro de 2007 e alguns dos participantes, como a China, lutaram para transformar o Foro em uma instância de adoção efetiva de tais acordos, outros, como a União Europeia, preferem considerá-lo como mero instrumento de diálogo e troca de experiências⁵². No entanto, embora os chineses defendam a adoção de medidas de caráter global, internamente exercem forte controle sobre as redes sociais

Os Estados Unidos da América do Norte, por sua vez, sempre participam das discussões,mas sob a justificativa de combate ao terrorismo, por exemplo, tomam medidas violadoras.

E ainda deve haver sempre uma preocupação dos Estados democráticos que uma concertação seja usada por Estados que não respeitam os

⁵¹Artigo 24.4 da Declaração Universal de Direitos Humanos.

⁵² Documento síntese – WWW.intgovforum.org/Rio_Meeting/Synth_portuguese.pdf.

direitos humanos e tem provedores. Portanto, há duas questões: os que assinam e não cumprem e os que assinam de boa-fé. Os Estados-democráticos, por sua vez, poderiam sofrer um duro golpe com mecanismos que pudessem controlar a liberdade de expressão por meio de um documento da ONU⁵³.

Uma proposta de regulação teria que levar a natureza dos conteúdos diante da realidade de cada um dos Estados, bem como das empresas e dos usuários dentro de uma proposta construída nas democracias de prestigiar os direitos relativos à manifestação do pensamento previstos nos tratados internacionais e documentos elaborados, mas também assegurar os direitos da personalidade das pessoas em nível global.

São três os principais sistemas de vigilância eletrônica⁵⁴, que até agora foram ignorados nas discussões das Nações Unidas: Echelon, Enfopol e Carnívoro.

Echelon é um tipo de sistema de interceptação de toda sorte de comunicação em nível mundial⁵⁵. O projeto que inicialmente para interceptar mensagens cifradas de países como a Líbia e o Irã nasceu em 1947, mas era uma questão de Estado qualificada como “ultra secreta” que apenas em 1999 chegou ao conhecimento do público⁵⁶, mas permitia a vigilância das comunicações de pessoas consideradas suspeitas.

No século XX e em especial com a Internet, o sistema passou a usar a infraestrutura e tecnologia para realizar vigilância e conseguir dados das comunicações em nível mundial, sendo reconhecido pela União Européia como um instrumento usado pela Espanha para combater o terrorismo basco⁵⁷ e pelo Congresso dos Estados Unidos da América do Norte a partir de 29 de outubro de

⁵³ MEXÍA GARCÍA, Pablo. **Derecho Europeu de Internet – Hacia La autonomía académica y La globalidade geográfica**. Espanha: Oleiros, 2009. p.26. Nesse sentido: “No se oculta que com ello sigue también vivo el riesgo de que Estados poco respetuosos de los derechos humanos, a libertad de expresión muy singularmente, ganen capacidad de decisión em el gobierno de Internet, com fines de proyectar al conjunto de la Red regímenes internos de aquella índole. Traduzi – Não se oculta que com ele segue vivo o risco de Estados pouco respeitosos com os direitos humanos, a liberdade de expressão mito singularmente, ganham capacidade de decisão em um governo de Internet, com fins de projetar ao conjunto da Rede regimes internos daquela índole”.

⁵⁴ PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**, p.177.

⁵⁵ GARCIA MOSTAZO, Nacho. **Echelon: La redespía global** <in><http://edec.iespana.es/edec/derinfor/index/html>.

⁵⁶ PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**, p.168.

⁵⁷ CAÑAS, Gabriela. **El País. La Eurocámara reconoce que Echelon espía a Europa y quiere montar una red similar** <in>[HTTP://ciberpais.elpais.es/d/20010913/cibersoc/htm](http://ciberpais.elpais.es/d/20010913/cibersoc/htm) Acesso em: 13 de agosto de 2018.

2001, para combater o terrorismo. Foi criada a lei norte-americana *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*⁵⁸, que permitia a interceptação das comunicações feitas por pessoas de algumas nacionalidades e que seriam suspeitas de terrorismo ou ligações com grupos dessa natureza.

Esse sistema Echelon tem vários satélites para interceptar as transmissões telefônicas, mensagens de correio eletrônico, páginas, arquivos e outros. Depois, computadores especialmente programados pelos especialistas são encarregados de interpretar as mensagens interceptadas, sendo que muitas dizem respeito somente a vida privada das pessoas.

Na Europa, em especial na União Europeia, o mesmo modelo foi criado e denominado de Enfopol, que significa Enforcement Police. É um mecanismo estruturado de escuta massiva nas ligações telefônicas e comunicações na Europa, com o objetivo de combater as ações ilícitas das máfias, organizações criminosas e facções terroristas. No entanto, devido a amplitude, as escutas por vezes atingem pessoas comuns dentro das suas vidas familiares e social.

Esse projeto de controle apenas foi possível pela aprovação do Parlamento e do Conselho da Europa, de uma Diretiva (2002/58/CE, de 12 de julho, sobre as comunicações eletrônicas) que autoriza no seu artigo 15, todos os provedores a reterem dados de conexão ou tráfego por um período de 12 meses, criando um banco de dados completo no tocante ao conteúdo. Pela letra “b” do artigo 2 desse Tratado do Direito Comunitário, que é uma Diretiva, há possibilidades de armazenar dados sobre a privacidade e as comunicações eletrônicas, pois os dados de tráfego são todos levados a efeitos durante uma comunicação, ou seja, todos que passam, independente do conteúdo.

Por isso fica claro que o modelo implantado e atualmente operando é um sistema de vigilância, que viola o direito à intimidade das pessoas e até hoje não foi devido discutido pelas Nações Unidas, pois as justificativas são ligadas à segurança europeia diante do terrorismo.

Há ainda um outro sistema denominado de Carnívore ou Digital CollectionSystem 1000. Trata-se de uma ferramenta criada visando aprimorar o

⁵⁸ USA PATRIOT Act.

trabalho de vigilância da agência norte-americana federal, o FBI, que se pensava agir somente sobre o correio eletrônico⁵⁹, mas que atinge também os celulares. O sistema composto de software e hardware visa interceptar, em tempo real, todos os conteúdos das comunicações particulares feitas na rede, incluindo Whatsapp.

Se a Organização das Nações Unidas ignora esse sistema norte-americano de espionagem, por pressão das entidades de direitos humanos norte-americanas,⁶⁰ o Congresso convocou em setembro de 2000, o diretor da área do FBI, Donald M. Kerr, para explicar as violações dos direitos da intimidade e funcionamento⁶¹. Portanto, embora exista uma preocupação, diante das informações fica patente que os Estados estão preocupados com seus interesses e diante de situações reais ou hipotéticas, tem buscado maneiras de violar direitos da personalidade.

⁵⁹ CASTELLS, Manuel. **La Galáxia Internet – Reflexões sobre a Internet, os negócios e a Sociedade**, p. 201.

⁶⁰ PEREIRA, Marcelo Cardoso. *Direito à intimidade na Internet*, p. 175

⁶¹ O texto completo se encontra na página:

[HTTP://WWW.fbi.gov/congress/congress00/kerr0906000.htm](http://www.fbi.gov/congress/congress00/kerr0906000.htm).

5 CONCLUSÃO

A temática desenvolvida versou sobre alguns dos direitos relativos à manifestação do pensamento escolhido dentro recorte desejado envolvendo uma ferramenta digital desenvolvida na rede mundial de computadores, à Internet. A plataforma mundial de computadores é usada para diferentes objetivos e finalidades.

Buscou-se demonstrar as mudanças trazidas pela Rede mundial de computadores e suas implicações na vida prática do indivíduo. A facilitação do acesso à informação e a dificuldade do Direito em acompanhar as transformações.

Tratou-se da responsabilidade civil pelos conteúdos ilícitos divulgados na Internet, analisando julgados norte-americanos que deixaram de condenar os provedores de serviços de Internet, justificando-se que caso exercessem um filtro das postagens, além da dificuldade, seria uma forma de censura.

Concluimos que não há motivos para que não se aplique a quebra de dados telefônicos e telemáticos em se tratando do juízo civil, visto que restringir a aplicação dessa ferramenta seria tolher direitos. É claro que essa supressão de direitos não é discriminada, ela seguirá regras, as mesmas impostas ao juízo criminal, inclusive sendo essencial a necessidade de uma autorização judicial.

Portanto, é admissível usar-se desse mecanismo sempre que o magistrado concluir necessário, para isso, alguns requisitos devem ser preenchidos: ser um crime grave ou que atinja um número indeterminado de pessoas, ter a autorização do juiz, por ser crime de natureza civil não temos a figura do delegado o que inviabiliza a fase administrativa do processo. Além disso, o juiz deverá fundamentar sua decisão.

Abordou-se a relevância do Marco Civil da Internet no ordenamento jurídico pátrio, apesar da dificuldade de acompanhar a revolução tecnológica, diferentemente do Estados Unidos da América do Norte, o Brasil preza pelo regramento.

O legislador brasileiro foi inovador ao trazer a Lei de Proteção de Dados que traz aspectos fundamentais no tocante a utilização da Rede. O principal instituto protegido pela lei são os Dados Pessoais dos usuários, sendo indispensável a autorização deste para a realização de qualquer ato no que diz respeito as suas informações.

Por fim, trouxemos o instituto do Direito ao Esquecimento, que protege os internautas, garantindo-lhes a possibilidade de remoção de conteúdos indevidos, difamatórios ou equivocados a seu respeito, por meio do remédio constitucional *habeas data*.

Importante ressaltar a vedação ao anonimato trazida pela nossa Constituição, que apesar de quando redigida não se dirigir a Internet, é completamente cabível sua aplicação, visto que na Rede é ainda mais difícil desvendar a autoria de crime cibernéticos, em razão da criptografia e da *deep web*

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Maria Fernanda de Toledo Pennacchi Tibiriçá. AMARAL, Sérgio Tibiriçá. Liberdade de expressão e os limites do direito da personalidade. in AMARAL, Sérgio Tibiriçá. SIQUEIRA, Dirceu Pereira. **Democracia, Liberdade e Justiça Social: fundamentos para uma teoria jurídica do conhecimento**. Birigui SP, Editora Boreal, 2015.

AMARAL, Maria Fernanda de Toledo Pennacchi Tibiriçá. OLIVEIRA, João Victor Mendes. Direito ao esquecimento e Autodeterminação informativa. in AMARAL, Sérgio Tibiriçá. SIQUEIRA, Dirceu Pereira. **Democracia, Cidadania e os Direitos da Personalidade: uma releitura contemporânea**. 1ª edição, Birigui – SP, 2017.

AMARAL, Sérgio Tibiriçá. **Parâmetros constitucionais do Direito à liberdade de Expressão na Internet** <in> Tese de Doutorado (Sistema Constitucional de Garantias). Instituição Toledo de Ensino: Bauru, 2010.

AMARAL, Sérgio Tibiriçá. O Direito de Informação na TV, a Convenção das Pessoas com Deficiência e o *ClosedCaption*. <in> Dirceu Pereira Siqueira; José Roberto Anselmo. (Org.). **Estudos sobre os Direitos Fundamentais e Inclusão Social**. 1 ed Birigui: Boreal, 2010;

ARAUJO, Luiz Alberto David. NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. São Paulo: Verbatim. 22ª edição, 2018.

ARANHA, Adalberto José Q. T. De Camargo. **Da Prova no Processo Penal**. São Paulo: 7ª ed. Rev. Atual. e ampl. Saraiva, 2006.

ASCENSÃO, José de Oliveira. *Hyperlinks, Frames, Metatags – A Segunda Geração de Referências na Internet* <in> **Estudos Sobre Direito da Internet e da Sociedade da Informação**. São Paulo: Almedina, 2001.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. São Paulo: Saraiva, 2014.

BRAGA, Caio Henrique Cristaldo. **A possibilidade do acesso à internet como direito fundamental no Brasil**. Monografia, 2017.

BRASIL. Supremo Tribunal Federal. STF – 2ª T – HC 93.050-6/RJ – Rel. Celso de Mello, decisão: 10-6-2008.

BARROSO, Luís Roberto. “Interceptação Telefônica para fins Penais – Inadmissibilidade da Prova Ilícita – Cabimento de Mandado de Segurança e não de Hábeas Corpus – CF, art. 5º, XII, LVI e LXIX”. Gêneses: Revista de Direito Administrativo n. 200, p. 333. 1995.

CAMBI, Eduardo. DOTTI, Rogéria. PINHEIRO, Paulo Eduardo D’arce. MARTINS, Sandro Gilbert. KOZIKOSVI, Sandro Marcelo. **Curso de Processo Civil Completo**. São Paulo: Editora: Revista dos Tribunais, 2017.

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Direito de informação e liberdade de expressão**. Imprensa: Rio de Janeiro, Renovar, 1999.

CASIMIRO, Sofia de Vasconcelos. **A Responsabilidade Civil pelo conteúdo da informação transmitido pela internet**. Porto, Portugal: Almedina, 2000.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2001.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.

CORREDOIRA Y ALFONSO, Loreto. **Lectura de la Declaración Universal de Derechos Humanos de 1948 em El paradigma de la nueva "Sociedade de la Información . Estudio específico del artículo 19 <in>Libertad em Internet – La red y las libertades de expresión e información (coordinador – Lorenzon Cotino Hueso)**, Valencia: Tirant lo Blanch, 2007.

DE LA CALLE RESTREPO, José Miguel. **Autodeterminación informativa y habeas data em Colombia – Análisis de La Ley 1266**. Bogotá: Temis, 2008

DELPECH, Horacio Fernández. **Internet: sua problemática jurídica**. Buenos Aires: Abeledo-Perrot, 2004.

Doe vs. Bates. Acesso em: 08 de maio de 2018. Disponível em:
<http://www.internetlibrary.com/pdf/Doe-Bates.pdf>

GARCIA MOSTAZO, Nacho. *Echelon: La red espía global*
 <in><http://edec.iespana.es/edec/derinfor/index/html>.

GHEDINI, Fred, GRAÇA, Antonio. **Comunicação: do Jornal à Internet**. São Paulo: Salesiana, 2010.

GIACHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A Garantia Constitucional à inviolabilidade da Intimidade e da Vida Privada como Direito dos Usuários no Marco Civil da Internet. LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**, São Paulo: Atlas, 2014.

GONÇALVES, Renato Afonso. **Bancos de dados nas relações de consumo**. São Paulo: Max Limonad, 2002.

KAMINSKI, Omar. **Internet Legal: o direito na tecnologia da informação**. Curitiba: Juruá, 2010.

DE LA CALLE RESTREPO, José Miguel. **Autodeterminación informativa y habeas data em Colombia – Análisis de La Ley 1266 de 2008**, Bogotá: Editorial Temis, 2009.

LEITE, George Salomão, LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

Lei nº 13.709, de 14 de agosto de 2018. Lei de Proteção de Dados.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Millennium, 2005.

LÔBO, Paulo. **Direito Civil: parte geral**. São Paulo: Saraiva, 2015.

MENDEL, Toby. **Liberdade de informação: um estudo de direito comparado**, 2ª Ed, Brasília: UNESCO, 2009.

MENKE, Fabiano. **Assinatura Eletrônica: aspectos jurídicos no direito brasileiro**. São Paulo: Editora Revista dos Tribunais, 2005.

MEXIA GARCIA, Pablo. **Derecho Europeu de Internet – Hacia La autonomia acadêmica y La globalidadgeográfica**. Espanha: Oleiros, 2009.

MILL, John Stuart. **Da liberdade**. Trad. E. Jacy Monteiro. Série Clássicos Da Democracia. São Paulo: Ibasa, 1964.

MORAES, Alexandre de. **Direito Constitucional**. – 29. ed. – São Paulo: Atlas, 2013.

PARDINI, Aníbal A. **Derecho de Internet**. 1ª ed. Buenos Aires. La Rocca. 2002.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 4ª ed. – São Paulo: Atlas, 2008.

PLAZA MOLES, Ramón Jordi. **Derecho y control en Internet – La regulabilidad de Internet**, Barcelona: Ariel Derecho, 2004.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na Internet**, Curitiba: Juruá, 2009.

PINHEIRO, Patricia Peck. **Direito Digital**. 2ª edição ver., atual. e ampl. – São Paulo: Saraiva, 2007.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros Editores LTDA., 2005.

SPYER, Juliano. **Conectado: o que a internet fez com você e o que você pode fazer com ela**. Rio de Janeiro: Jorge Zahar Ed., 2007.

TANCER, Bill. **Click: o que milhões de pessoas estão fazendo on-line e por que isso é importante**; tradução Renato Marques de Oliveira – São Paulo: Globo, 2009.

Porque o whatsapp está sob ameaça de bloqueio em diversos países? Acesso em: 13 de abril de 2018. Disponível em: http://www.bbc.com/portuguese/noticias/2015/02/150226_whatsapp_risco_lab

VENOSA, Silvio Salvo. **Direito Civil: parte geral**. 6 edição, São Paulo, 2006.

WHATSAPP. Acesso em: 12 de abril de 2018. Disponível em: https://www.whatsapp.com/?l=pt_br

WHATSAPP. Acesso em: 13 de abril de 2018. Disponível em: https://pt.wikipedia.org/wiki/WhatsApp#Suspens%C3%A3o_no_Brasil

ZANINI, Leonardo Estevam de Assis. **Direitos da personalidade: aspectos essenciais**. São Paulo: Saraiva, 2011. (coleção do professor Agostinho Alvim). Brasil tem 116 milhões de pessoas conectadas à internet. Acesso em: 12 de abril de 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>

Crise no Facebook: vazamento de dados para a Cambridge Analytics. Acesso em 07 de agosto de 2018. Disponível em: <https://marketingdeconteudo.com/facebook-vazamento-de-dados/>

Delegado de polícia pode acessar dados telefônicos sem autorização judicial. Acesso em: 17 de agosto de 2018. Disponível em: <https://www.conjur.com.br/2017-jun-13/academia-policia-delegado-policia-acessar-dados-autorizacao-judicial>

Fugiu do controle: O Whatsapp é o grande vilão desta eleição? Acesso em: 17 de outubro de 2018. Disponível em: <https://www.uol/tecnologia/especiais/whatsapp-e-o-vilao-da-eleicao.htm#mesmo-quem-ganhar-vai-perder>

In re Carrier Iq, Inc., 78 F. Supp. 3d 1051 (N.D. Cal. 2015). Acesso em 07 de Agosto de 2018. Disponível em: <<https://casetext.com/case/in-re-carrier-iq-inc-10?q=mobile%20app%20&p=1&tab=keyword&jxs=&sort=relevance&type=case>>

Jurisprudência Norte Americana caso US Telecom Association vs. Federal Communication Commission. Acesso em: 02 de agosto de 2018. Disponível em: <https://casetext.com/case/us-telecom-assn-v-fed-commcns-commn-3?q=whatsapp%20and%20blocking&p=1&tab=keyword&jxs=&sort=relevance&type=case>

Panorama setorial da Internet: Acesso à Internet no Brasil desafios para conectar toda a população. Acesso em 07 de agosto de 2018. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf

69% dos brasileiros já tem acesso à internet pelo celular, afirma IBGE. Acesso em: 07 de agosto de 2018. Disponível em: <https://tecnologia.ig.com.br/2018-04-27/acesso-a-internet.html>