FACULDADES METROPOLITANAS UNIDAS

LEONARDO FELIPE DE MELO RIBEIRO GOMES JORGETTO

A PROTEÇÃO CRIPTOGRÁFICA NOS APLICATIVOS DE TROCA DE MENSAGENS INSTANTÂNEAS COMO FORMA DE GARANTIA À PRIVACIDADE NO AMBIENTE DIGITAL.

O conflito entre o direito à privacidade e a segurança pública como direito fundamental

SÃO PAULO

2018

LEONARDO FELIPE DE MELO RIBEIRO GOMES JORGETTO

A PROTEÇÃO CRIPTOGRÁFICA NOS APLICATIVOS DE TROCA DE MENSAGENS INSTANTÂNEAS COMO FORMA DE GARANTIA À PRIVACIDADE NO AMBIENTE DIGITAL.

O conflito entre o direito à privacidade e a segurança pública como direito fundamental

Dissertação apresentada à Banca Examinadora do Centro Universitário das Faculdades Metropolitanas Unidas, como exigência parcial para obtenção do título de Mestre em Direito da Sociedade da Informação.

Orientador: Prof. Dra. Dra. Ana Elizabeth Lapa Wanderley Cavalcanti.

SÃO PAULO

2018

Jorgetto, Leonardo Felipe de Melo Ribeiro Gomes.
A proteção criptográfica nos aplicativos de troca de mensagens instantâneas como forma de garantia à privacidade no ambiente digital – O conflito entre o direito à privacidade e a segurança pública como direito fundamental/
Leonardo Felipe de Melo Ribeiro Gomes Jorgetto. – São Paulo: L.. Felipe de Melo Ribeiro Gomes Jorgetto, 2018.
104 f.

Orientadora: Ana Elizabeth Lapa Wanderley Cavalcanti
Dissertação (mestrado) – Faculdades Metropolitanas Unidas, Mestrado em Direito da Sociedade da Informação, 2018.

1. Privacidade. 2. Segurança Pública. I.
Autor. II. Jorgetto, Leonardo Felipe de Melo Ribeiro Gomes. III. Faculdades Metropolitanas Unidas. Mestrado em Direito da Sociedade da Informação. IV. Título.

CDD 340

LEONARDO FELIPE DE MELO RIBEIRO GOMES JORGETTO

A PROTEÇÃO CRIPTOGRÁFICA NOS APLICATIVOS DE TROCA DE MENSAGENS INSTANTÂNEAS COMO FORMA DE GARANTIA À PRIVACIDADE NO AMBIENTE DIGITAL.

O conflito entre o direito à privacidade e a segurança pública como direito fundamental

Dissertação apresentada à Banca Examinadora do Centro Universitário das Faculdades Metropolitanas Unidas, como exigência parcial para obtenção do título de Mestre em Direito da Sociedade da Informação.

Orientadora: Profa. Dra. Ana Elizabeth Lapa Wanderley Cavalcanti.

Data de aprovação:

___/ ___/_____

Banca examinadora:

Prof. Dra. Ana Elizabeth Lapa Wanderley Cavalcanti

FMU – Orientadora

SÃO PAULO

2018

Ao meu amor Raquel, companheira de todas as horas, incentivadora paciente que sempre esteve disposta a ajudar e compreender.

À minha mãe Susana, pelo apoio e incentivo incondicional que sempre me deu

Ao meu pai João (in memoriam), por sua criação amorosa e confiante.

À minha tia Inês, que com seu amor maternal sempre me acalmou e me reestabeleceu.

AGRADECIMENTOS

Agradeço à professora Dra. Ana Elizabeth Lapa Wanderley Cavalcanti (orientadora) por toda paciência, atenção e orientação prestada e à professora Dra. Greice Patrícia Fuller, apoiadora de primeira hora.

Ao amigo e professor Ms. Eduardo Sorrentino, que muito ajudou nessa jornada.

À professora Alessandra Sutti, motivadora incansável e conselheira certa.

Aos colegas do Mestrado.

Às Faculdades Metropolitanas Unidas (FMU).

RESUMO

O presente trabalho procura identificar os pontos teóricos da discussão sobre o aparente conflito entre o Direito à Privacidade e o dever do Estado em prover a Segurança e a Ordem Pública no que tange ao acesso estatal a conversas privadas no âmbito de aplicativos de troca de mensagens instantâneas mormente a quebra da criptografia que, em tese, protege a privacidade das conversas eletrônicas instantâneas mas também pode impedir a efetividade estatal no que tange à segurança pública. Para tal discorre sobre a dicotomia entre o público e o privado, tanto em perspectiva histórica quanto na atualidade líquida da Sociedade da Informação. Examina, também, a questão da criptografia como ferramenta de efetivação de proteção às conversas privadas e reflete na ponderação que o Estado brasileiro faz sobre essas questões em casos práticos judiciais, em especial o guardião da nossa Constituição Federal, o Supremo Tribunal Federal no julgamento das ações de Arguição de Descumprimento de Preceito Fundamental 403 e a Ação Direta de Inconstitucionalidade 5527.

PALAVRAS CHAVE: privacidade; segurança pública; mensagens instantâneas; criptografia; sociedade da informação

ABSTRACT

The present work seeks to identify the theoretical points of the discussion about the apparent conflict between the Right to Privacy and the State's duty to provide Security and Public Order with regard to state access to private conversations within the framework of instant messaging applications especially the breaking of cryptography, which, in theory, protects the privacy of instantaneous electronic conversations but can also impede state effectiveness in public security. To do so, it discusses the dichotomy between the public and the private, both in historical perspective and in the liquidity of the Information Society. It also examines the issue of cryptography as a tool for effective protection of private conversations and reflects in the consideration given by the Brazilian State to these issues in judicial practical cases, especially the guardian of our Federal Constitution, the Federal Supreme Court in the actions of Arbitration for Non-compliance with Basic Precept 403 and Direct Action of Unconstitutionality 5527.

KEY WORDS: privacy; public security; instant messages; cryptography; information society

SUMÁRIO

INTRODUÇÃO

A dinâmica da sociedade atual gerou diversos conflitos entre as estruturas sociais, políticas e jurídicas existentes e os avanços da sociedade da informação que modificaram diversos paradigmas e criaram fricções nessas estruturas. Esses conflitos, em muitos momentos, são sanados pelo avanço do conhecimento científico, em especial pelas ciências sociais e jurídicas, porém o caótico avanço do mundo digital às vezes cria situações que nem as ciências sociais e nem a ciência jurídica conseguem deslindar de plano, gerando dúvidas e também um campo fértil de discussões acadêmicas.

O nosso sistema jurídico, sedimentado pela Constituição Federal de 1988, por óbvio não pôde prever a rápida ascensão da era digital, da internet e da interconectividade que pauta hoje as relações humanas, criando facilidades mas também gerando novos problemas e, boa parte do labor dos operadores do Direito é mediar as novas situações e resolver os conflitos. Nesse passo, deve-se lembrar também que os Direitos Fundamentais, entre os quais encontraremos os Direitos da personalidade e, especificamente para esse projeto, o Direito à privacidade devem se colocar como o farol a iluminar e pautar a resolução de qualquer conflito.

Os Direitos Humanos, por força da sua característica de historicidade, sempre evoluem acompanhando as necessidades humanas e, embora tenhamos hoje enorme discussão sobre qual dimensão dos Direitos Humanos a proteção aos direitos ligados à informática pertença, é inegável que se ainda não se trata de um Direito Fundamental sedimentado, para isso caminha.

É nesse cenário que se teve, recentemente, um conflito entre princípios de natureza constitucional, orbitado pela crescente massificação do uso de ferramentas de comunicação digital.

Antes de se adentrar no tema, propriamente dito, tem-se que fazer uma breve introdução a esse fenômeno de massificação do uso da comunicação digital, mormente o uso dos chamados troca de mensagens instantâneas (IM - Instant Messaging)

Esse sistema de mensagem instantânea é um meio de comunicação a utilizar uma aplicação que permite o envio e o recebimento de mensagens de texto em tempo real. Por essa aplicação o usuário pode receber mensagens instantâneas de pessoas previamente cadastradas ou não, gerando conversações em tempo real, tanto individualmente como em grupos. Os aplicativos mais populares e modernos de mensagem instantânea incorporam também diversos recursos que vão desde a possibilidade de envio de imagens, vídeos e sons como a possibilidade de criptografar as conversas. Como se vê, o sistema de mensagens instantâneas diferem dos chamados e-mails pelo fato de que as mensagens instantâneas acontecem em tempo real, enquanto os e-mails não necessariamente, muito embora as conversas via mensagens instantâneas possam ter o histórico guardados (salvos) para consulta futura, e ser transmitida com criptografia e nesse ponto há de notar que os provedores de serviços de mensagens instantâneas teriam, em tese, acesso a essas conversas, cuja natureza privada é inegável. Porém para garantir essa privacidade, muitos aplicativos utilizam o sistema de criptografia que tem o objetivo de impedir a publicidade das conversas privadas para outros que não sejam os envolvidos, impedindo (em tese) que o próprio provedor tenha acesso a essas conversas, pois como será explicado adiante a criptografia codifica as conversas, utilizando uma chave criptográfica e apenas os usuários de ponta a ponta tem essa chave, estando (em tese) imunes de terem suas conversas privadas escrutinadas.

Como exemplos de sistemas de mensagens instantâneas temos o Facebook Messenger, BlackBerry Messenger, Wechat, Telegram e Whatspp entre outros.

Não é difícil perceber a evolução das comunicações interpessoais expandindo os horizontes para agasalhar essa atividade humana e proteger os valores fundamentais do Direito, como os Direitos da Personalidade, mais especificamente a privacidade. Sem querer aprofundar no tema, podemos notar que esse não é um fenômeno recente, haja vista que o sistema de comunicação interpessoal eletrônico pode ser rastreado desde o advento do telégrafo, sendo certo que a telefonia ampliou e modificou a própria dinâmica social do mundo

moderno, criando diversos pontos de conflitos que são até hoje objeto de discussão acadêmica, como por exemplo o caso de interceptação telefônica judicial, que tem amplo amparo legislativo, doutrinário e jurisprudencial no campo do Direito brasileiro e, mesmo assim suscita grandes dúvidas e batalhas intelectuais sobre sua aplicação e validade em face de conflitos entre princípios constitucionais como a proteção à privacidade e o direito à garantia da segurança pública.

Existem diferenças essenciais entre as duas formas de comunicação (a telefônica e a via internet como o caso de mensagens instantâneas), diferenças técnicas e jurídicas e um dos questionamentos que temos feito é: Essas diferenças suscitam também diferentes formas de proteção estatal?

Aqui tem-se a velha dicotomia da função Estatal, que pode ser simplificada e exemplificada nas diferentes acepções de Estado (Liberal x Social, entre outros). A nossa própria Constituição Federal transita entre uma Constituição garantista e uma Constituição dirigente, sendo praticamente pacífico que temos um viés muito mais dirigente, sem olvidar o seu caráter garantista.

Esses conflitos vieram à baila com as recentes decisões judiciais que ordenaram a suspensão do sistema de mensagens instantâneas em todo território brasileiro sob o argumento de que tais sistemas estariam a violar o dever fundamental do Estado de garantir a segurança pública eis que, em apertado resumo, investigados estariam utilizando essa nova tecnologia para se comunicarem anonimamente, planejando crimes (e portanto gerando provas de atos ilícitos), sendo inalcançável pela mão do Estado que não dispunha (em tese) de outros meios para interceptar as comunicações que não o auxílio da própria empresa fornecedora desse serviço.

E aqui tem-se justamente colocado o conflito objeto do estudo em pauta.

A segurança pública, enquanto Direito Fundamental insculpido no art. 6º da nossa Carta Política impulsiona o Estado em sua obrigação de prover o homem com o mínimo possível para que ele sinta segurança nas suas relações humanas e na sua vida privada. Portanto, temos um Direito Social positivo que muitas vezes enfrenta os Direitos Fundamentais negativos, criando conflitos aparentes

que devem ser dirimidos pela Ciência do Direito, e esse caso em especial serve de fio condutor para essa discussão.

Para desenvolver o presente trabalho, o principal referencial teórico será Zygmunt Bauman, por entender que a ideia da sociedade líquida penetra nas questões sociais e jurídicas e conseguem explicar a dinâmica do conflito da sociedade de consumo e da sociedade da informação, suas transformações rápidas e o desprezo pelo “sólido” (Estado) em favor do “líquido” (consumo, relações perenes) que podem explicar um pouco melhor a ascensão do Direito à Privacidade. Será utilizado o método dedutivo e estudo de caso para se conseguir chegar a uma conclusão.

O presente trabalho foi construído com base na no método dedutivo, portanto os capítulos se apresentam como premissas na forma a seguir exposta.

O primeiro capítulo tem como objetivo apresentar o conflito entre o público e o privado, analisando historicamente os conceitos de público e privado, sua evolução até sua aproximação com a Sociedade da Informação, em seguida, com essas premissas estudadas passa-se a estudar os conceitos jurídicos e legais dos Direitos à Privacidade e Segurança Pública propriamente ditos, em especial no campo dos Direitos Fundamentais para, finalizar o capítulo com um fechamento sobre a aplicação da Teoria da Proporcionalidade de Robert Alexy e como se pode vislumbrar seu uso em conflitos entre Direitos Fundamentais. Esse primeiro capítulo tem, portanto, o objetivo de construir um pensamento lógico do mais amplo que são conceitos como privacidade e segurança, passando pela codificação desses conceitos no nosso sistema jurídico ao mais específico que é a análise do conflito entre eles no campo teórico.

Faltando ainda subsídios para se proceder, pois muitas são as variáveis ainda não estudadas, passa-se a estudar outras premissas que irão preencher os conceitos estudados. O capítulo 2 trará subsídios mais técnicos, a compreensão de aspectos como a internet, o impacto da mobilidade comucacional e a conceituação de aplicativos de mensagens instantâneas. Esse capítulo tem o propósito de explicar a importância da comunicação instantânea e como isso modificou a forma de se viver em sociedade transformando e dando subsídio a

conceitos estudados no capítulo 1 que ficarão mais claros se observados em conjunto não apenas com a parte técnica trazida pelo capítulo 2, mas também com conceitos sociais e a evolução comandada pela informática.

O Capítulo 3 tende a aprofundar mais a parte técnica, explicando o conceito e a evolução da criptografia, de como ela funciona nos dias de hoje e o que são aplicativos de mensagens instantâneas, quais são os mais utilizados e quais proteções eles têm. Com o Capítulo 3 fecha-se o círculo técnico de informática, trazendo mais a realidade os conceitos tratados anteriormente. Agora, com a ideia de privado e público trabalhada em vários níveis, adequando essa ideia aos conceitos tecnológicos consoante as mudanças que a tecnologia trouxe, suas dificuldades e facilidades, enfrentamos o Capítulo 4, que é o retorno do público e o privado, agora temperado com o conhecimento técnico básico de informática para compreender a realidade jurídica atual com base no estudo de casos trazidos nesse Capítulo 4. Nesse Capítulo serão verificadas as principais decisões a respeito de bloqueio de aplicativos de mensagens móveis, a visão que se tem sobre o assunto na audiência pública e o teor das decisões. Por fim, a conclusão sobre o problema apresentado.

CAPÍTULO 1 – A DICOTOMIA ENTRE O PRIVADO E O PÚBLICO NA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS.

1.1 - A ESFERA PRIVADA E A ESFERA PÚBLICA – PERSPECTIVAS HISTÓRICAS E JURÍDICAS

Antes de se adentrar no assunto propriamente dito e abordado nesse capítulo, vale ressaltar que a dicotomia aqui estudada, *a priori*, é a questão das esferas públicas e privadas sob o ponto de vista do indivíduo e sua relação com o mundo externo, com o público e a evolução histórica e jurídica desses conceitos. Não é a questão de dicotomia entre o Direito Público e o Direito Privado, muito embora do ponto de vista jurídico o público e o privado fatalmente desaguem na questão de Direito Público e Direito Privado e resvale, como se verá, na questão do indivíduo e da pólis, da sociedade ao redor do indivíduo e sua luta pelo espaço privado em meio às transformações histórica e as mudanças conceituais sobretudo da privacidade.

O conceito moderno de privacidade começa a se evidenciar e a se destacar da esfera pública no século XIX quando a burguesia começa a especificar e valorizar a privacidade como uma esfera autônoma destacada e desejada, porém antes desse período chamado de “retorno ao privado; mas não mais o privado no sentido doméstico greco-romano, ou mesmo medieval” (COSTA, 1998, p. 191), devemos compreender que a diferença entre o privado e o público é muito anterior, como informa o historiador Peter Gay (2002, p. 270) ao apontar que os atenienses já distinguiam o domínio público e o domínio privado mas de forma a dar preponderância do primeiro sobre o segundo, exaltando o público e denegrindo o privado. Essa superioridade da esfera pública sobre a privada sobreviveu até a idade média, bastando lembrar, ainda que a palavra para privado em grego era ‘idios’, que também significa pessoa com debilidade mental, ou seja, fiel à ideia de que o público tinha total prevalência sobre o que seria a individualidade, imaginava-se que a proteção à esfera privada, para os gregos, consistia em afronta ao sentido de organização pública, uma idiotia egoísta e individualista.

Mas notemos que os gregos diferenciam a esfera daquilo que é próprio do homem (‘idios’), daquilo que é da casa (‘oikos’) e da esfera pública, dos assuntos da pólis (‘koinon’)

Antes do Iluminismo, ainda de acordo com Gay (2004, p. 271), “a condição humana geralmente aceita era a de viver em um palco”, mormente pelo fato de não haver espaço físico pois as famílias, em geral, residiam em casas pequenas, de um cômodo ou no máximo dois cômodos e temos, de fato, que os assuntos de cada indivíduos eram públicos pois a convivência era pública e até meados do século XIX as camadas mais pobres viviam em cortiços na Inglaterra e era impossível que tivessem um espaço próprio, chegando-se ao caso de a ama-de-leite ter seus mamilos inspecionados pela empregadora para saber se teria condições de exercer seu trabalho (GAY, 2004, p. 272). No século XVIII, Jean Jaques Rousseau busca um intimismo, regando a subjetividade no valor da privacidade e pavimenta a ideia liberal que haveria de pautar a privacidade nos séculos futuros.

É importante notar que essa mudança da dicotomia entre o privado e público, esse movimento pendular do valor do público para o privado trazido a partir do século XVIII é fruto da ascensão burguesa que começa a buscar um espaço privado mais restrito, transformando a ideia de privacidade em círculo especial de acesso para poucos enquanto a esfera pública se tornaria cada vez mais uma questão social.

Percebe-se essa evolução do conceito de privacidade em decorrência da facilidade de acesso a informações e fatos privados da população, especialmente com o início da migração do rural para a metrópole, que cria uma condição de proteção necessária, um individualismo novel que encontra supedâneo nos novos conceitos de privacidade.

Nesse passo, marco histórico crucial defendido por Doneda (2006, p. 137) como sendo a gênese do sentido de privacidade da sociedade moderna é a publicação do artigo “The Right to Privacy” , de Warren e Brandeis e publicado na Harvard Law Review em 1890, que alerta para os perigos da tecnologia

devassando a privacidade do homem, listando aparatos tecnológicos como máquina fotográfica, por exemplo. Começa dessa forma a dissociação entre da proteção da vida privada com a propriedade:

> o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade (WARREN: BRANDEIS, 1890, p. 205)

Prontamente se vê uma clara ligação entre a ascensão da burguesia e o avanço tecnológico como forma de fortalecimento do discurso mais liberal de preservação do espaço privado e, concomitantemente a mutação do conceito de questões públicas.

O início da materialização do conceito de privacidade moderna é melhor delimitado por Warren e Brandeis (1890, p. 214 – 218) da seguinte forma:

(I) o direito à privacidade não impede a publicação do que é de interesse geral;

(II) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito;

(III) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos;

(IV) o consentimento do afetado exclui a violação do direito;

(V) a alegação de veracidade da informação pelo agressor não exclui a violação do direito;

(VI) a ausência de dolo também não exclui a violação desse direito;

Do amálgama do crescimento urbano, da ascensão da burguesia e da evolução tecnológica surge a conceituação da privacidade como o direito de ser deixado em paz, sedimentando o direito da personalidade como um direito

intrínseco ao ser humano e separado, de maneira bastante clara da ordem pública.

Por esse ponto, a questão da dicotomia entre o público e o privado começa a criar relevos claros enquanto distinguimos as questões privadas das questões públicas, devendo esse último ser objeto de proteção estatal tanto quanto o primeiro, e assim o é de maneira bastante clara no nosso ordenamento jurídico.

> Toda vez que falamos de coisas que só podem ser experimentadas na privatividade ou na intimidade, trazemo-las para uma esfera na qual assumirão uma espécie de realidade que, a despeito de sua intensidade, elas jamais poderiam ter tido antes. A presença de outros que veem o que vemos e ouvem o que ouvimos garante-nos a realidade do mundo e de nós mesmos. (ARENDT, 2008, p. 60)

Essa dicotomia inicial entre o público e o privado é muito bem explicada por Hannah Arendt ao afirmar que as questões privadas tornam-se imediatamente públicas no momento que são difundidas dando-se acesso público ao que antes era privado:

Todavia, Arendt traça certos limites ao informar que existem coisas que são insuportáveis sob o escrutínio público, que não suportam a luz da esfera pública e que tudo aquilo que é irrelevante para a esfera pública remete a esfera privada (ARENDT, 2008, 61).

Por fim, para Arendt (2008, p. 65), “É o caráter público da esfera pública que é capaz de absorver e dar brilho através dos séculos a tudo o que os homens venham a preservar da ruína natural do tempo”.

1.2 - A SOCIEDADE DA INFORMAÇÃO COMO AGENTE DA MUTAÇÃO DAS ESFERAS PRIVADAS E PÚBLICAS.

A Sociedade da Informação ou Sociedade do Conhecimento ou ainda Sociedade Pós-Industrial é, de acordo com Roberto Senise Lisboa (2006, p. 10), uma expressão que identifica um período histórico que tem na informação o ponto focal, com preponderância dessa sobre os meios de produção, contendo não apenas a informática, mas a própria comunicação de dados estendendo-se da

televisão a cabo a computadores ou qualquer tipo de comunicação, presencial ou não, que use os dados como base.

Esse conceito de Sociedade da Informação é também trabalhado relacionando conceitos de produção e valor da seguinte forma:

> Na gênese semântica da expressão, há uma junção conceitual entre informação e modo de produção, como ocorre com o capitalismo e o socialismo, porém, revelando o resultado de inovações históricas promovidas pelo avanço tecnológico que atribuem à informação o status de principal mercadoria, ou valor, a ser produzido e perseguido no terceiro milênio, reorganizando as economias capitalistas e esse modo de produção. (BARRETO JÚNIOR, 2007, p. 62)

A informação, agora alçada ao status de mercadoria com alta carga valorativa na sociedade informacional, gera ampla modificação nos conceitos de público e privado eis que o rápido fluxo de informações cria novas formas de relações humanas que necessitam de novos conceitos.

A partir do século XX as transformações tecnológicas formaram, na ideia de Manuel Castells (2005, passim), uma revolução que ultrapassou em muito os limites técnicos informatizados permeando toda a sociedade, ampliando seus limites e abarcando praticamente todos os aspectos da vida moderna.

Segundo Castells (2005, p. 265), sempre houve informação na história da sociedade, a diferença seria a necessidade de substituir o ponto de vista estático das relações de antes por um novo paradigma dinâmico, de complexos informacionais organizados em redes que pela sua natureza causariam grande mudanças em vários fatores como o poder e a cultura e, também, por óbvio, na esfera privada.

Entre os antigos conceitos de diferenciação entre esferas privadas e esfera pública é a teoria dos círculos concêntricos que, elaborada em 1953 por Heinrich Hubmann, explica o sentimento de privacidade como círculos com graus diferentes de densidade em que o círculo maior se refere a privacidade, o círculo intermediário ao segredo e o menor, nuclear, se refere à intimidade (SZANIAWSKI, 1993. p. 337). Sem embargo, Heinrich Henkel desenvolveu mais

tal teoria de modo a enxergar os círculos concêntricos com uma esfera mais interior, que seria a do segredo, a esfera intermediária como da intimidade e a esfera mais externa a privacidade stricto sensu. Dessa forma, a esfera mais externa seria a da privacidade que conteria as relações mais rasas, em que o interlocutor do sujeito de direitos teria acesso a certos dados comuns a todos que tenham algum tipo de contato relativos a convivência normal do mundo moderno e que excluiria apenas aqueles que não tem contato algum com o referido sujeito de direitos enquanto a esfera intermediária, da intimidade, conteria dados disponíveis ao círculo mais íntimo de convivência contendo aqui informações relativas a sigilo familiar, profissional e algumas ligações telefônicas. A esfera do segredo seria a esfera mais íntima, que contaria com as informações que não são normalmente compartilhadas com outros indivíduos, intocável aos outros, como por exemplo a opção sexual e política.

Portanto, quanto mais interna for a esfera, maior será a distância entre o público e o privado (com prevalência do último), e essa visão de proteção à privacidade evoluiu, como se vê, em virtude do foco nas relações pessoais, no aumento da importância e preponderância do capital privado na vida das pessoas e que, com a valorização da informação até mesmo como bem de capital, gera uma mudança drástica na importância que se dá na esfera privada em relação a esfera pública.

A esfera pública perde espaço com a ideia liberal de proteção dos direitos da personalidade, afastando o poder público das esferas mais internas da privacidade, salvo exceções específicas que visam a proteção da sociedade, onde ainda se tem uma certa prevalência da esfera pública sobre a privada como se verá mais adiante.

Porém, a Sociedade da Informação tem como uma de suas característica a liquidez emprestada da sociedade moderna de consumo fazendo com que mesmo o conceito de esferas concêntricas acabe não mais servindo de maneira estanque para explicar os conflitos e limites entre os diversos níveis de privacidade e a esfera pública, transmutada em alguns aspectos como o da

ordem pública que passa a digladiar com a ideia de espaço privado absoluto (mas líquido) ao tentar garantir direitos sociais como o da segurança pública. Nesse ponto, o conflito entre uma modernidade líquida (baseada em indivíduos focados em si e nas suas esferas privada, baseada principalmente no consumo) e a tentativa de manutenção da solidez do status quo (poder estatal protetor da sociedade como um todo) é muito bem explicada por Bauman:

> "O "derretimento dos sólidos", traço permanente da modernidade, adquiriu, portanto, um novo sentido, e, mais que tudo, foi redirecionado a um novo alvo, e um dos principais efeitos desse redirecionamento foi a dissolução das forças que poderiam ter mantido a questão da ordem e do sistema na agenda política. Os sólidos que estão para ser lançados no cadinho e os que estão derretendo neste momento, o momento da modernidade fluida, são os elos que entrelaçam as escolhas individuais em projetos e ações coletivas – os padrões de comunicação e coordenação entre as políticas de vida conduzidas individualmente, de um lado, e as ações políticas de coletividades humanas, de outro." (BAUMAN, 2001. p. 12).

Um dos marcos históricos que radicalizou a proteção de dados privados na sociedade moderna em face do poder estatal foi a decisão do Tribunal Constitucional Alemão no julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 25-3-1982 que é considerada uma referência sobre como o indivíduo deve ter o controle sobre o fluxo de informações na sociedade (MENDES, 2014, p. 30). O Tribunal Constitucional Alemão decidiu pela inconstitucionalidade parcial da lei com base na proteção da dignidade da pessoa humana e o livre desenvolvimento da personalidade. Tal lei tinha como objetivo a coleta de dados dos cidadãos (profissão, moradia e local de trabalho) para que a administração pública tivesse informações sobre o crescimento populacional com o intuito de desenvolver políticas públicas. A lei previa multa para o cidadão que se recusasse a ceder seus dados além de informar que os dados seriam comparados com registros anteriores com a finalidade de averiguar a veracidade das informações fornecidas.

O Tribunal Constitucional conheceu o reclamo constitucional, declarando nulos os dispositivos que ordenavam a comparação dos dados coletados e a

transferência desses dados para outros órgãos da administração (MENDES, 2014, p. 31).

Essa decisão demonstra como a questão da proteção da esfera privada tornou-se uma obrigação de proteção estatal na sociedade moderna, comprovando a tendência de não apenas vislumbrar o direito à privacidade como um direito fundamental que deve ser protegido quase que de maneira absoluta, mesmo em face de argumentos de ordem pública, como também demonstra a nova importância que se dá a dados pessoais, como os referentes a profissão e moradia que antes poderia ser considerado uma esfera menos autônoma de privacidade e que, de acordo com o entendimento do Tribunal Constitucional Alemão nesse julgamento merece proteção pois é também considerado um representante do livre desenvolvimento da personalidade.

A Sociedade da Informação gerou uma enorme produção de dados em decorrência do avanço tecnológico e, em consequência se viu mergulhada em um novo universo cujas fronteiras entre o público e o privado não ficam tão claras. A vertiginosa velocidade da troca de informações e o amplo abastecimento de dados que nós mesmos fornecemos cria uma fronteira líquida de difícil conceituação entre o que são dados privados e o que são dados públicos. De fato, ao se mergulhar nessa sociedade tem-se muitos valores modificados a título de pagamento pelas maravilhas da inclusão digital.

A revolução trazida pela Sociedade da Informação modificou, portanto, o direito à vida privada, como bem explica Stefano Rodotá:

> “O desenvolvimento da informática colocou em crise o conceito de privacidade, e, a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em banco de dados.” (RODOTÀ, 2008. p. 267).

Como se não bastasse a explicação de Rodotá acerca da mudança de entendimento sobre privacidade em decorrência da revolução da Sociedade da Informação, tem-se que notar o fato dessa nova era digital trazer também, na esteira da inclusão digital, uma certa mudança de visão a respeito do que é

visibilidade, alargando ainda mais a esfera da privacidade. Não se trata mais de temer os 15 minutos de fama, mas buscá-la de maneira incessante. O pesadelo orwelliano do Grande Irmão (Big Brother – não por acaso título de um afamado programa televisivo de grande audiência) tornou-se o sonho do consumidor digital, a ponto de Bauman (2013, p. 30) afirmar que trocamos o pesadelo pan-óptico de “Nunca estar sozinho” pela esperança de “Nunca mais vou ficar sozinho”.

O próprio Bauman (2014, p. 28) ensina que o sacrifício da privacidade no mundo moderno pode ser o pagamento do preço por maravilhas oferecidas ou uma irresistível pressão social de sacrificar a autonomia pessoal no que tange ao manejo de sua própria privacidade a ponto de apenas alguns poucos indivíduos conseguirem resistir, relegando a maioria de nós a condição de ovelhas oferecidas em troca, ou seja mesmo que se pense que nem sempre, por livre e espontânea vontade, sacrifica-se a esfera privada em prol do público como paga pela ‘cidadania digital’, ainda assim a própria Sociedade da Informação exige, de maneira quase irresistível, que se sacrifique essa privacidade em nome do acesso aos benefícios digitais que imaginamos necessários. Mesmo que não se queira que nossos dados sejam utilizados, por exemplo, pelo Facebook, sabe-se que se não permitirmos livre acesso a esses dados de navegação pela empresa fornecedora de acesso, não se poderá conectar com amigos e colegas de trabalho via rede social. As fronteiras privadas diminuem pela força opositora da sociedade de consumo, aliada da Sociedade da Informação.

1.3 - O DIREITO À PRIVACIDADE COMO DIREITO DA PERSONALIDADE E SUA CONSTRUÇÃO TEÓRICA E LEGAL.

Os direitos da personalidade, na forma mais próxima como se conhece, foram criados na segunda metade do século XIX e tiveram essa expressão concebida por jusnaturalistas franceses e alemães para designar certos direitos inerentes ao homem, tidos como preexistentes ao seu reconhecimento por parte do Estado, essenciais ao ser humano (SCHREIBER, 2014. p. 5).

Sempre existiu uma enorme dificuldade em delimitar o que seriam os direitos da personalidade, sendo certo que a maioria das doutrina o considera como os direitos inerentes a própria pessoa o que causou, também grande celeuma em autores clássicos como Savigny que negava a existência dos direitos da personalidade por considera-los inconsistentes, uma contradição em si mesma eis que eram direitos que tinham o próprio sujeito como objeto (nessa acepção, seria um intransponível paradoxo pois se a personalidade consistia na capacidade de ter direitos, não podia essa mesma personalidade ser objeto de direito) (SCHREIBER, 2014. p. 5).

A dissonância existe por se confundir os aspectos subjetivos com os aspectos objetivos. A pessoa é sujeita de direitos, eis aqui o aspecto subjetivo, enquanto objetivamente, ou seja externamente, tem-se o conjunto de direitos que chamamos de personalidade que se pode delimitar da seguinte forma:

> São prerrogativas de toda pessoa humana pela sua própria condição, referentes aos seus atributos essenciais em suas emanações e prolongamentos, são direitos absolutos, implicam num dever geral de abstenção para a sua defesa e salva- guarda, são indisponíveis, intransmissíveis, irrenunciáveis e de difícil estimação pecuniária. Outrossim, são inatos (originários), absolutos, extrapatrimoniais, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis erga omnes, segundo a melhor doutrina e o artigo 11 do Código Civil". (BITTAR, 2003, p. 11).

Nessa concepção, pode-se usar ainda a lição de Bittar para explicar as duas acepções essenciais dos direitos da personalidade (BITTAR, 2003, p. 41):

a) os próprios da pessoa em si (originários), existentes por sua natureza, como ente humano, com o nascimento;

b) e os referentes às suas projeções para o mundo exterior (a pessoa como ente moral e social, ou seja, em seu relacionamento com a sociedade).

Nessa segunda acepção pode-se colocar, por exemplo, o direito à privacidade cuja construção jurídica que tanto se encontra encartado como um

direito formal e materialmente fundamental em nossa Carta Magna[1] quanto no Código Civil, nesse último em apenas em um único artigo[2].

A esses dispositivos, tem-se também que fazer uma leitura conjunta do artigo 11 do Código Civil[3] posto que essa previsão legal é que agasalha o direito a privacidade como irrenunciável e ilimitado (mesmo em caso de limitação voluntária) e cria alguns questionamentos.

Por aqui deve-se açular o debate sobre os limites da proteção ao direito à privacidade posto que, dentro da construção teórica e legal aqui trazida, se não observarmos mais atentamente o construto jurídico, parece restar pouca dúvida sobre o caráter absoluto da proteção à privacidade. E essa discussão é de enorme importância pois carecemos de uma construção legislativa mais complexa que delimite a realidade social em confronto com a nova realidade dos direitos da personalidade em especial de seu caráter liberal. Não há, como se sabe, esse caráter absoluto de proteção ao direito à privacidade, muito embora a leitura legislativa em primeiro momento parece assim indicar. Não se pode ter caráter absoluto em nenhum direito fundamental, porém no caso do direito à personalidade os problemas são maiores e remontam ao questionamento da própria gênese dos direitos da personalidade e o confronto entre a subjetividade e a objetividade desses direitos. O nosso sistema jurídico já pacificou o entendimento de que há limites à proteção dos direitos à privacidade, como no julgado da Ação Declaratória de Inconstitucionalidade 4815, o famoso caso das biografias não autorizadas, que questionava a constitucionalidade dos artigos 20 e 21 do Código Civil. Esse caso é emblemático pois ultrapassa até mesmo a questão de se abrir mão ou não da proteção do direito à privacidade, que no texto

---

[1] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(…)
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

[2] "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

[3] "Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária."

de lei é considerada irrenunciável e inalienável, posto que aqueles que em tese tiveram seus direitos da personalidade violados não abriram mão deles, ao contrário, exigiram daqueles que pretendiam escrever biografias sobre suas vidas e intimidades tivessem uma prévia permissão para fazê-lo.

O conflito entre direitos fundamentais é claro, como o da liberdade expressão, da vedação de censura e dos direitos da personalidade. A parte da decisão, em ementa, que melhor expressa esse pensamento foi a que segue:

> (...) 8. Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade da intimidade, da privacidade, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias. (BRASIL, 2016b)

Dessa forma fica muito claro que há limites na proteção do direito à privacidade, mormente quando em conflito com outro direito fundamental. Nesse mesmo sentido e de uma maneira muito mais simples, o Tribunal de Justiça do Rio de Janeiro decidiu que uma modelo não merecia indenização por violação ao seu direito da personalidade por fazer topless em local público:

> Indenização responsabilidade civil. Publicação jornalística. Dano moral. Inocorrência. Modelo profissional. Direito a imagem. Violação do direito. Inexistência descabimento sentença confirmada. Desprovimento do recurso. Responsabilidade civil. Fotografia publicada em revista semanal. Dano moral. Inocorrência. Modelo flagrada quando fazia topless na piscina de um hotel. Pessoa pública que voluntariamente expôs sua imagem em local de acesso público. Inexistência de violação ao seu direito de intimidade. Indenização descabida. Desprovimento do recurso. Manutenção da sentença que julgou improcedente o pedido inicial". (TJRJ, ApCiv. 0122463-44.1997.8.19.0001, 2.ª Câm. Cív., rel. Des. Leila Mariano, *DJ* 17.04.2001). (BRASIL, 1997)

Portanto a voluntariedade, a autonomia da vontade de desconstruir a rede protetiva sobre os direitos da personalidade tem o condão de inibir os efeitos, em tese absolutos, irrenunciáveis e inalienáveis dos direitos da personalidade. Não poderia ser diferente, por óbvio, eis que na modernidade líquida em que vivemos, uma concepção absoluta de um direito, mormente em casos que envolvem outros

direitos fundamentais, não tem espaço, precisa se diluir frente aos desafios e vontades diversas da nossa Sociedade da Informação.

O grande desafio imposto hoje é de se proteger os direitos da privacidade e a, ao mesmo tempo, torna-los elásticos e permeáveis, posto que a Sociedade da Informação obriga essa liquidez nas relações interpessoais, no alargamento da esfera privada como paga de acesso aos benefícios consumeristas dessa realidade capitalista e de rápido consumo somado ao fato de haver uma questionável proteção aos direitos da personalidades, agora cheios de exceções, na maioria vinculados à própria vontade do usuário que não raro abre mão dessa proteção de maneira consciente ou inconsciente, direta ou indireta, o que gera uma resposta e uma nova visão sobre o direito à privacidade com vistas a essa nova realidade da modernidade líquida.

Continua a existir a tensão entre a necessidade de haver uma proteção jurídica mínima à privacidade e a necessidade de exposição como forma de acesso a essa nova cidadania digital. Com isso, novas camadas do direito à privacidade surgem, uma mutação natural em vista da irradiação dos avanços tecnológicos para as relações sociais e os novos paradigmas protetivos. Uma das formas de nova categorização da privacidade no ambiente digital, nascida da necessidade de se criar um patamar protetivo mínimo maior, é a criação do que a doutrina e a legislação chamam de dados sensíveis e que é melhor definida como um determinado dado de informação que, conhecido e processado, poderia potencialmente ser utilizado de maneira discriminatória ou especialmente lesiva representando maiores riscos potenciais para o indivíduo do que na média o seriam dados não sensíveis (DONEDA, 2006, p. 160).

Por esse raciocínio, dados e informações capazes de afetar individuo a ponto de causar, em maior grau, grande perturbação e desconforto em sua vida pessoal e intimidade seriam categorizados como dados sensíveis, cuja definição podemos encontrar no General Data Protection Regulation europeu que entrará em vigor em 25 de maio de 2018 da seguinte forma:

> Artigo 9 (1) - É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (COUNCIL OF EUROPEAN UNION INTERINSTITUTIONAL FILE, 2015)

Como uma irradiação, essa necessidade de dar maior proteção a dados sensíveis se espalha pelo mundo está presente no Brasil também por força do projeto de lei 5276/16, em trâmite na Câmara dos Deputados, e que trata sobre proteção de dados pessoais em seu artigo 5º, inciso III[4] define dados sensíveis como os dados pessoais sobre a origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou organizações de caráter filosófico, religioso ou político bem como dados referentes a saúde, vida sexual e dados genéticos e biométricos.

Dessa forma pode-se perceber que há um movimento no sentido de criar proteções específicas para informações privadas sensíveis, ainda que essa proteção não possa ser absoluta, tanto a legislação europeia como o projeto de lei brasileiro tendem a proteger o núcleo dos dados sensíveis, salvo algumas exceções como no caso de haver consentimento livre, inequívoco, informado, expresso e específico do titular para o uso desses dados. Nesse mesmo passo, o GDPR europeu também exige aprovação explícita do titular para o processamento desses dados e, entre outras exceções menos abrangentes, cria a exceção para o caso desse tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular. Não se pode negar, portanto, que essa nova categorização de dados privados tem gênese na necessidade protetiva em face da voracidade informacional do capital que trata dados pessoais, sejam eles quais forem, como valorosa mercadoria, criando-se essa nova esfera privada em que se vinculam exceções ao uso de dados

[4] Art. 5º - Para os fins dessa lei, considera-se: (…) III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;

sensíveis por terceiros a casos muito específicos e ao aspecto volitivo do titular do direito, ou seja, como regra, a proteção aos dados sensíveis atende à proteção da privacidade do indivíduo como valor inicial degradando-se apenas nos casos previstos em lei e pela expressa e inequívoca vontade do titular.

Um aspecto que se pode trazer para ilustrar a mudança de perspectiva dos Direitos da Personalidade frente aos desafios da Sociedade da Informação é o direito ao esquecimento.

Aqui se demonstra as mudanças ocorridas no Direito à Privacidade como espécie de Direito da Personalidade frente a Sociedade da Informação, e o Direito ao Esquecimento é uma nova espécie de Direito da Personalidade que nos serve para demonstrar as mudanças que certos Direitos sofrem com o alargamento das esferas privadas.

Esse desdobramento do Direito à Privacidade, também chamado “the right to be alone”, representa a necessidade do indivíduo de se ausentar da memória coletiva, o direito que se tem de não ser lembrado a todo momento, em especial quando se trata de fatos antigos que já cumpriram seu papel e que hoje serve como fonte de angústia e agonia, mormente quando se tratam de erros antigos que já foram superados de alguma forma.

Nas palavras de Anderson Schreiber (2014, p. 172)

> A internet não esquece. Ao contrário dos jornais e revistas de outrora, cujas edições antigas se perdiam no tempo, sujeitas ao desgaste do seu suporte físico, as informações que circulam na rede ali permanecem indefinidamente. Pior: dados pretéritos vêm à tona com a mesma clareza dos dados recentes, criando um delicado conflito no campo do direito. De um lado, é certo que o público tem direito a relembrar fatos antigos. De outro, embora ninguém tenha direito de apagar os fatos, deve-se evitar que uma pessoa seja perseguida, ao longo de toda a ida, por um acontecimento pretérito.

Veja-se que mais um conflito se faz aqui, entre o Direito ao Esquecimento e o Direito à Informação.

Logo se vê que o Direito à Privacidade, enquanto um Direito da Personalidade, ganha novos contornos com o avanço da tecnologia e com isso novos conflitos surgem e o Direito nem sempre está equipado para lidar com isso.

1.4 O DIREITO À SEGURANÇA PÚBLICA E SUA CONSTRUÇÃO TEÓRICA E LEGAL ENQUANTO DIREITO FUNDAMENTAL.

Primeiramente deve-se delimitar o tema aqui tratado, eis que há muita confusão entre ordem pública e segurança pública e haveremos de notar que essa confusão existe até mesmo no texto da nossa Constituição Federal.

Para Lazzarini a segurança pública é uma espécie do gênero ordem pública:

> temos entendido ser a segurança pública um aspecto da ordem pública, ao lado da tranquilidade e da salubridade públicas. [...] Cada um deles é por si só a causa do efeito ordem pública, cada um deles tem por objeto assegurar a ordem pública. (LAZZARINI, 1995, p 53).

E, para melhor explicar ordem pública, Lazzarini citando Bernard, afirma que a ordem pública tem como objeto a segurança pública, mas também a tranquilidade e a salubridade pública. Também é esse o pensamento de José Afonso da Silva (1994, p. 622) que entende ser a ordem pública uma busca pela paz social em que a segurança pública é uma das ferramentas.

Esse entendimento é retirado do caput do caput do art. 6º [5] da Constituição Federal, no capítulo de direitos sociais dentro do título dos direitos e garantias fundamentais e também em seu art. 144[6] do mesmo diploma, ou seja, trata-se de um direito formal e materialmente fundamental.

Aqui deve-se delimitar as esferas de proteção dos direitos fundamentais; Uma seria a clássica obrigação negativa do Estado de não ferir os direitos e

[5] "Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição. " (BRASIL, 1988).

[6] "Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos (...)" (BRASIL, 1988)

garantias individuais, colocando o Estado como o sujeito adversário de certos direitos, entre eles, por exemplo, o direito à privacidade e, por isso, a Carta Magna cria um espaço em que o Estado deve-se se abster de intervir ou abusar de seu poder para não limitar a própria dignidade da pessoa humana. Nesse plano, Gilmar Mendes (2014, p. 632) aponta que havendo a violação do Estado frente a um desses direitos fundamentais, o indivíduo tem a correspondente pretensão que pode consistir em:

> 1) pretensão de abstenção (Unterlassungsanspruch);
> 2) pretensão de revogação (Aufhebungsanspruch);
> 3) pretensão de anulação (Beseitigungsanspruch);
>
> E ainda mais duas relativas diretamente ao direito de defesa ou de liberdade:
>
> 1) pretensão de consideração com ponderação do caso concreto (Berücksitigungsanspruch);
> 2) pretensão de defesa ou de proteção em face de terceiro (Schutzanspruch);

A outra esfera da proteção a direitos fundamentais por parte do Estado se verifica nos direitos fundamentais de segunda dimensão, ou seja, direitos sociais que exigem uma prestação positiva, uma ação concreta do Estado que se não for prestada configurará numa ofensa ao princípio da dignidade da pessoa humana, ou seja, no caso do Estado deixar de prestar sua obrigação constitucionalmente prevista estará impondo uma violação a efetividade da própria condição humana. Tal é o caso da obrigação de prover segurança insculpido no caput do art. 6º da Constituição Federal. Para essas obrigações positivas, Mendes (2014, p. 638) assinala três espécies de deveres para o Estado:

1) o dever de proibição (Verbotspflicht), que consiste na obrigação estatal de ativamente proibir determinada conduta;

2) o dever de segurança (Sicherheitspficht), que impõe o dever do Estado de proteger o indivíduo contra ataques de terceiros;

3) o dever de evitar riscos (Risikopflicht), que autoriza o Estado a prevenir o risco pra o cidadão em geral mediante a adoção de medidas de proteção, especialmente em relação ao desenvolvimento técnico ou tecnológico;

Nesse arcabouço jurídico, a questão da ordem pública nos interessa apenas quando se refere a segurança pública e a própria questão de segurança pública, a título de estudo aqui proposto, se limita ao conceito de segurança pública enquanto objeto da ordem pública e objetivo do Estado, não nos debruçando sobre a questão da construção da segurança pública quanto aos seus órgãos e organização administrativa.

É claro que a questão da segurança pública é impossível de ser destacada de seus efetivos órgãos, mas para esse capítulo em específico nos importa saber o conceito jurídico de segurança pública para que possamos traçar um paralelo, em termos de direitos fundamentais com o direito da personalidade.

A essa questão de segurança pública retornamos a dicotomia entre público e privado e podemos, também, retornar no tempo para lembrar que

As teorias contratualistas que se iniciaram no século XVII ensinam sobre o pacto entre os homens que renunciaria a parte de seus direitos em busca da segurança e da liberdade, criando um refluxo na ideia de que a segurança do homem era um problema individual. Dessa forma o Estado tem uma função de fornecedor da segurança, momento em que o homem se verga ao poder Estatal, diluindo sua própria autonomia da vontade em busca do bem comum.

Esse poder / dever do Estado em exercer a força para manter a ordem pública, pela via da segurança pública e seus órgãos é aceita como uma necessidade social para o bem-estar e convívio. A força física pode se impor em alguns casos sobre direitos e garantias individuais para garantir outros direitos e garantias individuais, conforme se têm na explicação a seguir.

> Em situações de injusta agressão a bens jurídicos como a vida ou à integridade física, o estado de segurança pode vir a ser alcançado através do uso da força física, que é empregado, naturalmente, como exercício do poder. (BOBBIO, 2004, p. 1292)

O indivíduo aceita essa interferência em sua vida privada como um exercício natural do poder de polícia do Estado, de fato na atualidade principalmente, o indivíduo tem reforçado esse papel do Estado de garantidor da paz e da segurança.

Esse entendimento encontra eco nos julgados da nossa Suprema Corte que compreende a especialidade da segurança pública como obrigação do Estado a ponto de dar provimento a medida cautelar (posteriormente, ratificada com a procedência da ação principal) na ADI 1942 [7] e rechaçar uma lei, a lei 6.010 de 1996 do Estado do Pará que instituía uma taxa de serviço de segurança pública em casos de solicitação de apoio da polícia militar para eventos privados. A argumentação que assegurou a inconstitucionalidade da lei nesse ponto foi de que o serviço de segurança pública é indivisível e para todos, uma obrigação do Estado para com todos, independentemente de pagamento de taxa.

Há na doutrina e na jurisprudência uma certa dificuldade em se delimitar o conceito de segurança pública. A maior parte da doutrina e dos julgados brasileiros acabam por vislumbrar mais a parte formal do que parte material da segurança pública. Ou se concentra na questão da responsabilidade estatal em fornecer a segurança pública (e aqui muito se confunde com ordem pública) ou se concentra na organização dos órgãos de segurança pública.

De fato, as definições aqui trazidas também sofrem de um certo grau de ambiguidade e elasticidade, tal qual a definição de privacidade. Porém nota-se

[7] “EMENTA: Ação direta de inconstitucionalidade. Art. 2º e Tabela V, ambos da Lei 6.010, de 27 de dezembro de 1996, do Estado do Pará. Medida Liminar. - Em face do artigo 144, "caput", inciso V e parágrafo 5º, da Constituição, sendo a segurança pública, dever do Estado e direito de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através, entre outras, da polícia militar, essa atividade do Estado só pode ser sustentada pelos impostos, e não por taxa, se for solicitada por particular para a sua segurança ou para a de terceiros, a título preventivo, ainda quando essa necessidade decorra de evento aberto ao público. - Ademais, o fato gerador da taxa em questão não caracteriza sequer taxa em razão do exercício do poder de polícia, mas taxa pela utilização, efetiva ou potencial, de serviços públicos específicos e divisíveis, o que, em exame compatível com pedido de liminar, não é admissível em se tratando de segurança pública. - Ocorrência do requisito da conveniência para a concessão da liminar. Pedido de liminar deferido, para suspender a eficácia "ex nunc" e até final julgamento da presente ação, da expressão "serviço ou atividade policial-militar, inclusive policiamento preventivo" do artigo 2º, bem como da Tabela V, ambos da Lei 6.010, de 27 de dezembro de 1996, do Estado do Pará.” (BRASIL, 1999)

que enquanto a definição de privacidade parece ter merecido uma atenção maior, a questão de segurança pública acaba tendo um foco maior no aspecto formal, o que pode explicar muitos dos conflitos entre segurança pública e defesa da privacidade. E esse conflito tem algumas características que serão melhor estudadas nos capítulos posteriores, porém podemos dizer que tal qual o direito a privacidade, o direito a segurança pública é indisponível [8], e é um direito positivo do Estado.

1.5 - ANÁLISE DA QUESTÃO DO CONFLITO ENTRE DIREITOS FUNDAMENTAIS E A TEORIA DA PROPORCIONALIDADE DE ROBERT ALEXY.

Tradicionalmente os Direitos Fundamentais são divididos em 3 dimensões, respectivamente baseadas no lema da Revolução Francesa (Liberdade, Igualdade e Fraternidade) e representando esferas de proteção, como por exemplo, a 1ª dimensão (Liberdade) dos Direitos Fundamentais se refere a direitos negativos, oponíveis ao Estado, representando as conquistas liberais da sociedade enquanto a 2ª dimensão (Igualdade) representa os direitos sociais, as liberdades positivas, aquelas que obrigam o Estado a um dever e que tem como marco histórico a Revolução Industrial e a obrigação de se forçar a mão do Estado a uma postura mais ativa. Aqui não mais se requer a ausência do Estado opressor, mas sim o Estado paternal, clama-se por uma intervenção reguladora do Estado, conforme se depreende a seguir:

> As Constituições do México (1917) e de Weimar (1919) trazem em seu bojo novos direitos que demandam uma contundente ação estatal para sua implementação concreta, a rigor destinados a trazer consideráveis melhorias nas condições materiais de vida da população em geral, notadamente da classe trabalhadora. Fala-se em direito à saúde, à

[8] *"*O direito a segurança é prerrogativa constitucional **indisponível**, garantido mediante a implementação de políticas públicas, impondo ao Estado a obrigação de criar condições objetivas que possibilitem o efetivo acesso a tal serviço. É possível ao Poder Judiciário determinar a implementação pelo Estado, quando inadimplente, de políticas públicas constitucionalmente previstas, sem que haja ingerência em questão que envolve o poder discricionário do Poder Executivo.
[RE 559.646 AgR, rel. min. Ellen Gracie, j. 7-6-2011, 2ª T, *DJE* de 24-6-2011.]
= ARE 654.823 AgR, rel. min. Dias Toffoli, j. 12-11-2013, 1ª T, *DJE* de 5-12-2013" (grifo nosso)

> moradia, à alimentação, à educação, à previdência etc. Surge um novíssimo ramo do Direito, voltado a compensar, no plano jurídico, o natural desequilíbrio travado, no plano fático, entre o capital e o trabalho. O *Direito do Trabalho*, assim, emerge como um valioso instrumental vocacionado a agregar valores éticos ao capitalismo, humanizando, dessa forma, as até então tormentosas relações jus laborais. No cenário jurídico em geral, granjeia destaque a gestação de normas de ordem pública destinadas a limitar a autonomia de vontade das partes em prol dos interesses da coletividade." (SARNENTO, 2006, p. 9)

Aqui podemos compreender também entre os direitos de 2ª dimensão direitos como trabalhistas, saúde e segurança pública.

Por fim, tem-se os direitos de 3ª dimensão (fraternidade) que são os direitos à fraternidade, a solidariedade, são os direitos difusos e coletivos como o direito a um meio-ambiente saudável, aqui olha-se o ser humano como um todo, sem distinções, fraternos.

Pois bem, existem outras classificações das dimensões dos Direitos Humanos, ampliando-se ainda mais esse número, porém para o presente trabalho nos basta examinar esses direitos. De fato, nos basta examinar as duas primeiras dimensões.

Conforme essa classificação, o direito da privacidade seria um direito de "ser deixado só", um direito negativo e, portanto um direito liberal de 1ª dimensão enquanto o direito à segurança pública seria uma obrigação Estatal fornecer essa segurança e ordem pública sendo, portanto um direito social da 2ª dimensão.

Essas dimensões dos Direitos Fundamentais são importantes para podermos compreender melhor a natureza dos conflitos entre esses Direitos. No caso aqui tratado temos um direito negativo, de 1ª dimensão em conflito com um Direito positivo, de 2ª dimensão, o conflito entre privacidade e segurança pública é o conflito entre a obrigação do Estado de deixar de fazer algo (no caso invadir a esfera privada do indivíduo) e a obrigação do Estado em fazer algo (zelar pela segurança pública do indivíduo). É também, portanto, um clássico conflito entre o liberal e o social.

Posto dessa forma, passemos a analisar formas de solucionar esse conflito de acordo com o melhor Direito, lembrando que nenhum Direito Fundamental é absoluto, havendo limitações impostas pela própria Constituição Federal ao pleno exercício desses Direitos, mormente quando em conflito com outros Direitos.

Uma maneira eficiente de se enfrentar esse problema é compreender o sentido de norma, dividindo-a entre regras e princípios e é nessa ideia que trabalha Robert Alexy, que se utiliza nesse trabalho dada a adequação de seu pensamento em solucionar o problema proposto. Robert Alexy considera regras como mandamentos de concretização, com baixo grau de generalização, ou seja, entende que as regras são espécies de normas mais rígidas, de caráter binário, "[...] são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve-se fazer exatamente aquilo que ela exige; nem mais, nem menos. Regras contêm, portanto, determinações [...]" (ALEXY, 2008, p. 91) enquanto os princípios são mandamentos de otimização (ALEXY, 2008, p. 90) que, diferente das regras, tem um alto grau de generalidade, se adequando e se amoldando melhor ao caso concreto.

Por conta do grande valor axiológico dos Direitos Fundamentais e da sua abstração pode-se dizer que esses Direitos têm forte natureza principiológica, muito embora tal assertiva também não possa ser absoluta.

> No que concerne as normas de direitos fundamentais, mister ressaltar que não há identidade perfeita entre direitos fundamentais e princípios. No entanto, é perceptível o caráter principiológico que as normas de direito fundamentais possuem por conta do forte conteúdo axiológico em face dos bens jurídicos que visam proteger. (BELCHIOR, 2009, p. 152)

Conforme já esposado na ideia de Alexy, trabalhar os nossos Direitos Fundamentais como normas-princípios garante o grau de abstração e generalidades necessários para que se possa lidar com os conflitos entre eles de maneira mais eficiente. e "nos casos concretos, os princípios têm pesos diferentes" (ALEXY, 2008, p. 94).

E tal são os princípios mandamentos de otimização que se imbricam perfeitamente na Sociedade da Informação, dinâmica por excelência, líquida que exige uma permuta axiológica no caso concreto, em perfeita comunhão entre as necessidades mutacionais da nossa sociedade e a elasticidade e abstração dos princípios, “o conteúdo dos direitos fundamentais, por conseguinte, é dinâmico, estando em constante transformação, haja vista que o conceito de dignidade humana não é engessado.” (BELCHIOR, 2006, p. 166)

A forma como Alexy resolve o conflito entre princípios é pela proporcionalidade e seus subprincípios: adequação, necessidade e proporcionalidade em sentido estrito.

> Afirmar que a natureza dos princípios implica a máxima da proporcionalidade significa que a proporcionalidade, com suas três máximas parciais da adequação, da necessidade (mandamento do meio menos gravoso) e da proporcionalidade em sentido estrito (mandamento do sopesamento propriamente dito), decorre logicamente da natureza dos princípios, ou seja, que a proporcionalidade é deduzível dessa natureza. (ALEXY, 2008, p. 116)

Esses subprincípios são utilizados para resolver conflitos entre princípios dentro da ideia de proporcionalidade, sendo que são divididos da seguinte forma:

1) Adequação: A aplicação do princípio no caso concreto é adequada ao fim desejado? No caso de conflito, se afastarmos certo princípio, o resultado desejado em virtude da prevalência de outro princípio será adequado? Caso seja adequado, ou seja, a aplicação desse princípio resultará no resultado prático pretendido, então devemos passar a análise de outro subprincípio.

2) Necessidade: Nesse ponto deve-se analisar em termos de comparação; Há outra maneira menos gravosa de se dar validade a determinado princípio em detrimento do outro? Há necessidade, de fato, do afastamento de um princípio para que o outro tenha validade? Examina-se aqui qual princípio está sendo restringido e determina se não há uma outra maneira de se chegar ao mesmo objetivo sem que se afaste o princípio em perigo.

3) Proporcionalidade em sentido estrito: Aqui trata-se do balanceamento ou ponderação entre o princípio que está sendo ferido e o princípio que está se sobressaindo, ou seja, qual o grau de intervenção de um princípio sobre o outro, levando-se em conta que "quanto maior o grau de não-satisfação ou de detrimento de um princípio, maior a importância de se satisfazer o outro" (ALEXY, 2003, p. 136), aqui se pondera se a satisfação do princípio, em termos de grau de intervenção, justifica ou não a restrição de determinado princípio.

Com a construção teórica adequada para resolver o problema proposto, algumas ponderações devem ser feitas antes de analisarmos mais profundamente a questão. Primeiro que o pensamento de Alexy para resolver conflitos referentes a normas-princípio é extremamente complexo e torna-se proporcionalmente mais complexo em virtude do caso concreto. Segundo que em nossa atual Sociedade da Informação que preza a liquidez e o dinamismo das relações e das coisas o uso da interpretação conforme a proporcionalidade é muito perene pois a mudança de situação da coisa objeto da proteção ou violação pelo Direito se modifica rapidamente e, terceiro, os princípios da privacidade e da segurança pública tem altíssimo grau de abstração, sobretudo o primeiro princípio que sofre influência imediata do meio em que se encontra, sendo que existem vários níveis de privacidade, sobretudo no mundo digital.

E, ainda, no caso da privacidade e da segurança no mundo digital não se tem certeza, como se verá nos capítulos seguintes, de certos fatores que podem influenciar a análise do caso concreto, como por exemplo o grau de confiabilidade da criptografia utilizada ou a real necessidade de se proceder a quebra do sigilo telemático para garantir a segurança pública. São dados que foram captados pela presente pesquisa, sobretudo na análise das audiências públicas, mas que ainda tem um alto grau de desconfiança, Portanto a aplicação aqui dessa forma de solucionar conflitos deve ser encarada de maneira mais ampla do que restrita, não como uma solução mas como uma ferramenta adequada a medida que os fatores que permeiam essa discussão (inclusive fatores técnicos) vão se elucidando.

Pois bem, tendo em vista que já se tem nessa altura uma ideia mais bem construída sobre os conceitos de privacidade e segurança pública podemos tentar aplicar a teoria da proporcionalidade nesse caso.

A privacidade se modificou, como foi demonstrado, com a evolução dos tempos e hoje, diferente de ontem, é um princípio, um escudo contra a gula da Sociedade da Informação que trata as informações e, principalmente, os dados como mercadoria. Ao mesmo tempo, a segurança pública é uma preocupação constante da vida moderna e uma dependência que temos da estrutura sólida do Estado.

Se olharmos a história do conflito entre a privacidade e a segurança pública veremos que o segundo sempre teve certa preponderância sobre o primeiro. Por exemplo é possível a interceptação telefônica por meio de ordem judicial e, nesse caso se aplicássemos a Teoria da Proporcionalidade de Alexy veríamos que poderíamos passar pela fase da adequação, da necessidade e chegaríamos a fase da proporcionalidade propriamente dita perguntando se a satisfação do princípio da segurança pública é suficientemente proporcional em relação a insatisfação com o direito ‘a privacidade. A questão, como se pode ver, é complexa pois necessita-se de mais dados para elaborar o raciocínio como, por exemplo, qual crime está sendo investigado e o que foi interceptado nas conversas telefônicas. Como se vê, esse conflito só pode ser resolvido pela proporcionalidade de Alexy quando se tiver acesso a todos os dados e danos possíveis, e aí resvalamos em questões técnicas que serão melhor tratadas em capítulos posteriores. Por enquanto basta que se entenda que há possibilidade de aplicação da presente teoria para tentar resolver o conflito.

CAPÍTULO 2 – A COMUNICAÇÃO ELETRÔNICA POR TROCA DE MENSAGENS INSTANTÂNEAS PELA INTERNET.

2.1- A CRIAÇÃO DA INTERNET E A MUDANÇA DO PARADIGMA DE COMUNICAÇÃO INSTANTÂNEA.

O homem é um animal social, nas palavras de Aristóteles, um animal que utiliza a fala como meio de construir uma vida social (*politika*) e essa propensão para viver em sociedade impulsionou as formas de comunicação, fazendo com que o homem, a medida que se desenvolve em sociedade também desenvolve novas formas de comunicação.

Dentre as diversas formas de comunicação utilizada pelo homem, podemos destacar a comunicação epistolar por conta da sua carga emotiva e sensível, bem como por ser uma das formas de comunicação interpessoal das mais antigas, salvo, por óbvio a própria fala.

As cartas (do grego *khártés*) constituem objeto de estudo especial pois contém também caracteres próprios que a valorizam, como por exemplo a carga emotiva, sua longevidade (*Verba volant, scripta manent,* antigo adágio em latim) mas também era uma ferramenta para poucos, os letrados e cultos.

> Escrever cartas era prerrogativa das pessoas de classes sociais mais altas e dos comerciantes; muitas vezes elas eram ditadas aos “escravos secretários” e aquele que a ditava colocava uma inscrição final de próprio punho. Gregos e romanos escreviam em lâminas ou tabletes de cera e entregavam a um escravo para levá-las ao destinatário. A escrita, feita por meio de um estilete, era gravada em um só lado da lâmina, que era envolvida por uma fita, contendo, no extremo, o carimbo; na parte externa, gravava-se o endereço. Posteriormente foi adotado o papiro ou charta, conhecida desde Alexandre Magno, a qual se compunha de duas folhas atravessadas por um cordão, que terminava em nó, com um carimbo. (VASCONCELLOS, 2008, p. 372-373)

Ainda assim, podemos afirmar que com a troca de cartas se iniciou o paradigma de comunicação com certas características como a pessoalidade, a

privacidade e a perenidade. Podemos adicionar também o fato de, diferente da fala, a carta não proporcionar uma comunicação instantânea.

A questão da privacidade na comunicação por cartas, há que se notar, evoluiu ao mesmo tempo que o próprio conceito de privacidade, a ponto de se anotar como um dos marcos iniciais da proteção legal à privacidade na comunicação a data de 10 de agosto de 1790, quando a Assembleia Nacional em Paris declarou inviolável o sigilo postal que, posteriormente, foi encampado pelo código penal (GAY, 2002, p. 273 – 274).

A primeira grande mudança no paradigma da comunicação interpessoal se deu com o telefone (deixemos um instante de lado o telégrafo pois seu propósito e constituição não nos parece constituir uma comunicação interpessoal que tenha características de massificação) que adicionou como característica a velocidade da comunicação, porém manteve a imobilidade. Apenas com os telefones celulares é que a questão da mobilidade foi adicionada, modificando mais uma vez o paradigma das comunicações interpessoais.

Porém, antes desse ponto cumpre salientar aquela que foi a grande mudança causada pela tecnologia e que revolucionou de maneira inconteste todos os aspectos da vida humana e social, a criação da Internet.

A internet surge no contexto da Guerra Fria, na busca frenética da superioridade tecnológica e bélico-militar entre os Estados Unidos e a União Soviética e, dessa disputa surge em 1958 a agência de projetos ARPA (Advanced Research Projects Agency), uma agência norte-americana cujo objetivo era avançar a tecnologia norte-americana e superar a União Soviética. Logo em 1969, Paul Baran e Donald Davies inventaram a Arpanet, um sistema que visava proteger as comunicações norte-americano em caso de ataque nuclear soviético. A ideia era criar um sistema de comunicação militar descentralizado em que os computadores se conectariam de maneira independente com mensagens trocadas em bloco, entre dois terminais, independentes do centro de controle e comando.

A evolução natural da Arpanet é, agora a comunicação com redes externas, mas para que essa comunicação ocorra seria preciso uma “linguagem comum” e, para tal, em 1973 surge o TCP, um protocolo comum de comunicação, dividido em 1978 em dois protocolos, os chamados TCP/IP (Transmission Control/Internet Protocol – padrão até hoje utilizado).

A Arpanet foi, portanto a gênese da Internet que somente começou a tomar forma, porém apenas na década de 1990 é que temos a Internet no formato que a conhecemos, com o surgimento de navegadores da www e com uma Internet privatizada:

> Em meados da década de 1990, a internet estava privatizada e dotada de uma arquitetura técnica aberta, que permitia a interconexão de todas as redes de computadores em qualquer lugar do mundo; a www podia então funcionar com software adequado, e vários navegadores de uso fácil estavam à disposição do público. Embora a internet tivesse começado na mente dos cientistas da computação no início da década de 1960, uma rede de comunicações por computador tivesse sido formada em 1969, e comunidades dispersas de computação reunindo cientistas e hackers tivessem brotado desde o final da década de 1970, para a maioria das pessoas, para os empresários e para a sociedade em geral foi em 1995 que ela nasceu. (CASTELLS, 2003, p. 19)

Manuel Castells (2005, passim) afirma que estamos, agora, diante de uma revolução da tecnologia, uma onda que modifica a própria sociedade em que vivemos e pontua as diferenças inerentes a essa nova sociedade em rede da seguinte forma:

> Internet é sociedade, expressa os processos sociais (...) ela constitui a base material e tecnológica da sociedade em rede. (...) Esta sociedade em rede é a sociedade (...) cuja estrutura social foi construída em torno de redes de informação a partir de tecnologia de informação microeletrônica estruturada na Internet. Nesse sentido, a Internet não é simplesmente uma tecnologia; é o meio de comunicação que constitui a forma organizativa de nossas sociedades; é o equivalente ao que foi a fábrica ou a grande corporação na era industrial. A Internet é o coração de um novo paradigma sociotécnico, que constitui na realidade a base material das nossas vidas e de nossas formas de relação, de trabalho e de comunicação. O que a Internet faz é processar a virtualidade e transformá-la em nossa realidade, constituindo a sociedade em rede, que é a sociedade em que vivemos (CASTELLS, 2003, p.286-287).

Como colocado por Castells, a Internet cria novos paradigmas, mormente no campo da comunicação. Não estamos mais presos, limitados, estamos interconectados numa sociedade cuja velocidade de dispersão de dados e conhecimento é enorme. Há acesso móvel a Internet pelo uso de telefones celulares, a velocidade toma-se o primado da comunicação interpessoal e mistura a comunicação de massa com a comunicação pessoal.

Os conceitos de privacidades expostos no capítulo anterior sofrem profunda mudança com a internet, esse novo paradigma de comunicação que prioriza a velocidade que é também uma das características dessa modernidade líquida. Os antigos pensamentos sobre privacidade e comunicação sofrem profundo abalo com o surgimento da Internet.

Conforme evolui a ideia de internet e de seu uso na Sociedade da Informação, podemos citar como um dos efeitos a questão de intercomunicação que se expande por conta da mobilidade trazida pelo uso de *smartphones* e *tablets* principalmente que se interligam a rede mundial de computadores de maneira *wireless*[9]. A possibilidade de se conectar à internet em qualquer lugar que tenha cobertura *wireless* permitiu a consagração da interação em tempo real via celulares, *smartphones, tablets* e até mesmo relógios com o mundo exterior, modificando drasticamente o paradigma de comunicação existente, conforme explica Ferreira (2005, apud SILVEIRA, 2012, p.35):

> A “Internet Móvel”, a exemplo do “Telégrafo Falante” ou do “Telégrafo sem fio”, ainda está baseada no seu antecessor que quebrou antigos paradigmas e inaugurou novos tais como interatividade, tempo real, comércio eletrônico, entre outros, que fazem parte do vocabulário da web.

Essa mudança de costumes trazidas pela mobilidade comunicacional via internet, mais um impacto da Sociedade da Informação em nosso meio, trouxe profundas mudanças sociais. Ainda de acordo com Silveira

[9] Também chamada de internet sem fios, internet móvel e M-Internet é a convergência da tecnologia web com o acesso *wireless* (sem fio) propriamente dito que possibilita o acesso remoto a uma gama de serviços tais quais *e-comunication* (comunicação eletrônica), *e-service* (serviço eletrônico) e *e-commerce* (comércio eletrônico). (SILVEIRA, 2012, p. 35).

(2012, p. 36) a internet fixa é mais utilizada para negócios, socialização com amigos e familiares distantes e pesquisas pessoais relacionada a temas sobre a formação educacional e profissional e a internet móvel é utilizada para entretenimento, consumo de conteúdo de relevância com o meio (jogos, música, vídeo e foto), socialização com amigos ou pessoas mais íntimas através de mensagens eletrônicas. No interior dessa revolução comunicacional surge, como sói acontecer com a dinâmica da Sociedade da Informação, pequenas revoluções internas que alteram substancialmente nosso modo de agir e atuar no meio-ambiente social. Da comunicação eletrônica fixa, evolui-se para o universo wireless, dinâmico, para uma comunicação eletrônica móvel, que expande a possibilidade comunicacional via internet para qualquer tempo, desde que com acesso a internet wireless. Ficamos conectados o dia inteiro com nossos celulares, smartphones e tablets, não mais dependentes de pontos fixos de computadores de mesa (desktops). A partir daí o passo seguinte dessa pequena revolução é a massificação do uso de mensagens eletrônicas em tempo real, com o uso de aplicativos de mensagens específicos para isso instalados em equipamentos menores e de fácil mobilidade.

2.2 A COMUNICAÇÃO ELETRÔNICA INSTANTÂNEA E A MOBILIDADE COMUNICACIONAL.

Para que se possa melhor definir a questão da comunicação eletrônica instantânea com a mobilidade comunicacional deve-se se ater a algumas características básicas que expliquem o que é essa internet móvel e onde ela difere da internet em geral. De imediato é inegável que a possibilidade de poder ter acesso a comunicações instantâneas longe de um ponto fixo já altera a maneira como se utiliza socialmente a internet. Essa mudança da estrutura de uso da internet (da fixa para móvel), em especial no que tange a comunicação instantânea, traz características básicas importantes para que se possa compreender a penetração social do uso dessa ferramenta eletrônica no mundo moderno. A esse respeito traçam-se algumas características, tais quais:

> Imediaticidade: Os celulares têm capacidade de escrita e mensagens para respostas imediatas, sendo um grande facilitador de comunicação para os usuários de telefonia móvel;
>
> Privacidade: Mesmo quando recebidos em lugar público, os dados e imagens enviados através da tecnologia móvel se mantêm privados aos seus usuários e ou consumidores;
>
> Ubiquidade: O consumidor pode ser alcançado em qualquer lugar e a qualquer hora. Este pode conseguir a informação que deseja, não importa onde esteja, por aparelhos celulares que acessem a Internet;
>
> Personalização: A internet possui uma enorme quantidade de informações e serviços. A relevância da informação que o usuário recebe é muito importante. Ele quer receber e acessar somente o que lhe interessa no momento de seu interesse;
>
> Flexibilidade: Pela própria característica móvel e portátil dos aparelhos celulares, o usuário poderá conduzir transações enquanto viaja ou se locomove a pontos diferentes de um local;
>
> Disseminação: Algumas infra-estruturas sem fio suportam a entrega simultânea de dados a todos os usuários numa área geográfica específica. Este é um excelente meio de disseminar informação em larga escala. (TEZZA;BORNIA;ALBUQUERQUE, 2008, p. 02 apud SILVEIRA, 2012, p. 38).

Deve-se ponderar sobre algumas dessas características para compreender o impacto das comunicações eletrônicas instantâneas nas relações sociais e, com isso, no Direito atual.

Primeiro pode-se observar que a imediaticidade das comunicações na internet móvel alimenta o usuário para uma “vida precária, vivida em condições de incerteza constante” (BAUMAN, 2005, p. 08), ou seja, a liquidez da vida exige uma imediaticidade que a Sociedade da Informação supre muito bem com a possibilidade de acesso à internet móvel. O poder de acessar a internet imediatamente, de qualquer lugar (ubiquidade) e com flexibilidade de uso (pode-se acessar e contatar outros usuários remotamente tanto de um celular como de um tablet ou mesmo por um relógio, por exemplo) transformou as comunicações. Uma característica essencial que alimenta essa mudança do paradigma de comunicação trazida pela mobilidade comunicacional é a privacidade. A impressão de privacidade é uma característica essencial dessa forma de comunicação pois se o usuário não tiver uma relativa impressão de privacidade ele não se comunicará da mesma maneira como se comunica normalmente

quando entende ser essa conversa pública. Como se vê, a internet fixa difere em muitos pontos da internet móvel no que tange a comunicação instantânea. Algumas características são similares, porém a mobilidade não apenas da comunicação em si (já existente com o uso de celulares, ainda que sem acesso a internet), mas do acesso à internet móvel trouxe uma nova flexibilidade na comunicação. Com a internet móvel não se tem apenas uma comunicação de ponto a ponto, tal qual um celular ou um rádio tem, mas permite a troca de conteúdo instantaneamente acessado na rede mundial, ampliando as comunicações instantâneas a não apenas uma transmissão de voz ou textos à distância, mas também com uma troca efetiva de informações como fotos, sons, *hyperlinks*, dados em geral, de maneira imediata, transformando a comunicação pela internet em verdadeira troca de dados de toda sorte.

Ainda a respeito das mensagens instantâneas, é interessante notar que essa massificação da mobilidade comunicacional é explicada também na ideia de Bauman (2000, p. 70) sobre o confronto entre “o discurso de Joshua” e “o discurso da Genêsis” perante a sociedade capitalista em que o primeiro representa a ordem como regra perante a desordem indesejada, o segundo representa a desordem como regra e a ordem como exceção. Nesse ponto de vista, “o discurso de Joshua” seria o “pesado”, representando, por exemplo a estrutura do pensamento fordista em que as coisas ficam em seu lugar, usando como alegoria o livro “1984” de George Orwell no espírito de que a estrutura capitalista (antiga) exigia a imobilidade ordenada, tal qual uma linha de montagem sendo a desordem algo incompatível com a felicidade. Nesse discurso sabe-se muito bem o que se quer e para onde se vai, a ordenação, a imobilidade traria a única resposta aceitável para a sociedade. Ainda segundo Bauman (2000, p. 70), o livro “Admirável Mundo Novo” de Aldous Huxley traria a manifestação do “discurso da Genêsis” e representaria melhor o “capitalismo leve”, “líquido” dos tempos atuais, em que seríamos passageiros de uma nau que não sabemos quem pilota ou para onde vamos. A modernidade líquida se contrapõe, dessa forma, à sociedade estratificada, “pesada” de antes. A mobilidade é a chave

dessa nova sociedade e o uso de celulares uma de suas mais importantes ferramentas. O capital é leve.

> Hoje o capital viaja leve – apenas com bagagem de mão, que inclui nada mais que pasta, telefone celular e computador pessoal. Pode saltar em quase qualquer ponto do caminho, e não precisa demorar-se em nenhum lugar além do tempo que durar sua satisfação. (BAUMAN, 2000, p. 80)

Assim, a mobilidade comucacional é parte integrante hoje da nossa forma de viver e agir. Além de também fazer parte da forma como empreendemos economicamente, nos comunicamos com os outros em assuntos íntimos ou não, é também preponderante na nossa relação com a política e na forma como se formam movimentos sociais que atuam em relação ao Poder Estatal, como nos exemplos trazidos da primavera árabe, da revolução egípcia, do movimento dos indignados da Espanha e dos movimentos de julho de 2013 no Brasil entre outros pois, de acordo com Castells (2017, p. 192), “o uso das redes de comunicação da internet e dos telefones celulares é essencial, mas a forma de se conectar a rede é multimodal”, ou seja, ainda que nesses movimentos houvesse a necessidade de se ocupar espaços públicos, toda organização se deu pela Internet, em especial no uso de celulares que eram utilizados para organização dos eventos. Por força da horizontalidade desses movimentos, a conexão sem fio foi (e é) fundamental (CASTELLS, 2017, p. 198) e comprova a penetração da mobilidade comunicacional no estilo de vida da sociedade atual, impregnando todo os setores da sociedade moderna, não por acaso chamada de Sociedade da Informação. A informação hoje deve ser móvel para ser mais eficientemente utilizada. E tal mobilidade se dá, majoritariamente hoje em virtude do uso de aplicativos de mensagens instantâneas instalados em telefones celulares.

2.3 CONCEITUAÇÃO DE APLICATIVOS DE MENSAGENS INSTANTÂNEAS PARA FINS DE PESQUISA E O SEU USO ATUAL.

O sistema de mensagens instantâneas (*instant messaging* ou simplesmente IM), de acordo com Vleck (2001), teve início em 1965, ano em que

Noel Morris e Tom Van Vleck criaram uma ferramenta para o CTSS[10] chamada *.saved* que permitia ao usuário logado ao CTSS trocar linhas de textos que eram imediatamente recebidas e percebidas por outro usuário que também estivesse logado ao mesmo tempo. Ainda de acordo com o autor essa teria sido a primeira vez que se utilizou mensagem instantânea entre dois usuários logados. Posteriormente, o *.saved* foi ainda adaptado para informar imediatamente o usuário da chegada de mail em sua caixa postal. Por óbvio o sistema não era chamado ainda de instant messaging, nome que só foi amplamente utilizado a partir dos anos 90. Porém, antes mesmo desse termo ser utilizado a troca de mensagens em tempo real já começava a ficar popular com o advento das BBS (Bulletin Board Systems) que eram serviços que conectavam o computador de um ou vários usuários, via uso de modem conectado à linha telefônica, com um computador central, também conectado à linha telefônica por modem, ainda fora da Internet (conexão peer to peer). Esse computador central, que passivamente recebia as ligações dos usuários externos, utilizava um dos vários sistemas de administração de BBS, em geral com gráficos gerados por textos, chamados códigos ASCII, fornecendo uma gama de serviços aos usuários que se conectavam ao sistema. Entre os serviços podemos citar o acesso a arquivos previamente colocados à disposição da BBS, jogos e comunicação eletrônica. Na ponta do computador central que utilizava o software da BBS ficava o administrador, chamado de Sysop (System Operator) que podia manter um controle posterior daquilo que o usuário lançava na BBS ou mesmo um controle instantâneo do acesso do usuário acessante. Nesse ponto era possível uma troca instantânea de mensagens entre o usuário e o Sysop, onde se podia antever a necessidade de troca imediata de mensagens.

[10] “CTSS is basically a system which will allow an evolutionary development of time-sharing while continuing to allow more conventional background systems to operate.” (CORBATÓ et al, 1963, p. 05). É, portanto um sistema operacional criado na década de 60 que, de maneira inovadora, permitiu o uso de mais de um software ao mesmo tempo em uma mesma máquina, poupando tempo pois permitia que o sistema operacional funcionasse ao mesmo tempo em que a máquina utilizava parte de seu processamento para outra função. Hoje esse processamento múltiplo em uma única máquina é padrão, porém no final da década de 50 e início da década de 60 os computadores só processavam uma função por vez.

Posteriormente, nos anos 90, com a popularização da Internet e dos computadores pessoais, surgiram os serviços provedores de mensagens instantâneas como o AOL (America Online), que provia o AIM (America Online Instant Messenger) e o ICQ (acrônimo de “I seek you”), da empresa israelense Mirabilis, que adicionou várias funcionalidades como a busca de usuários usando um diretório próprio, troca de arquivos e conversa entre vários usuários ao mesmo tempo (BRUIN, 2018, p. 08).

A partir do último biênio do século XX empresas como Microsoft e Yahoo passaram a operar no âmbito das mensagens instantâneas com seus serviços respectivos, os MSN Messenger e Yahoo Messenger (originariamente Yahoo Pager) concluindo que o caminho para a comunicação na Internet obrigava o uso de aplicativos de mensagens instantâneas. Mais tarde aplicativos como Skype criaram um espaço específico para esse tipo de serviço.

É importante ressaltar que, embora se reconheça a importância dos aplicativos de mensagens instantâneas em computadores fixos, a grande mudança no paradigma das comunicações surge com a inclusão desses aplicativos em *smartphones*, levando as pessoas a aumentarem enormemente o uso desses aplicativos a ponto de se tornarem uma forma de comunicação tão natural quanto a própria comunicação interpessoal, com grande influência e pressão na sociedade (BRUIN, 2018, p. 06).

Portanto, uma definição lógica sobre aplicativos de mensagens instantâneas é que são softwares de aplicação que processam a troca de mensagens de texto instantaneamente, ou seja, em tempo real (BRUIN, 2018, p. 03), que servem como intermediários entre dois ou mais usuários na troca de dados via rede mundial. Esse software, chamado aqui de aplicativo de mensagem instantânea tem como função precípua a administração de dados entre os usuários de maneira imediata, providenciando assim a privacidade, a ubiquidade e a flexibilidade exigidas pela sociedade moderna. São empresas, corporações privadas que administram e fornecem esses serviços, por meio de software, muitas vezes sem que haja pagamento em pecúnia por esse serviço. A maioria

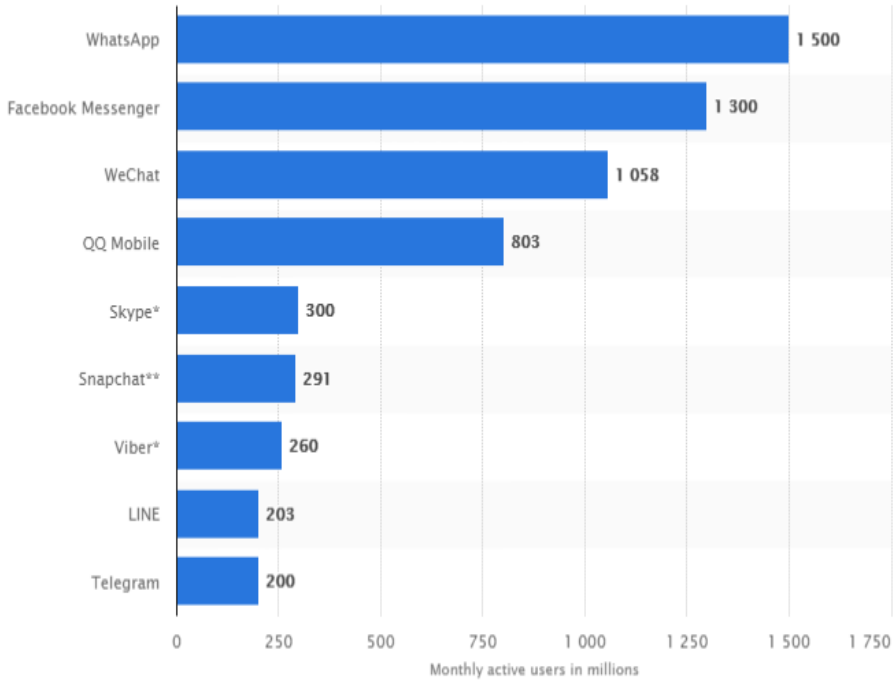
deles, como veremos, tem a funcionalidade tanto em computadores fixos, que operam sistemas operacionais como Windows e Linux, como em smartphones que operam com diversos sistemas operacionais como Android e iOS (sistema operacional dos smartphones da Apple).

Dessa forma, os aplicativos de mensagens instantâneas não estão limitados a um meio apenas, podem também estar dispersos em diversos tipos de equipamentos, sejam fixos, como computadores de mesa, ou móveis como celulares, tablets e relógios. A característica de mobilidade, dessa forma, não define um aplicativo de mensagens instantâneas, porém essa característica é que torna o uso de mensagens instantâneas muito mais popular. Outra característica importante é o acesso que esses aplicativos têm aos seus dados, em especial dados referentes a contatos que permitem a ligação, via software, entre usuários desse serviço. A depender do serviço que se utiliza esses dados podem ser apenas uma conta cadastrada no próprio aplicativo ou o número de telefone.

A possibilidade da mobilidade no uso de mensagens instantâneas via aplicativos tem modificado o cenário de mídia a ponto de alguns autores entenderem que a própria mídia social está se fundindo com *instant messaging* (SHEN et al, 2011; HOGAN, QUAN-HAASE, 2010 apud BRUIN, 2018, p. 05) e, mais, a possibilidade de utilização de aplicativos de mensagens instantâneas ao mesmo tempo que se acessa a rede mundial e todos os dados de computadores modifica a forma como se lida com essa tecnologia a ponto de imaginar que, no futuro, os aplicativos de mensagens instantâneas substituirão os e-mails (BRUIN, 2018, p. 06). De fato, uma das principais funcionalidades dos aplicativos de mensagens instantâneas mais populares é poder não apenas trocar mensagens de texto, mas imagens, grandes arquivos de textos, planilhas, sons e *hyperlinks*, que são capturados instantaneamente da própria internet e repassados ao outro usuário com quem se está comunicando, de maneira rápida, fácil e eficiente. Por conta dessa agilidade, os aplicativos de mensagem instantânea são muito utilizados como ferramentas comerciais também, servindo como meio se concluir empreendimentos comerciais, oferecimento e até efetivação de serviços em especial por conta da agilidade e privacidade que esses aplicativos oferecem.

Definido o aplicativo de mensagem instantânea para o propósito do presente trabalho, faz-se necessário que entendamos quais são os principais aplicativos dessa espécie em uso no mundo.

Figura 1 – Uso mensal de aplicativos de mensagens instantâneas.



Fonte: STATISTA – THE STATISTICS PORTAL, 2018

De acordo com o sítio especializado em estatística, o STATISTA – THE STATISTICS PORTAL[11] uma pesquisa realizada em outubro de 2018 demonstrou que o aplicativo de mensagem instantânea com maior número de usuários ativos, por mês, no mundo é o WhatsApp (com um bilhão e quinhentos milhões de usuários/mês), seguido pelo Facebook Messenger (um bilhão e trezentos milhões de usuários/mês), WeChat (um bilhão e cinquenta e oito milhões de usuários/mês), QQ Mobile (oitocentos e três milhões de usuários/mês), Skype (trezentos milhões de usuários/mês), Snapchat (duzentos e noventa e um milhões

[11] "Within just a few years, Statista managed to establish itself as a leading provider of market and consumer data. Over 500 visionaries, experts and doers continuously reinvent Statista, thereby constantly developing successful new products and business models." (STATISTA, 2018). STATISTA é um sítio com sede em Hamburgo, Alemanha que provê estatísticas para fins comerciais e de pesquisa desde 2011.

de usuários/mês), Viber (duzentos e sessenta milhões de usuários/mês), LINE (duzentos e três milhões de usuários/mês) e, por fim, Telegram (duzentos milhões de usuários/mês). A pesquisa, por tratar de usuários ativos por mês, indica o uso real de cada aplicativo e não apenas os potenciais usuários. Com isso podemos ter uma ideia melhor da penetração de cada aplicativo de mensagem instantânea na sociedade. Cada um desses aplicativos atua de maneira diferente, por exemplo o Skype e o Viber são originariamente um meio de comunicação do tipo VoIP[12], que dão ênfase à comunicação por voz enquanto o Snapchat é um aplicativo de mensagens instantâneas que serve primariamente para o envio de imagens por tempo determinado, que desaparecem após vinte e quatro horas.

Dentro desse universo de característica distintas, o certo é que o WhatsApp e o Facebook Messenger aparecem com destaque. O Facebook Messenger tem mais usuários nos Estados Unidos da América, enquanto o WhatsApp é mais utilizado no resto do mundo (STATISTA – THE STATISTICS PORTAL, 2018).

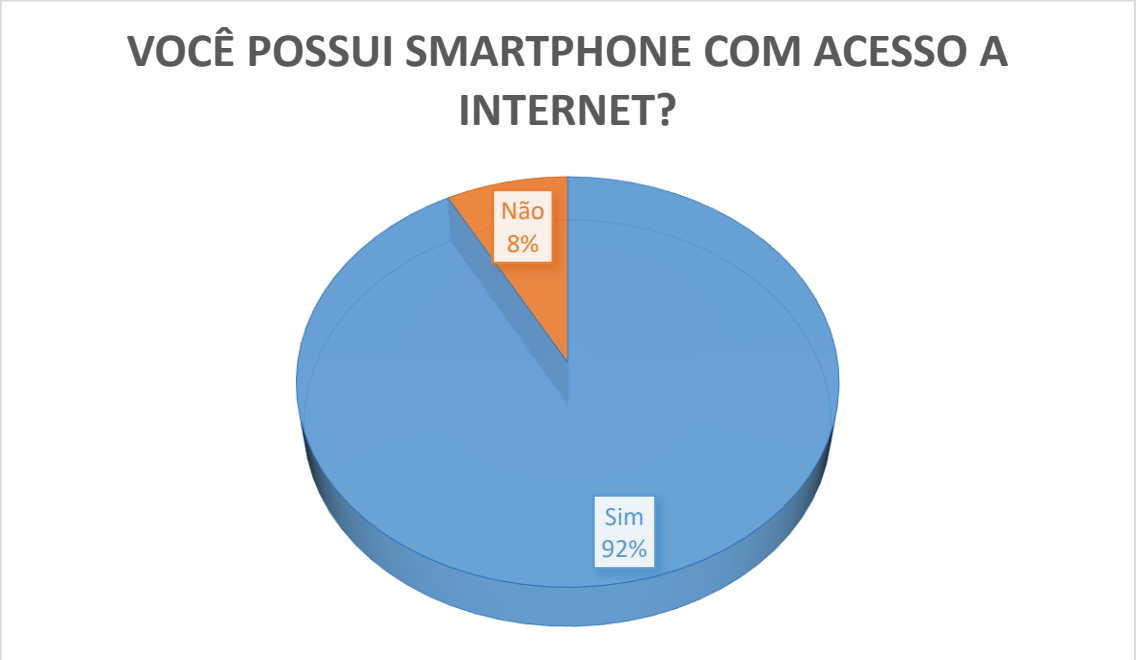
No Brasil o quadro não é muito diferente. O aplicativo de mensagens instantâneas mais utilizado é o WhatsApp, seguido pelo Facebook Messenger e Telegram (PANORAMA MOBILE TIME, 2018).

A base de dados aqui apresentada para embasar essa parte do presente trabalho é a pesquisa independente Panorama Mobile Time/Opinion Box - Mensageria no Brasil e “é uma pesquisa independente produzida por uma parceria entre o site de notícias Mobile Time e a empresa de soluções de pesquisas Opinion Box.”(PANORAMA MOBILE TIME, 2018). A edição da pesquisa aqui utilizada, segundo informado pelo próprio site de notícias, entrevistou 2007 brasileiros que acessam a internet e possuem celular no mês de janeiro de 2018, respeitando-se as proporções de gênero, idade, renda mensal e distribuição geográfica dos entrevistados e, tal pesquisa, tem margem de erro de 2,2 pontos percentuais e grau de confiança de 95% (PANORAMA MOBILE TIME, 2018).

[12] VoIP (Voice over Internet Protocol) é um meio de comunicação por voz que não utiliza telefonia convencional e sim a própria Internet para entabular conversações entre usuários.

A pesquisa inicia considerando a definição de smartphone como um celular que possui tela sensível ao toque e que permite ao usuário instalar e desinstalar aplicativos livremente e pergunta : “você possui smartphone com acesso a Internet?”, conforme figura 2 abaixo demonstra.

Gráfico 2 – Você Possui Smartphone com Acesso a Internet?

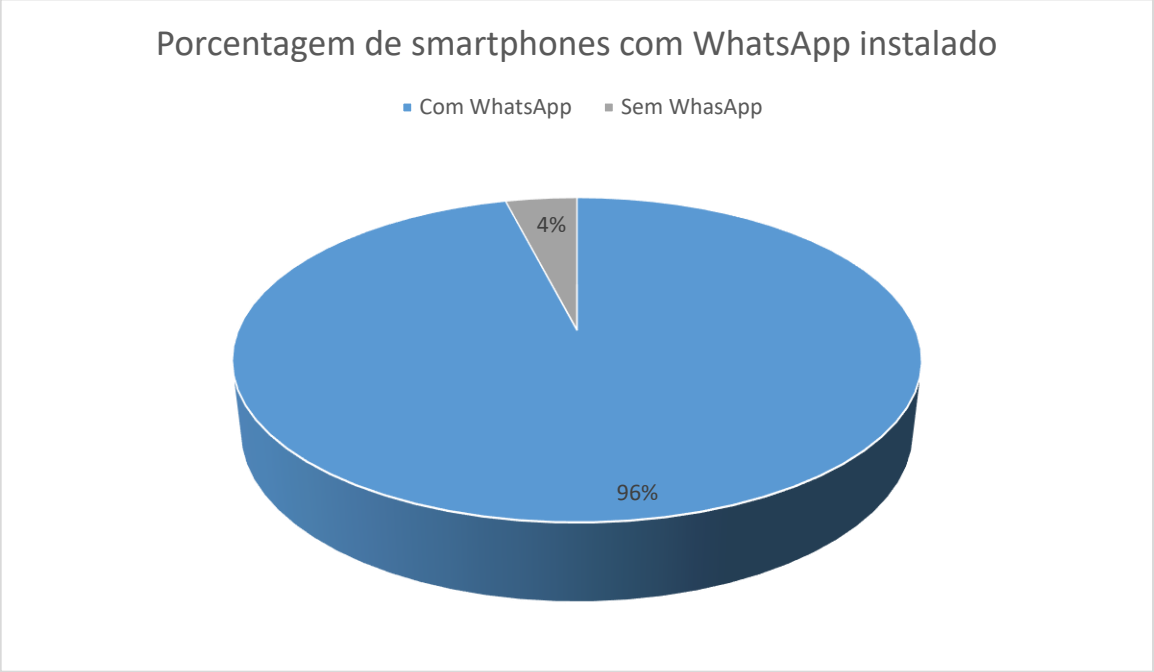


Fonte: PANORAMA MOBILE TIME, 2018

Dessa feita, uma grande parcela dos usuários pesquisados utiliza smartphones como forma de acesso a internet. Tal pesquisa é congruente com a última análise apurada na pesquisa PNAD Contínua do IBGE feita em 2016 demonstrando que 64,7% dos brasileiros acima de 10 anos utilizam a internet (considerando-se para pesquisa o uso nos últimos 3 meses) e, ainda, que desse universo de usuários que utilizam internet, 94,6% utilizaram a internet via celulares (IBGE, 2016).

Dos smartphones de usuários brasileiros que contém acesso a Internet, os aplicativos de mensagens instantâneas mais instalados são, respectivamente, WhatsApp, Facebook Messenger e Telegram, conforme gráfico abaixo.

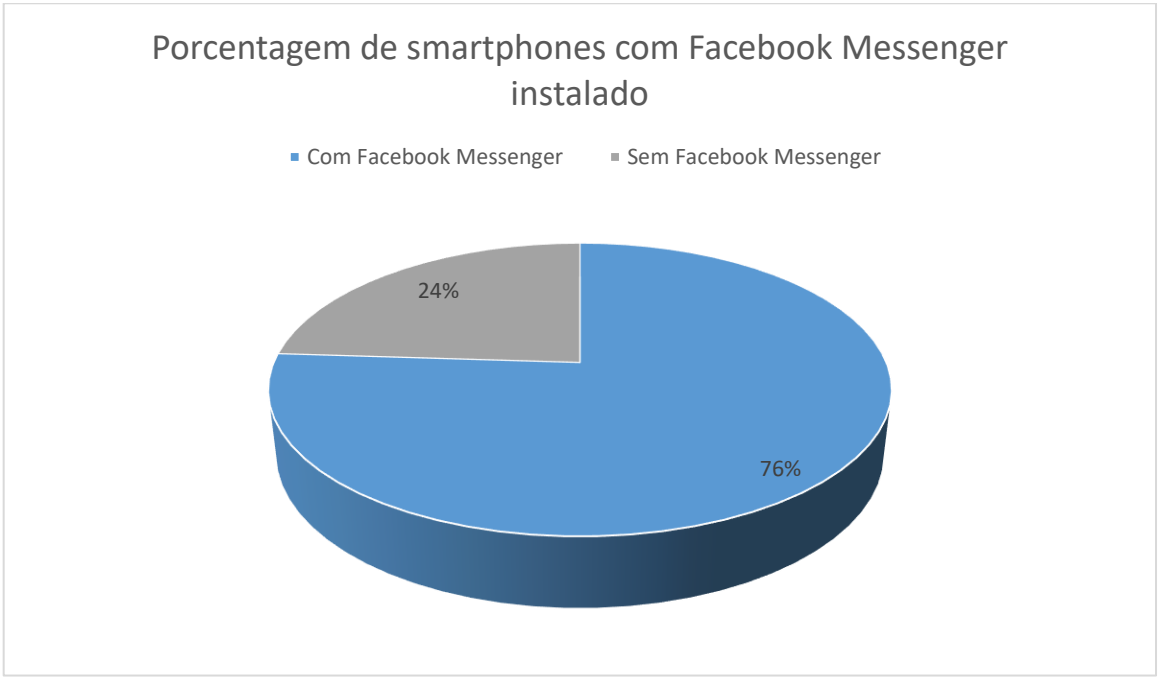
Gráfico 3 – Porcentagem de smartphones com WhatsApp instalado



Fonte: PANORAMA MOBILE TIME, 2018

De acordo com a pesquisa mais de 96% dos smartphone de brasileiros tem instalado o WhatsApp, isso significa que quase tão popular quanto o próprio smartphone é o WhatsApp que pode ser considerado quase que parte integrante do telefone.

Gráfico 4 – Porcentagem de Smartphone com Facebook Messenger instalado

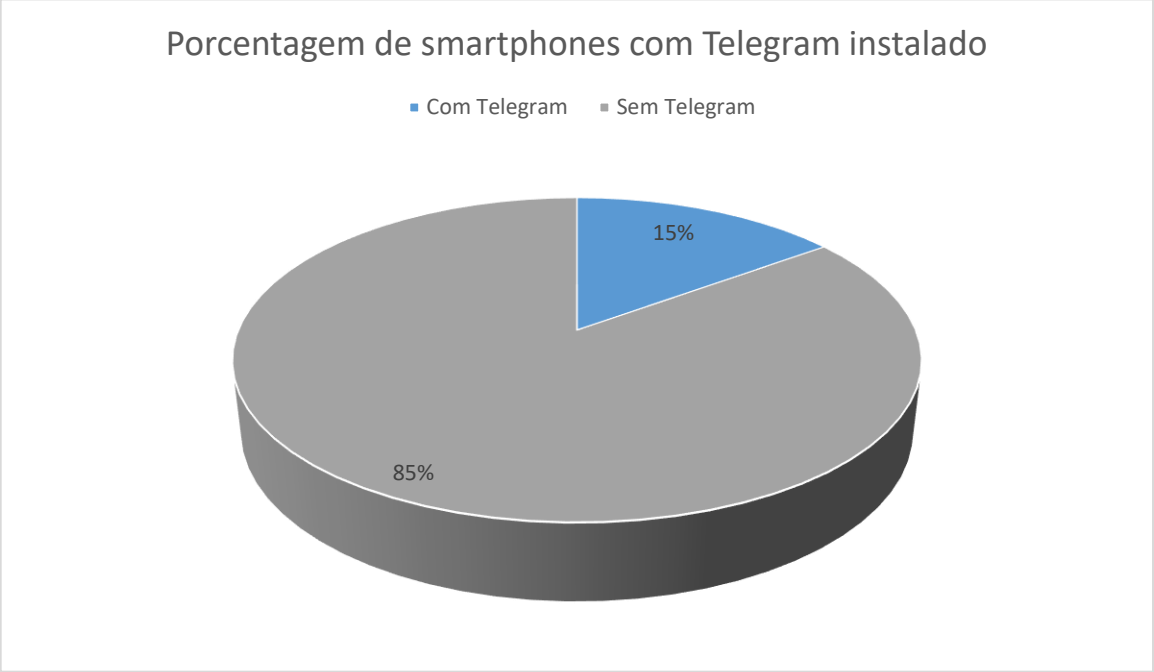


Fonte: PANORAMA MOBILE TIME, 2018

Comparando-se o Facebook Messenger com o WhatsApp temos uma dramática queda do número de aplicativos instalados, porém ainda assim há uma maioria ampla do número de smartphone com esse aplicativo instalado. Não podemos olvidar que o próprio WhatsApp é de propriedade do Facebook e que certamente a instalação do aplicativo de redes sociais, Facebook, influencia de maneira significativa o número de aparelhos que tem o Facebook Messenger instalado.

Por conta disso é espantoso os números do aplicativo WhatsApp instalados se compararmos com o do Facebook Messenger.

Gráfico 5 – Porcentagem de smartphones com Telegram instalado



Fonte: PANORAMA MOBILE TIME, 2018

No Brasil, portanto, o WhatsApp é sem dúvida o aplicativo mais popular, seguido pelo Facebook Messenger presente em 76% dos aparelhos e, por último o Telegram em apenas 15%.

Quando se observa o uso efetivo desses aplicativos, a disparidade em favor do WhatsApp é ainda maior. Em resposta a questão “Pensando nos últimos meses, com que frequência você abre o WhatsApp/Facebook Messenger/Telegram para ler ou enviar mensagens?” temos a Tabela 1 que demonstra a frequência de uso dos aplicativos de IM mais populares instalados, confirmando uma ampla aceitação e uso do WhatsApp (com 93% de uso diário), muito distante do Facebook Messenger (que consta 36% de uso diário entre aqueles que tem esse aplicativo instalado.

Essa parte da pesquisa demonstra claramente que o uso de aplicativos de Mensagem Instantânea tornou-se natural, diário para uma grande parte da população brasileira, sobretudo quando se trata do WhatsApp. Não é difícil concluir que a popularidade e aceitação do uso desses aplicativos modificou muito a forma como se lida com a comunicação em nosso país. Hoje, o uso desses aplicativos de tão natural e acessível, é parte integrante da forma comunicacional dos brasileiros. E o uso desses aplicativos de mensagens não mostra sinais de diminuir, conforme demonstra o gráfico 6.

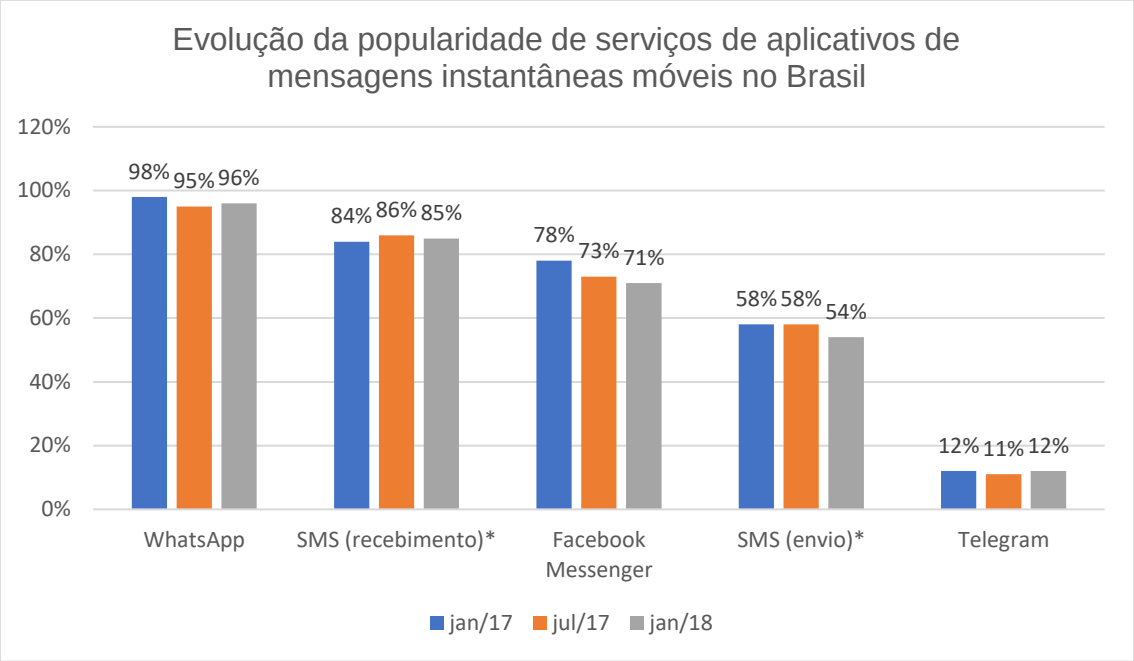
Tabela 1 – Frequência de uso dos aplicativos de IM mais populares

	Todo dia	Quase todo dia	Algumas vezes por semana	Algumas vezes por mês	Quase nunca	Nunca
WhatsApp	93%	5%	1%	1%	0%	0%
Facebook Messenger	39%	24%	21%	9%	7%	0%
Telegram	32%	18%	17%	13%	16%	4%

Fonte: PANORAMA MOBILE TIME, 2018

Note-se que mesmo o uso de SMS é inferior ao uso do WhatsApp, mesmo quando dividimos o uso dos SMS em passivo (recebimento apenas) e ativo (envio de SMS, que pode acarretar algum custo), ainda assim o WhatsApp é mais utilizado, conforme o gráfico a seguir demonstra.

Gráfico 6 – Evolução do uso dos IM mais populares nos últimos três anos no Brasil.



Fonte: PANORAMA MOBILE TIME, 2018

Com os dados trazidos à baila, temos como certo que a difusão do uso de aplicativos de mensagens instantâneas está amplamente difundido no mundo e no Brasil e, entre os aplicativos mais utilizados no Brasil temos o WhatsApp, o Facebook Messenger e o Telegram. O WhatsApp é, também o aplicativo de mensagens instantânea mais popular no mundo e por isso será usado como exemplo no desenvolvimento da pesquisa.

Cada um desses aplicativos de mensagens instantâneas traz um tipo de proteção criptográfica que pretende proteger as conversas dos usuários e, muito embora haja diferenças entre os aplicativos, o importante para a presente pesquisa é o fato da criptografia estar presente como forma de defesa da esfera privada do usuário e não tanto o tipo de criptografia, a não ser a título de potencial protetivo, suas consequências e a possibilidade de rompimento dessa proteção, em especial pelo poder público. Não é o objetivo da presente pesquisa alcançar todos os aplicativos de mensagens instantâneas eis que a cada dia

surgem novos aplicativos dessa espécie, ademais o principal escopo do trabalho é a criptografia como forma de proteção geral da privacidade das conversas entre usuários pelos aplicativos de mensagens instantâneas e a possível intervenção do poder público, enquanto provedor de segurança estatal, na esfera privada criada pelos aplicativos mencionados. Para tal, faz-se o recorte mais específico da utilização dos três aplicativos de mensagens instantâneas mais utilizados pelos usuários brasileiros, de acordo com a pesquisa aqui apontada. O WhatsApp, o Facebook Messenger e o Telegram, com ênfase no primeiro não apenas por ser de longe o mais popular mas também por ser o que mais questionamentos judiciais trouxe a respeito do conflito entre privado e público, porém antes de focar no aplicativos em si e na sua intenção de proteção da privacidade, há necessidade de explorar um pouco mais o conceito de criptografia.

CAPÍTULO 3 – A CRIPTOGRAFIA E A GARANTIA DA PROTEÇÃO DE DADOS PRIVADOS.

3.1 O CONCEITO DE CRIPTOGRAFIA EM PERSPECTIVA HISTÓRICA E TÉCNICA.

Podemos definir a criptografia como “a arte de escrever em cifra ou em código, de modo a permitir que somente quem conheça o código possa ler a mensagem” (MARCACINI, 2010, p. 10), ou seja a criptografia é uma forma de mandar mensagens cifradas com o intuito de manter em segredo seu conteúdo, uma forma de manter em privado ideias e mensagens que serão disponibilizadas apenas entre o emitente (ou emitentes) e receptor (receptores).

A história da criptografia se mistura com a história da própria escrita pois ambas servem para a comunicação entre pessoas sendo o segredo o laço que une a comunicação propriamente dita e a criptografia enquanto forma de enviar mensagens.

De maneira geral, os primeiros sinais daquilo que modernamente pode-se considerar criptografia surgiram há cerca de 4000 anos no Egito antigo, onde se encontrou no túmulo de Khnumhotep II, um nobre egípcio (1900 ac), hieróglifos incompreensíveis para o resto da população. Porém não apenas no Egito antigo pode-se imaginar que surgiu a criptografia. Em outros pontos e em outros tempos há sinais da intenção de ocultar mensagens, como no caso dos hebreus e as cifras *Atbash, Atbah e Albam*[13] que utilizavam o alfabeto hebraico como chave para cifrar mensagens secretas (NETO et al, 2014, p. 05).

No ano 100 ac, em Roma, Júlio César utilizava criptografia para transmitir mensagens secretas aos seus generais por meio de uma forma de criptografia por substituição[14] chamada de cifra de César, ou troca de César. A função criptográfica usada por César foi uma mudança por 3 cifras. Cada letra foi pulada

[13] Atbash vem da grafia das letras hebraicas **A**leph, **T**av, **B**eth, **Sh**in enquanto Atbah vem da grafia das letras hebraicas **A**leph, **T**eth, **B**eth e **H**eth e a cifra Albam das letras **A**leph, **L**amed, **B**eth e **M**em e esse tipo de criptografia consistia na substituição de umas letras por outras com o intuito de embaralhar a mensagem e torna-la legível apenas para quem soubesse a cifra.

[14] Consiste em uma técnica de simples substituição da letra de um texto por outra do alfabeto de acordo com uma tabela pré-designada.

em 3 posições, então a letra 'A' seria substituído por 'D', 'B' seria substituída por 'E' e assim por diante e, quando chegasse a última letra, retornaria o alfabeto do começo.

Embora a Cifra de César seja talvez a mais famosa forma de criptografia antiga, ainda existem outros importantes marcos históricos da criptografia, como a Cifra de Vigenere, surgida no século XVI e que é a primeira cifra que utiliza uma chave para criptografar mensagens e que consiste na utilização de várias cifras de substituição monoalfabéticas, em vez de apenas uma, com uma chave de código específica que deve ser empregada para criptografar cada símbolo de texto sem formatação, que resultará em cifras conhecidas como polialfabéticas.

> O artifício incide basicamente em substituir cada letra na mensagem por outra que estivessem deslocadas algumas “casas `a frente no alfabeto. Ele versa de 26 alfabetos, sendo que na primeira linha está o alfabeto na ordem correta e nas linhas seguintes utiliza-se a Cifra de César deslocando uma casa em comparação com a linha anterior (...) (SANTOS, 2016, p. 09)

Assim como na cifra de César, a cifra de Vigenere também pode ser facilmente decifrada, no entanto, a cifra de Vigenere trouxe a ideia de introduzir chaves de criptografia, aumentando a dificuldade de quebra do código. Dessa feita, comparando-se as duas cifras, o sigilo da mensagem depende do sigilo da chave de criptografia é mais importante do que o sistema em si, por essa razão a Cifra de Vigenere é muito mais confiável do que a Cifra de César.

Como podemos notar, a criptografia tornou-se uma ferramenta de guerra em muitos aspectos e, por isso, no início do século XX, com advento do uso da tecnologia como máquina de guerra, a criptografia começou a ser operada por máquinas, tanto para criptografar como nas tentativas de descriptografar informações estratégicas. Essa mecanização levou a aceleração e complexidade do processo de cifragem e decifragem tendo como melhor exemplo na segunda guerra mundial.

A mais famosas dessas formas de mecanização em cifragem utilizada na segunda guerra mundial foi a máquina conhecida como Enigma, utilizada pelos alemães. A Enigma se parecia com uma máquina de escrever, porém ao invés de papel, um painel luminoso com o alfabeto se mostrava. Essa máquina utilizava

uma chave para decifrar ou cifrar mensagens e, com rotores eletromecânicos, configurava-se a máquina conforme a necessidade.

Dentre estes equipamentos o mais conhecido é a máquina Enigma, utilizada pelos alemães durante a Segunda Guerra Mundial.

A Enigma lembra um pouco uma máquina de escrever, onde ao invés de colocar o resultado no papel, o mesmo era mostrado em um painel luminoso com os caracteres do alfabeto. A chave usada para cifrar/decifrar uma mensagem era configurada por meio de rotores eletromecânicos (3 ou mais) que podiam ser alterados conforme a necessidade para formar a chave. Por muito tempo, pela complexidade trazida pela máquina, a criptografia criada a partir de um dispositivo eletromecânico foi considerada indecifrável e, tal concepção, só foi modificada com o esforço de cientistas, dos quais Alan Turing era o mais conhecido e, mesmo assim, utilizando a ajuda do que poderíamos hoje classificar de computador.

Atualmente, são duas as formas de criptografias utilizadas convencionalmente: simétrica e assimétrica (MOTA, 2016, p. 13; MARCACINI, 2010, p. 26), sendo que a simétrica é um tipo de criptografia mais antiga que consiste numa chave secreta que pode ser um número, uma palavra ou uma sequência de letras e números que é compartilhada apenas entre os comunicantes. Existem cinco pontos que classificam a criptografia simétrica:

> a) Texto em claro: Mensagem ou dados em claro, perfeitamente inteligíveis que alimentarão o algoritmo de criptografia como entrada;
> b) Algoritmo de criptografia: Sequência de regras e procedimentos lógicos previamente definidos que realizam inúmeras trocas e transformações no texto em claro;
> c) Chave: Trata-se de um valor independente do texto claro e do algoritmo e será utilizado também como entrada para o algoritmo criptográfico. As trocas e transformações realizadas pelo algoritmo no texto em claro dependem desta chave;
> d) Texto Cifrado: Mensagem embaralhada. É a saída do algoritmo de criptografia. Essa saída é um fluxo de dados aleatórios em formato ininteligível;
> e) Algoritmo de decriptografia: Basicamente é o algoritmo de criptografia executado de forma inversa. Utiliza o texto criptografado e a chave secreta para a formar novamente o texto original em claro. (STALLINGS, 2008 apud MOTA, 2016, p. 14)

O grande problema desse tipo de criptografia é que essa chave utilizada para criptografar e decriptografar a mensagem deve ser compartilhada entre os comunicantes o que cria uma vulnerabilidade a partir do momento em que há real possibilidade de interceptação dessa chave e, quem o fizer, pode decifrar o teor das mensagens criptografadas com essa chave. Logo se vê que esse método é, em seu fundo, tal qual a Cifra de Vigenere ou mesmo a Cifra de César, uma codificação que depende de uma chave conhecida entre as partes e, portanto, não tão difícil de ser decriptada.

Por conta dessa fragilidade, é proposta a criptografia assimétrica em 1976 por Whitfield Diffie e Martin Hellman, em artigo intitulado *"New directions in cryptography"* (MARCACINI, 2010, p. 31) em que duas chaves secretas, uma pública, aberta, para todos que queiram enviar uma mensagem para certa pessoa e uma segunda, privada, que apenas o usuário possui, dessa forma um texto para ser decodificado precisa da chave pública e da chave privada, gerando muito mais segurança.

> A criptografia assimétrica, ao contrário da convencional, utiliza-se de *duas* chaves: uma das chaves dizemos ser a *chave privada*, e a outra, a *chave pública*. Estas duas chaves são números que funcionam como complemento um do outro, se assim as podemos explicar, estando de tal modo relacionadas que não poderiam ser livremente escolhidas pelo usuário, devendo ser calculadas pelo computador. (MARCACINI, 2010, p. 31).

Então, pode-se agora compreender a chamada criptografia de ponta-a-ponta, que nada mais é do que a criptografia assimétrica que faz a decriptação da mensagem com a chave privada em cada ponta, ou seja, cada usuário, o que envia e o que recebe, tem chaves privadas únicas em seu poder, e apenas ele, com essa chave, pode decriptar a mensagem enviada. Apenas "nas pontas" ou, de maneira mais apropriada como originariamente se chama, *end-to-end,* se processa a decriptação.

Os aplicativos de mensagens instantâneas utilizam diferentes formas de proteção de privacidade, sendo o mais destacado a criptografia que se modifica dependendo do aplicativo, cada aplicativo utiliza um sistema, chamado de protocolo além de diferença quanto ao acionamento da proteção criptográfica propriamente dita nas conversas. Mas todos convergem no sentido de que a

criptografia é uma forma de proteção da privacidade sendo seu valor proporcional ao nível de segurança que esse método criptográfico traz às conversas privadas.

Atualmente, conforme já observamos em capítulos anteriores, o conceito de privacidade mudou a medida que a sociedade mudou e adentrou a pós-modernidade, adaptando-se a liquidez das relações humanas pautadas pelo capitalismo que permeia a Sociedade da Informação. Conforme já explicado, a própria informação tem um valor pecuniário e, como tal, é objeto de cobiça e merece proteção no nosso direito. A medida que avança a busca e o acesso a informação, não raro a privacidade é solapada e, como resposta a isso, o Direito tem trazido novas perspectivas de defesa nesse sentido. Na Europa entrou em vigor o General Data Protection Regulation (PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA, 2016) em 25 de maio de 2018, cujo objetivo é proteger a esfera privada do indivíduo, os dados gerados por ele e criar mecanismos que diluam o acesso, em especial comercial, a dados sensíveis, porém embora o GDPR simbolize uma vitória da privacidade na sociedade atual, não trata de criptografia de maneira direta, mas de encriptação e, ainda assim apenas como recomendação de uso para proteção e dados privados, sem obrigação de que se adote a criptografia. Nesse passo, também foi aprovada recentemente no Brasil a Lei de Proteção de Dados Pessoais no Brasil, a Lei 13.709 de 14 de agosto de 2018, que segue o modelo da GDPR em tentar proteger os dados pessoais privados, porém nem mesmo chega a mencionar a criptografia ou encriptação. Ambas as legislações demonstram de maneira bastante clara que não se pode mais tratar a quebra da privacidade como um efeito colateral da vida digital e tentam impor regras claras sobre o assunto.

A lei brasileira de proteção de dados, já em seu artigo 2º, no primeiro inciso[15] anuncia que o respeito a privacidade é o fundamento dessa lei, dessa forma, em comparação com a GDPR europeu vemos que embora haja previsão legal de proteção à privacidade, a encriptação é apenas sugerida como uma diretriz de segurança da informação o Decreto 8.771 de 11 de maio de 2016, que

[15] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
(...)" (BRASIL, 2018)

regulamenta o Marco Civil da Internet, trata dessa forma a encriptação em seu artigo 13, IV[16].

Portanto, pode-se concluir que cada provedor de aplicativos de mensagens instantâneas no Brasil tem o dever legal de proteger a privacidade dos seus usuários, mas o uso de criptografia é apenas uma ferramenta sugerida como forma de proteção à privacidade. Resta, portanto, saber como cada aplicativo faz essa proteção de dados privados, em especial as conversas e se há limites a essa proteção.

3.2 AS FORMAS DE PROTEÇÃO DE DADOS MAIS UTILIZADAS NOS APLICATIVOS DE COMUNICAÇÃO INSTANTÂNEA MAIS POPULARES.

A criptografia ainda é a forma de proteção de dados mais utilizada entre os aplicativos de mensagens instantâneas, utilizada conforme cada aplicativo exige. Existem vários aplicativos de mensagens instantâneas que se adequam à conceituação apresentada, porém o recorte aqui feito trata dos três aplicativos de mensagens instantâneas mais populares no Brasil, de acordo com a pesquisa da Panorama Mobile Time (2018), e que utilizam alguma forma de criptografia. Tais aplicativos servirão como base para entendermos as diferentes formas de criptografia pois não apenas são os mais populares no Brasil, mas também utilizam criptografia com certas diferenças importantes.

O WhatsApp é um aplicativo de mensagens instantâneas criado em 2009 pelo ucraniano Jan Koum e pelo norte-americano Brian Acton, ex-funcionários do Yahoo, originalmente como um aplicativo de "atualização de status" mas que rapidamente se tornou um aplicativo tal qual conhecemos, um aplicativo de mensagens de texto e software por voz (já em 2009 o WhatsApp incorporou a

[16] "Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
(…) IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes." (BRASIL, 2016)

funcionalidade de troca de fotos) com foco na liberdade, tráfego de dados irrestritos e interoperalidade (FAURE; SANTOS, 2018).

Em 2014, ano em que o WhatsApp foi adquirido pelo Facebook, já contava com mais de 400 milhões de usuários no mundo, quebrando a barreira do um bilhão de usuários em 2016.

O WhatsApp adicionou a criptografia de ponta-a-ponta assimétrica em 2016 como regra para todas as conversas, não podendo ser desligada mesmo que o usuário queira. Essa proteção, em tese, permite que apenas os próprios usuários envolvidos tenham acesso ao conteúdo das mensagens trocadas, arquivos e imagens enviadas, sendo certo que nem mesmo o provedor de serviço tem acesso a esse conteúdo.

> WhatsApp end-to-end encryption ensures only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. For added protection, every message you send has an unique lock and key. All of this happens automatically: No need to turn on settings or set up special secret chats to secure your messages.[17] (WHATSAPP, 2018)

O WhatsApp utiliza o protocolo Signal, do Open Whisper Systems, lançado em 2016 e é obrigatório para toda a conversa pelo WhatsApp. Tal protocolo tem o código-fonte aberto ao público, ou seja, qualquer usuário tem acesso aos códigos de programação do protocolo garantindo a transparência de seu uso. Porém, embora se possa comprovar a segurança do protocolo em si, não existe comprovação da implementação desse protocolo no WhatsApp e como se dá o seu uso, salvo esparsos estudos que explicam apenas genericamente como se aplica o protocolo no WhatsApp (ANTUNES; KOWADA, 2018)

A criptografia ponta-a-ponta assimétrica utilizada pelo WhatsApp fornece uma proteção enorme pois, de acordo com o WhatsApp, as mensagens não ficam

[17] “Criptografia ponta-a-ponta do WhatsApp garante que somente você e a pessoa com quem você se comunica possam ler o que foi enviado, sem nenhum intermediário, nem mesmo o WhatsApp. Suas mensagens são fechadas com trancas e somente o receptor e você tem as chaves especiais para destrancar e ler suas mensagens. Para aumentar a proteção, toda mensagem enviada tem uma única fechadura e chave. Tudo isso acontece automaticamente: Sem necessidade de ligar nas configurações ou abrir conversas privadas para garantir a segurança das suas mensagens. “ (tradução livre)

salvas nos servidores depois de enviadas ao receptor (WHATSAPP, 2018) e, dessa forma, a única forma razoável de se ter acesso às mensagens seria ter acesso ao telefone, ou ao chip com o número de telefone cadastrado. A esse respeito, em 2017 o jornal inglês The Guardian informou o que seria uma quebra na segurança do WhatsApp em referência exatamente à troca de um chip de telefone, por exemplo, em que, em tese, se alguém tiver acesso ao chip de um dos usuários e instalar esse chip em outro celular poderia continuar conversando com o outro sem que haja ciência da troca e, ainda pior, caso haja alguma mensagem que não foi entregue, pelo receptor estar offline, essa mensagem será novamente encriptada pois a instalação de um novo WhatsApp gera novas chaves e a mensagem será entregue nesse novo telefone que utiliza o chip de telefone original, sendo que o emissor não terá ciência de que a mensagem, originalmente enviada para certo receptor, está agora com um outro receptor que possui o chip original. Ou seja, de acordo com essa reportagem (GANGULY, 2017), poderia ser interceptada a mensagem antes que ela chegasse ao receptor, bastando que o telefone desse receptor estivesse offline e, somente quando o telefone voltasse a estar online (ou com o chip original do receptor ou com um chip recadastrado com aquele telefone do receptor), as mensagens seriam todas enviadas de uma vez e o novo receptor receberia tais mensagens, sem que o emissor soubesse que a mensagem foi recebida por um emissor que não aquele pretendido. O WhatsApp, conforme explicado, sempre que instalado em um novo telefone gera novas chaves, mas isso não gera, a princípio, nenhuma informação ao emissor de que houve mudança na chave. Tudo é feito internamente, a não ser que o usuário especificamente peça, na configuração do seu WhatsApp, a two-step verification (verificação em duas fases) que foi introduzida em fevereiro de 2017 e consiste em criar uma senha de seis dígitos que deve ser adicionada juntamente com o número do telefone e que será utilizada a cada sete dias como comprovante de identidade.

Como se vê, há sempre vulnerabilidades e pouca certeza sobre a efetividade da criptografia no WhatsApp, muito embora estudos apontem o uso do protocolo Signal, de maneira eficiente (ANTUNES; KOWADA, 2018), ainda assim

a forma como é utilizada internamente pelo WhatsApp deixa ainda algumas dúvidas.

O outro aplicativo de mensagens bastante popular no Brasil, que também utiliza criptografia ponta-a-ponta, é o Facebook Messenger, porém com algumas diferenças cruciais em relação ao WhatsApp informado alhures, como por exemplo o fato de não ser obrigatório o uso desse tipo de criptografia, ao contrário, para que se possa ter acesso a proteção criptográfica é necessário que o usuário escolha “conversa secreta” e, somente nesse modo que a criptografia assimétrica será acionada, de maneira semelhante ao Signal (também utilizado pelo WhatsApp), inclusive com as conversas não sendo arquivadas nos servidores do Facebook. Porém, isso somente ocorre nas “conversas secretas”

> As conversas secretas no Messenger são criptografadas de ponta a ponta. Isso significa que as mensagens são destinadas apenas a você e à outra pessoa, a mais ninguém, nem à nossa equipe. As conversas secretas são diferentes das conversas comuns do Messenger. Por exemplo, você pode optar pela configuração que faz as mensagens desaparecerem. (FACEBOOK, 2018)

Essas “conversas secretas”, diferente das conversas normais, não são acessíveis de outras plataformas (O Facebook Messenger pode ser acessado, da mesma conta, em diversas plataformas, tais quais computadores, tablets e celulares) mas, nunca é demais lembrar, essa “conversas secretas”, que só ocorrem individualmente, não em grupo, não são o padrão, para acessar essa proteção há que ligá-la. Outro inconveniente é que o usuário tem que ter uma conta no Facebook para poder utilizar o Messenger, porém em termos de proteção o rito é semelhante o suficiente com o WhatsApp para que se possa considerar no mesmo nível de segurança.

Por fim, o terceiro aplicativo mais utilizado é o Telegram. Lançado em agosto de 2013 pelos irmãos russos, Pavel e Nikolai Durov, surgiu como reforço a ideia de comunicação segura entre usuários, com criptografia ponta-a-ponta entre usuários, antes mesmo do WhatsApp impor esse tipo de proteção. Porém, tal qual ocorre com o Facebook Messenger, tal mecanismo não é habilitado como padrão, mas sim deve ser iniciado como um “chat secreto” que, tal qual ocorre com seus concorrentes WhatsApp e Facebook Messenger, criptografa a mensagem nas “

pontas” , impedindo que um terceiro, inclusive a própria empresa, tenha acesso ao conteúdo das conversas. Esse aplicativo tem sido objeto de muitas discussões (KARASZ, 2018), em especial no que tange o uso do protocolo de criptografia MTProto, um protocolo que não é aberto, de fabricação própria e que, portanto, ninguém sabe mesmo como funciona, suas falhas e limites. Esse protocolo foi testado pelo MIT que descobriu falhas de segurança que permitiam, com certa facilidade, se descobrir metadados que apontavam, por exemplo, quem conversava com quem e em que horário. Por outro lado, o próprio fundador do Telegram, Pavel Durov, insiste que o protocolo Sigma, utilizado pelo WhatsApp e Facebook Messenger é que não merece confiança, pois teria sido financiado pelo governo dos Estados Unidos da América (DUROV, 2017).

Interessante notar que o Telegram está, em tese, bloqueado na Rússia justamente por se negar a fornecer dados, ainda que haja uma legislação específica que assim obrigue, o Telegram conseguiu, até o momento, esconder seu tráfego como se fosse tráfego do Google, escapando assim do bloqueio russo (BURGESS, 2018);

Além dessas discussões, o Telegram tornou-se popular no Brasil por conta dos bloqueios judiciais ocorridos que baniram o uso, temporariamente, do WhatsApp em todo território brasileiro.

CAPÍTULO 4 – O CONFLITO ENTRE A PRIVACIDADE E A SEGURANÇA PÚBLICA NAS DECISÕES JUDICIAIS RECENTES NO CASO DO “WHATSAPP”

4.1 AS DECISÕES JUDICIAIS QUE ENVOLVERAM O PÚBLICO E PRIVADO EM RELAÇÃO AO “WHATSAPP”.

No Brasil, a questão da privacidade na proteção de dados criptografados em aplicativos de mensagens instantâneas é focado no uso do aplicativo WhatsApp, o mais popular no país.

A primeira decisão sobre o assunto se deu em 25 de fevereiro de 2015, em cumprimento a mandado judicial expedido pela Central de Inquéritos da Comarca de Teresina determinando a suspensão temporária, em todo o Brasil, do WhatsApp, tendo em vista, de acordo com Irineu Francisco Barreto Júnior e Marco Antonio Lima (2016, p. 39) a inoperância do WhatsApp em fornecer dados que pudessem levar ao sucesso da investigação criminal que buscava provas “de imagens de crianças e adolescentes expostas sexualmente no aplicativo de mensagens instantâneas”. O trâmite do processo encontra-se em segredo de justiça e também não prosperou além do mesmo dia, não surtindo efeitos, eis que a decisão foi derrubada pelo Tribunal de Justiça do Piauí sob o argumento de que a decisão monocrática era desproporcional (BARRETO JÚNIOR; LIMA, 2016, p. 39). Vemos aqui a primeira ocorrência do conflito entre a questão pública e privada que foi solucionada de maneira transversal com base no argumento da desproporcionalidade na decisão que, levada a efeito, causaria prejuízo a milhões de brasileiros e, por consequência a empresa WhatsApp. Veja que a pressão para forçar a empresa a fornecer os dados que o Poder Público entendia necessários para proceder a defesa da segurança pública demonstra exatamente o conflito aqui estudado, porém o Poder Judiciário em sua segunda instância não enveredou pela discussão a respeito do conflito entre os direitos e sim pela questão da desproporcionalidade e dos efeitos da decisão.

A primeira decisão que, de fato causou algum efeito foi prolatada no final do mesmo ano, em dezembro, quando o WhatsApp foi bloqueado por 48 horas por uma determinação da 1ª Vara Criminal de São Bernardo do Campo (SP). Na decisão que tratou da questão de crime organizado foi cassada também em segunda instância em decisão da 11ª Câmara Criminal do Tribunal de Justiça do Estado de São Paulo que determinou o restabelecimento do aplicativo, também apelando a questão da desproporcionalidade da decisão conforme trecho destacado da decisão:

> Sob esse aspecto, em face dos princípios constitucionais, não se mostra razoável que milhões de usuários sejam afetados em decorrência da inércia da impetrante, mormente quando não esgotados outros meios disponíveis para a obtenção do resultado desejado. Cita a magistrada que foi imposta multa coercitiva, sem sucesso, daí a adoção da medida extrema. Mas é possível, sempre respeitada a convicção da autoridade apontada como coatora, a elevação do valor da multa a patamar suficiente para inibir eventual resistência da impetrante, solução que, aparentemente, não foi adotada na origem. (BRASIL, 2017)

A argumentação da proporcionalidade se sustenta nessa decisão, amparada por outro argumento que é bastante importante para o trabalho aqui desenvolvido que é a possibilidade de se conseguir o efeito desejado por outros meios juridicamente possíveis, no caso segundo sugestão do magistrado *ad quem,* a elevação da multa diária. Abre-se, portanto, a possibilidade de se chegar ao um resultado aceitável na busca do interesse público sem ter que suprimir o direito ao uso do aplicativo.

No ano seguinte, em março, o juiz da Vara Criminal de Lagarto (SE) decretou a prisão de Diego Jorge Dzodan, vice-presidente do Facebook na América Latina por conta da negativa de quebra do sigilo telemático em certo processo criminal sobre tráfico de drogas interestadual. De acordo com o processo, a Polícia Federal solicitou, por diversas vezes, que o Facebook determinasse a quebra das comunicações. O Sr. Dzodan chegou a ser levado para o Centro de Detenção Provisória de Pinheiros até que foi concedida liminar em Habeas Corpus para libertar o paciente em decisão do Desembargador plantonista Ruy Pinheiro da Silva, do Tribunal de Justiça do Estado de Sergipe (BRASIL, 2016). Como as investigações continuaram, mas a negativa de

fornecimento dos dados requeridos pelo Poder Público também continuou, em maio de 2016, novamente a Vara Criminal de Lagarto (SE) determinou que a inoperância do Facebook em obedecer as requisições do juízo deveria resultar em ordem no sentido de suspender os serviços do aplicativo WhatsApp em todo o território brasileiro por 72 horas. Primeiramente o pedido de liminar no Mandado de Segurança 201600110899 impetrado pelo Facebook pretendendo o restabelecimento do aplicativo foi negado (BARRETO JÚNIOR, LIMA, 2017, p. 40) mas, embora em segredo de justiça, parte do embasamento da decisão que negou o pedido de liminar e fez permanecer a decisão de bloqueio pode ser examinado pois em outro caso a argumentação dessa decisão foi levada aos autos[18] e vale aqui mencioná-la:

> Em verdade, o direito à privacidade dos usuários do aplicativo encontra-se em conflito aparente com o direito à segurança pública e à livre atuação da Polícia Federal e do Poder Judiciário na apuração de delitos, em favor de toda a sociedade. Neste primeiro momento, percebo que a impetrante, em verdade, minimiza a importância da investigação criminal de componentes de organização criminosa que utilizam o aplicativo em questão, escamoteando a gravidade do delito supostamente praticado (tráfico interestadual de drogas), sob a pecha de garantir o direito à intimidade de seus usuários. Ora, o uso do aplicativo por quem quer que seja e para qualquer fim não pode ser tolerado sem ressalvas. Deve, sim, sofrer restrição quando atinge outros direitos constitucionalmente garantidos, como no caso em comento. (BRASIL, 2016)

Nessa decisão, o desembargador Cezário Siqueira Neto, plantonista no momento em que decidiu pelo não acolhimento da liminar, enfrenta de maneira bastante rápida a questão do conflito entre a privacidade e o direito a segurança pública, dando claramente prevalência do segundo sobre o primeiro no caso concreto, indicando que não se pode usar o direito fundamental à privacidade sem ressalvas. Essa decisão foi logo em seguida modificada em virtude de um pedido de reconsideração que, apreciado pelo desembargador titular Ricardo Múcio Santana de Abreu Lima foi acolhido pondo fim ao bloqueio do WhatsApp. Infelizmente por força do segredo de justiça decretado no processo, não se tem

[18] Essa parte da decisão em segredo de justiça do MS 201600110899/SE foi trazida na decisão de primeiro grau prolatada pela juíza Daniela Barbosa Assumpção de Souza, da 2ª Vara Criminal de Duque de Caxias (RJ) que não se encontra em segredo de justiça (BRASIL, 2016).

acesso ao teor da decisão do desembargador. Um dos pontos mais importantes nesse último caso, porém, é que o WhatsApp já utilizava criptografia ponta-a-ponta, e uma das argumentações do Facebook na época foi de que não possuía o WhatsApp acesso às mensagens trocadas pois não estavam mais registradas em seus servidores, apenas nos aparelhos celulares dos comunicantes, portanto o Poder Público requisitava um dado que a empresa não possuía.

Apenas dois meses depois o WhatsApp voltou a ser bloqueado por ordem judicial, dessa vez a ordem veio da 2ª Vara Criminal de Duque de Caxias (RJ), novamente por conta do descumprimento de ordens, por parte do Facebook, em desabilitar a chave de criptografia, conforme trecho da decisão:

> Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia.(BRASIL, 2016)

De acordo com os estudos aqui apresentados, em especial pelo funcionamento da criptografia de ponta-a-ponta, seria impossível desabilitar essa chave sem que os usuários envolvidos tivessem ciência, porém o ponto mais interessante da decisão vem a seguir:

> Há de se considerar, porém, que a codificação criptografada imposta às conversações online pelo Whatsapp não pode servir de escudo protetivo para práticas criminosas que, com absurda frequência, se desenvolvem através de conversas, trocas de imagens e vídeos compartilhados no aplicativo. Nem se deve entender que a quebra do sigilo e interceptação telemática do aplicativo traria insegurança aos usuários, uma vez que a decisão judicial é sempre fundamentada, específica e abarca usuários que estejam praticando crimes dentro do território nacional. Ora, se assim não fosse, inviável seria a quebra do sigilo de correspondência, ligações telefônicas ou correios eletrônicos (Gmail, Yahoo, Hotmail etc), sempre possível em decorrência de ordem judicial, sendo certo que tais serviços – ou suas empresas – jamais deixaram de ser confiáveis em virtude da possibilidade legal de quebra. (BRASIL, 2016)

De acordo com essa decisão, temos que o Poder Público teria um poder de, guardada as devidas cautelas legais, se imiscuir na vida privada sob o argumento de que o sigilo é relativo e sua quebra não destrói a confiança na

proteção à privacidade. Há uma relativização da privacidade enquanto direito fundamental em face do direito social à segurança pública. Essa linha de raciocínio é semelhante a desenvolvida por Tércio Sampaio Ferraz Júnior (et al, 2016) em artigo na Folha de São Paulo no qual ele defende que o Estado não podendo, sob nenhuma hipótese, ter acesso às conversas do aplicativo WhatsApp estaria impotente em certa área da atividade humana e, então, seria a primeira vez que o Estado não teria acesso a um certo espaço. Teríamos uma espécie de buraco negro, intocável pelo Estado o que desidrataria o Poder de Polícia gerando uma omissão constitucional na obrigação e garantir a segurança pública. Algo parecido com o que foi alegado na decisão acima comentada, em que se traz à luz outras formas de comunicação, inclusive informática como mail que estão sujeitos ao escrutínio do Poder Estatal.

Essa linha de raciocínio é seguida também em outros pontos do globo, como no caso da Primeira-Ministra britânica Theresa May que já alegou, de acordo com o jornal The Guardian (HERN, 2018) que a encriptação cria “espaços seguros para se comunicar”, referindo-se a terroristas que teriam, por conta da encriptação, espaços livres, inacessíveis ao Estado gerando problemas de segurança pública.

A decisão de suspensão do WhatsApp da 2ª Vara Criminal de Duque de Caxias foi derrubada por força de liminar concedida por José Roberto Lagranha Távora, desembargador do Tribunal de Justiça do Rio de Janeiro, concedida em Mandado de Segurança impetrado pelo Facebook, porém essa decisão não teve efeitos práticos eis que antes o ministro Ricardo Lewandowski do Supremo Tribunal Federal havia também deferido uma liminar em sede de controle concentrado de constitucionalidade, mais precisamente na Arguição de Descumprimento de Preceito Fundamental 403 proposta pelo Partido Popular Socialista em face da decisão da Vara Criminal de Lagarto (SE) sob a argumentação de que a suspensão do aplicativo e de seus serviços aparentemente violaria preceito fundamental da liberdade de expressão e comunicação além da legislação pertinente (BRASIL, 2016). Ainda em controle de constitucionalidade, foi também proposta a Ação Direta de Inconstitucionalidade

5527 pelo Partido da República (PPR) arguindo a inconstitucionalidade dos Arts. 10 e 12, III e IV, da Lei nº 12.965/2014 (Marco Civil da Internet) eis que esses artigos embasavam boa parte das suspensões dos serviços de WhatsApp. Ao convocar a audiência, o ministro elaborou

4.2 A ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403 E A AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5527.

As ações de controle concentrado de constitucionalidade que tratam do assunto dos bloqueios do WhatsApp e, consequentemente, do conflito entre a necessidade de manter a privacidade em confronto com os designíos da segurança pública, foram propostas no mesmo ano com focos diferentes, dentro das especificações de cada ação. A Arguição de Descumprimento de Preceito Fundamental tem como objeto evitar ou reparar lesão a preceito fundamental resultante de ato do Poder Público ou solucionar controvérsia constitucional a respeito de lei ou ato normativo federal, estadual ou municipal, nos termos da Lei 9.882/99 (BRASIL, 1999) e, especificamente a ADPF 403/DF questiona a decisão da Vara Criminal de Lagarto (SE) que suspendeu o uso do WhatsApp em todo o país e que, de acordo com a inicial da ADPF, viola preceito fundamental específico contido no artigo 5º, IX da Constituição Federal[19] no que tange a interpretação da norma constitucional em destaque. Em 19 de junho do mesmo ano o pedido liminar foi acolhido em decisão do Ministro Ricardo Lewandowski para "para suspender a decisão proferida pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ (...)" (BRASIL, 2016a) e fundamentou sua decisão na desproporcionalidade da medida relacionando também uma análise rápida de possível afronta à liberdade de expressão, eis que a suspensão do

[19] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...)
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;" (BRASIL, 1988);

serviço alijou grande parte dos brasileiros da comunicação instantânea pelo aplicativo mais popular desse tipo.

> Ora, a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa. (BRASIL, 2016a)

Importante salientar também que o Ministro Lewandowski, tomando cuidado de não adentrar muito no mérito, mencionou a importância específica do aplicativo de mensagens instantâneas WhatsApp em nosso país ao acomodar em sua decisão o fato do aplicativo ser utilizado inclusive como forma de comunicação de atos do poder judiciário como despachos e intimações em casos urgentes (KOPLIN, 2016).

A ADPF 403/DF tem uma estrutura e pedidos muito mais simples do que a ADI 5527/DF proposta pelo Partido da República (PR), da relatoria da Ministra Rosa Weber. O pedido consiste “na declaração da inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14, bem como a interpretação conforme do art. 10, §2º, a fim de que seja limitado o seu alcance aos casos de persecução criminal.” (BRASIL, 2016a).

Basicamente, o petitório utiliza como argumentação a liberdade de expressão e uso da internet livre por todos, sem a sombra do Estado a limitá-la, conforme se depreende do trecho abaixo, que apresenta o argumento da exordial nesse ponto:

> Cenários desastrosos como os recentemente impostos por decisões que suspenderam o acesso a tais serviços de troca de mensagens online foram previstos por Jonathan Zittrain. Há quase dez anos, o renomado autor anteviu que o futuro da internet estaria em risco, pois detentores de poder econômico e autoridades com poder de polícia interfeririam cada vez mais no modelo aberto, descentralizado e criativo da internet, sob o argumento de segurança e controle (BRASIL, 2016a)

Com efeito, por conta do grande envolvimento do assunto e dos inúmeros *amicus curiae* presentes, o Ministro Edson Fachin decidiu convocar uma

Audiência Pública para discutir a questão da criptografia no WhatsApp nas duas ações conjuntas.

Para tal, o foram criadas 4 questões que deveriam ser abordadas pelos convidados:

> 1 - Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?
> 2 - Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?
> 3 - Seria possível desabilitar a criptografia ponta a ponta (ent do end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
> 4 - Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível 'espelhar" as conversas travadas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação de um usuário específico? (BRASIL, 2016a)

Com a audiência pública, podemos ter uma melhor noção dos problemas técnicos e jurídicos sobre o assunto, conforme a seguir será exposto.

4.3 AS AUDIÊNCIAS PÚBLICAS QUE DISCUTIRAM A QUESTÃO DA PROTEÇÃO DE DADOS PRIVADOS NO ÂMBITO DA COMUNICAÇÃO INSTANTÂNEAS NO SUPREMO TRIBUNAL FEDERAL (ADPF 403 E ADI 5527).

A audiência pública se deu nos dias 02/06/2017 e 05/06/2017, e foram ouvidos 24 especialistas: os professores universitários Anderson Nascimento (University of Washington-Tacoma), Diego Aranha (Unicamp) e Marcos Simplício (Poli-USP), representantes da Federação das Associações das Empresas de Tecnologia da Informação (Fabio Maia), do Centro de Pesquisa e Desenvolvimento em Telecomunicações (Alexandre Braga), do Laboratório de Pesquisa Direito Privado e Internet da Universidade de Brasília (Marcelo Gomes), do Centro de Competência em Software Livre do Instituto de Matemática e Estatística da USP (Nelson Lago), do Comitê Gestor da Internet (Demi Getschko), além de Brian Acton, co-fundador e vice-presidente do WhatsApp.

Conforme já havia sido exposto no presente trabalho e ficou claro nas exposições, é impossível a interceptação de mensagens, mesmo pelo próprio WhatsApp sem que se modifique o próprio protocolo criptográfico (ABREU, 2017).

De acordo com os especialistas, as razões pelas quais a imposição dessas mudanças não resolveria o problema:

> - seria ineficaz, uma vez que não impediria, na prática, que criminosos detectassem a vigilância nem tivessem acesso, por outros meios, a versões seguras de criptografia para se comunicar;
> - fragilizaria todo a segurança do aplicativo, já que a introdução de uma forma de 'acesso excepcional' tornaria o sistema mais complexo e, por isso, mais vulnerável;
> - traria problemas de escala, uma vez que o aplicativo teria de ser 'particularizado' para o Brasil, impondo dificuldades de gestão e execução a nível mundial;
> - violaria liberdades, de programadores (de construir sistemas seguros), de usuários (de se comunicar de forma segura e privada, o que é especialmente sensível quando se pensa em ativistas de direitos humanos e profissionais como médicos, advogados e até agentes de segurança) e da empresa (de empreender e oferecer serviços seguros). (ABREU, 2017)

O primeiro a expor foi Felipe Alcântara de Barros Leal (Departamento de Polícia Federal), que iniciou sua exposição indicando que as primeiras argumentações do Facebook a respeito de pedidos de cooperação em investigações era de que eles não se confundiam com o WhatsApp, não podendo responder por eles. O segundo ponto atacado pelo expositor da Polícia Federal se deu no tocante a impossibilidade alegada de que o WhatsApp não podia acessar o conteúdo criptografado, o que levou o expositor a questionar sob outro ponto de vista:

> A pergunta não é "Os senhores têm viabilidade técnica?". Não. A pergunta é: "Por que não as têm?", "Por que não procuram tê-las?". Porque, se for assim, qualquer meio de comunicação vai se blindar alegando uma questão técnica. Simples assim. E aí, nesse ponto, como que a polícia vai realizar a prevenção, como que a polícia vai realizar a obstrução, a neutralização de ações criminosas e como vai apurar, na melhor forma, ou como se imagina, ou como se espera da Polícia Federal, uma ação com essa? (BRASIL, 2016b, p. 18)

Após, o seu colega de Polícia Federal, Ivo De Carvalho Peixinho, complementou a exposição informando que seria possível que o WhatsApp fornecesse os metadados (dados gerais como número de telefones, horário da ligação, duração da conversa entre outros) sem que isso envolvesse a criptografia propriamente dita.

Em seguida expôs, pelo WhatsApp, Brian Acton, co-fundador do WhatsApp, que iniciou relatando sua história pessoal e a de Jan Koum, seu amigo e o outro co-fundador para explicar a importância da privacidade na vida deles. Também reafirmou que, por conta da criptografia, o WhatsApp não tem condições de ler o conteúdo das mensagens e, se fizesse algo para que isso se tornasse possível, abriria possibilidade para que hackers agissem e também afirmou que seria impossível interceptar tais mensagens por força da criptografia, que as tornaria ilegíveis e, respondeu também negativamente quanto a possibilidade de ´desligar´ a criptografia quanto a usuários específicos. Também disse ser impossível espelhar uma conta do WhatsApp em outro dispositivo, muito embora parecesse que o WhatsApp webchat o fizesse, ele disse que não era o caso, que na verdade o WhatsApp webchat cria um ´túnel´ em que utiliza o seu telefone e sua conta do WhatsApp que, se não estiver acessível, não funciona. Acton confirmou, porém, que o WhatsApp detém alguns dados (os chamados metadados) e que eles são disponibilizados à Polícia quando requisitados, porém as mensagens criptografadas são impossíveis de se acessar. (BRASIL, 2016b, p. 26-40).

Neide Cardoso de Oliveira, pelo Ministério Público foi a próxima a se apresentar e reafirmou aquilo que foi dito pelo representante da Polícia Federal a respeito da responsabilidade do Facebook perante o WhatsApp, também informou que não se pode aplicar o princípio da continuidade ao WhatsApp pois este não se enquadra como serviço essencial, que é regulamentado e está sob a supervisão de órgãos regulamentadores. (BRASIL, 2016b, p. 40-47).

Aqui tocamos, novamente, na questão do poder público em contrapartida ao privado, no ponto que o Ministério Público questiona a própria natureza do

serviço prestado pelo WhatsApp e nos remete a natureza do serviço público que é a busca do bem comum e, portanto, sofre regulamentações muito gravosas para assegurar que a administração não se desalinhe de sua finalidade. O WhatsApp é um aplicativo de uma empresa privada e não tem como finalidade o bem comum e sim o lucro, como sói acontecer nas relações comerciais privadas. Ao se arvorar de protetor da privacidade, um caro preceito fundamental como vimos, ele se diz um provedor de um direito fundamental sem, no entanto, se submeter ao controle estatal, ficando ao seu talante como fazer e quando fazer essa proteção. Guardadas as devidas proporções, seria como termos segurança privada que não se submete a regulamentação estatal. É claro que essa argumentação é limitada, pois o WhatsApp se submete as leis do país e a certa regulamentação, mas não há agências regulamentadoras, como há em outros meios de comunicação e em outros espaços da administração pública.

Fernanda Domingos, do Ministério Público questionou alguns pontos da criptografia do WhatsApp, desconfiando do fato, por exemplo, do WhatsApp saber quais são os vídeos virais trocados por mensagens se não teria acesso ao conteúdo das conversas e trocas de arquivos por conta da criptografia. Também questionou a impossibilidade de se usar o chamado ataque do “ homem do meio”, em que a empresa poderia forçar uma nova troca de chaves, “passando a ser responsável pelo intercâmbio das mensagens, criando duas sessões - uma com cada interlocutor - sem interferir no processo criptográfico dos demais usuários” (BRASIL, 2016b, p. 49), apontando que o único problema seria de que os usuários poderiam vir a saber que estão sendo vigiados conferindo cada mensagem e o *QR Code*[20]*,* porém tal procedimento só seria pensado por especialistas. Vladimir Barros Aras, o próximo expositor do Ministério Público apenas usou como argumentação que os dispositivos do Marco Civil atacados não são novidades quanto a proteção jurídica em face de empresas que cometam infrações contra a administração pública, ou seja, que o bloqueio do WhatsApp poderia ter sido pedido inclusive com base em outros dispositivos legais.

[20] Código QR (Quick Response ou Resposta Rápida) é um código de barras bidimensional que pode ser lido por uma câmera, geralmente de smartphone e traduzido em uma sequência alfanumérica.

Bruno Magrani do Facebook Brasil basicamente tratou da separação jurídica e comercial entre o Facebook e o WhatsApp, informando que são entidades distintas e independentes e também falou que a criptografia é uma efetivação da proteção dos direitos humanos reconhecida inclusive pela Assembléia Geral das Nações Unidas.

Demi Getchko, por sua vez, trouxe um lado mais técnico sobre a internet e também trouxe argumentos interessantes para a nossa pesquisa, como o fato da internet “se defender”, ou seja, caso haja uma violação, digamos da proteção da privacidade, a internet, os usuários, programadores arranjarão uma forma de resolver isso criando soluções para manter íntegra a ideia da liberdade na internet. Outro ponto que Getchko trouxe foi que uma das soluções propostas, o ataque do homem-do-meio, não serviria para a finalidade da segurança pública pois aquilo que ele chama de “usuário do mal” estaria sempre cauteloso e buscando saber se há alguém interceptando suas conversas e, de acordo com o que se pode apurar, ele poderia saber se tivesse o conhecimento básico de segurança da informação, como, por exemplo, examinar o *QR Code.* O “usuário comum”, de acordo com Getchko é que poderia sofrer intervenção em sua privacidade sem sabe-lo.

O apontamento de Getchko é muito importante pois leva ao raciocínio de que nem sempre uma regra (ou princípio) com o objetivo de beneficiar alguém acaba por beneficiar de fato. Na verdade, acaba criando mais conflitos em áreas não esperadas. Seria o caso de se ter uma legislação para combater o “usuário do mal” mas que por abranger todos os usuários acaba por prejudicar também o usuário comum. Não seria tão ruim se o “usuário do mal” como Getchko põe não pudesse facilmente resolver esse problema por outros meios como simplesmente deixando e se comunicar por esse aplicativo.

As outras exposições confirmaram essas primeiras argumentações de uma forma ou de outra com pensamentos pontuais como a do Alberto Ribeiro, da Associação dos Magistrados do Brasileiros, que fortaleceu a ideia de que não pode existir um espaço que fuja da jurisdição estatal.

Basicamente, portanto, podemos perceber a formação de duas linhas argumentativas na audiência pública. Uma que diz inviável tecnicamente colocar um acesso excepcional ao WhatsApp (formada pelo WhatsApp, Professor Anderson Nascimento, Professor Marcos Simplício, ASSEPRO NACIONAL, LAPIN, CTS e CCSLUSP) e outro grupo que diz ser possível algum tipo de acesso excepcional à criptografia do WhatsApp (Polícia Federal, Ministério Público Federal, Insper, Conselho Federal da OAB, IASP, CFOAB, MCTIC e FEBRATEL).

E, numa espécie de linha cinzenta, ficam aqueles que entendem que pode ser possível um acesso excepcional, mas não seria recomendável dada a fragilização da criptografia se houvesse tal acesso excepcional.

A audiência pública foi de enorme importância pois deixou a entender que o grande problema é de fato a criptografia, que a maioria pensa que existem formas de burlar essa criptografia, porém que isso não seria adequado e que há de fato um conflito escancarado entre a busca pela segurança pública e a defesa da privacidade. Devemos notar que as ações de controle de constitucionalidade orbitam ao redor de casos extremos como o do bloqueio de uso do aplicativo WhatsApp em caso de descumprimento de ordem judicial, quando na verdade o nosso ponto focal do presente trabalho é bem mais sutil, pois trata da posição da criptografia no confronto entre o direito à privacidade e o direito à segurança pública.

5. CONSIDERAÇÕES FINAIS E CONCLUSÃO

Diante da construção feita até agora, podemos chegar a algumas conclusões. Primeiro, diante da contextualização histórica podemos ver os dois Direitos em conflito e perceber que o Direito à Privacidade sofreu muito mais mudanças com o passar dos anos, o pensamento liberal moldou o conceito de privacidade para que se adequasse a uma perspectiva mais fechada e o advento da internet pareceu esgarçar um pouco esse conceito em virtude de variáveis que se sobrepuseram à privacidade em determinados casos, porém sempre com o usuário sobre controle dos limites dessa privacidade (quando consciente dela). Como vimos e ensina Bauman, a modernidade líquida (e a Sociedade da Informação) são intimamente ligadas ao consumo, portanto em muitos pontos o consumo, a vontade rápida de possuir se sobrepõe à privacidade. Podemos dar um exemplo do uso diário da internet em que concordamos em ceder dados pessoais para que se possa ter acesso a certas páginas de internet “gratuitas” ou aplicativos “gratuitos”. Um exemplo que se adequa bem ao estudo que se empreende aqui é o caso do telefone. Antes da popularização do WhatsApp não se permitia que uma outra pessoa tivesse acesso ao seu número de telefone. Hoje, para termos possibilidade de uso do aplicativo devemos nos inscrever com o nosso número de telefone que fica acessível a todos que fazem parte de determinado grupo. Inclusive pedimos para nos adicionar cedendo a estranhos o nosso número de telefone com uma tranquilidade que não tínhamos antes.

Outro apêndice do Direito à Privacidade, que não foi aprofundado no presente trabalho pois não era esse o escopo, mas foi utilizado como comprovação da hipótese de mudança drástica operada nos Direitos da Personalidade por força da internet é o Direito ao Esquecimento, um direito umbilicalmente vinculado à Sociedade da Informação visto que a velocidade e potencialização da informação fez surgir um dano à privacidade cada vez mais comum. E também fez surgir novos conflitos, como em face ao Direito à

Informação que também sofreu uma hipertrofia nessa nossa sociedade a medida que o Direito à Privacidade foi mitigado pela vontade do próprio cidadão.

A Sociedade da Informação projeta uma sobra também na questão da segurança pública, na medida que a vivemos em muito mais segurança do que gerações anteriores em decorrência dos avanços tecnológicos. Pululam câmeras de vigilância, o sistema de segurança pública é muito mais eficiente e, no entanto, vivemos com muito mais medo do que qualquer geração anterior, de acordo com Bauman. Anna Milton, citada por Bauman responde dizendo que a necessidade de segurança se torna um vício. Quanto mais seguro estamos, mais seguros precisamos nos sentir. O Estado provedor da segurança pública perde espaço dia a dia e nisso Castells e Bauman convergem. O primeiro em sua nova obra "Ruptura" atenta que o Estado foi se desmantelando a ponto de não conseguir mais prover as necessidades da população, não detém mais controle sobre muitos aspectos da vida comunitária, sobretudo quando levamos em conta que "vida comunitária" agora abrange também o meio ambiente digital que, conforme aponta Bauman, está além do Estado, que tem que encontrar soluções globais com poderes locais.

Conforme a pesquisa aponta, a questão da segurança pública e do Direito à Segurança Pública são direitos fundamentais sociais que não são enfrentados de maneira adequada frente aos novos desafios da Sociedade da Informação. Essa pesquisa demonstrou que o conceito de segurança pública mudou menos do que o conceito de privacidade e as mudanças, em especial com o advento da Constituição Federal de 1988, se deram quase que totalmente no campo da formatação hierárquica. A Constituição Federal pouco fala sobre Segurança Pública como objeto e sim, e sim como construção da corporação. Deixa para normas infraconstitucionais a obrigação de cuidar da segurança pública. Porém, pode-se adiantar, de acordo com a pesquisa entabulada, que a segurança e ordem pública são pilares da nossa sociedade, um dos "sólidos" de Bauman.

A pesquisa tratou de pavimentar alguns conceitos para melhor percepção do problema e, entre esses conceitos, a questão da internet como revolução

digital é primordial. Todos os conceitos de privacidade, segurança e até mesmo do próprio Homem se modificaram frente a criação da internet. Ironicamente, a internet surgiu como uma resposta à busca pela segurança e hegemonia nos tempos da Guerra Fria. Surge como um sistema de proteção em face a ataque nuclear soviético e torna-se, em relativamente pouco tempo, um símbolo liberal. Ou seja, surge como um ato do Estado e gradativamente se destaca deste e torna-se um ente autônomo (até certo ponto). Hoje, ironicamente, temos o Estado tentando recuperar o terreno perdido e interferir na sua criação. A criatura volta-se contra o criador, num conflito quase edipiano, a Internet procura matar seu pai (Estado) e casar-se com sua mãe (cidadãos / usuários).

Diante desse quadro surge a necessidade do cidadão se proteger do Estado, e o faz no campo da privacidade com o uso de ferramentas como da criptografia.

A internet e a Sociedade da Informação forçam o cidadão a se reinventar, no sentido de que ele não pode mais esperar pelo Estado como provedor de certos Direitos e, portanto, acaba utilizando a própria rede mundial como provedora de direitos. Ele alija o Estado em virtude de outros novos direitos que surgem, como o direito ao acesso privado a dados. Mas aqui há um problema. O Estado ainda é o guardião da segurança e ordem pública e a internet é algo amorfa, anárquica e, muitas vezes, perigosa. Aqui temos o conflito entre a vontade do usuário de ser completamente independente em sua cidadania digital, sem que o Estado o observe e a necessidade de intervenção Estatal na proteção de casos concretos. Nada muito diferente do mundo real, não digital, porém com uma diferença básica da liquidez e dinamismo do ambiente digital. A sensação de segurança no ambiente digital é muito grande (para a maioria dos leigos) e é contrária a sensação de segurança no mundo real em que geralmente esse sentimento é menor. Conforme dito, o medo no dia-a-dia causa essa insegurança muitas vezes exagerada. Com isso clamamos com muito mais força pela segurança no ambiente real e relevamos o ambiente digital. A consequência é que buscamos uma convalidação de direitos na rede mundial de maneira privada, preferimos colocar nosso Direito à Privacidade nas mãos da criptografia, por

exemplo, embora não se saiba como funciona. É claro, o cidadão exige que o Estado interfira na medida da manutenção dos direitos privados da coletividade, opondo-se, em geral, a interferência estatal na rede que macule isso, ainda que seja para preservar outros direitos (com exceção, é claro, do caso particular de afronta a um direito do próprio cidadão). É como se o cidadão digital ficasse alienado diante do dinamismo e das inúmeras ofertas da rede mundial, anestesiado e egoísta, requer apenas um Estado ausente da sua ambientação digital. Não se pode culpar totalmente o cidadão. Bauman o faz com reservas, conforme se destacou na pesquisa, ao afirmar que o cidadão digital sacrifica sua privacidade em troca desses benefícios da rede mundial, mas ressalva que muitas vezes ele não tem escolha.

Além disso, o Estado historicamente oprime o cidadão. É natural que haja grande desconfiança em relação ao Estado nesse ponto. Basta lembrar, ainda no campo da privacidade, que o Estados Unidos da América é sempre acusado de espionagem digital. O *Patriot Act* e, posteriormente o *Freedom Act*, permitem uma série de intervenções na esfera privada do cidadão Norte-Americano a pretexto de combater o terrorismo. A desconfiança em relação ao Estado aumenta proporcionalmente em relação ao aumento da vivência digital, sem fronteiras.

A criptografia surge, também primeiramente como uma ferramenta de guerra e torna-se no mundo moderno uma ferramenta para afastar o Estado da vida privada, conforme foi visto.

Com a disseminação da internet, a criptografia tornou-se uma ferramenta de controle da privacidade do usuário, reconhecida até pela legislação estatal.

Em vários dispositivos legais, como visto na pesquisa, a criptografia é considerada como uma forma de efetivação do Direito à Privacidade. Ela é prevista em lei e até mesmo requisitada como uma das formas de garantir que o outro tenha acesso a seus dados privados.

Com isso podemos concluir que a criptografia é entendida até pelo Estado como uma aliada na efetivação de Direitos.

Nesse ponto, podemos estender a conclusão para a questão da criptografia especificamente na questão dos aplicativos de mensagens instantâneas.

A presente pesquisa analisou os conceitos de mobilidade na comunicação e os aplicativos de mensagens instantâneas concluindo que: 1) o uso de smartphones com esses aplicativos está disseminado entre os brasileiros; 2) Como se tornaram um meio de comunicação muito difundido, a proteção nos dados privados é um requisito de qualidade desses aplicativos.

A disseminação do uso de aplicativos de mensagens instantâneas no Brasil é assombrosa. É tão comum que hoje não praticamente podemos dizer que um smartphone é um apêndice desses aplicativos. Há muito mais comunicação via aplicativos desse tipo do que qualquer outro tipo de comunicação telefônica, conforme pesquisa apontou. Usuários utilizam esses aplicativos constantemente para troca de mensagens, fotos, textos, etc...

A mobilidade comunicacional mudou a forma como vivemos hoje, em especial em grandes centros urbanos. O fato de se ter um smartphone com acesso à internet nos levou a uma conexão muito maior com grupos de pessoas inteiros.

Esse trabalho constatou que esses aplicativos estão completamente inseridos na vida cotidiana do brasileiro a ponto de até mesmo a nossa legislação prever a possibilidade de uso desses aplicativos para uso oficial como intimação, conforme foi citado na decisão liminar sobre o bloqueio do WhatsApp pelo Ministro Ricardo Lewandowski.

Outro ponto levantado pela pesquisa foi que dentre os diversos aplicativos de mensagens instantâneas, o WhatsApp é, de longe, o mais popular no Brasil, seguido pelo Facebook Messenger e o Telegram. O Facebook Messenger deve sua popularidade ao fato de ser vinculado diretamente a uma rede mundial, enquanto o Telegram tornou-se popular após os bloqueios judiciais de uso do WhatsApp. Com isso os problemas judiciais relativos a conflitos entre privacidade, direito à livre expressão e a segurança pública foram focados no WhatsApp no Brasil.

A criptografia propriamente dita foi estudada de maneira rápida nos aplicativos propriamente ditos, mas suficiente para que se pudesse compreender a forma como se dá essa proteção, suas virtudes e debilidades e, com isso o trabalho foi enriquecido no sentido de se compreender melhor as limitações existentes em face de pedidos de decriptação e interceptação de mensagens.

De acordo com as decisões trazidas à pesquisa bem como o levantamento bibliográfico sobre o assunto e, principalmente, as audiências públicas nos casos de controle concentrado de constitucionalidade, a criptografia do WhatsApp é bastante segura e parte dessa segurança se deve ao fato de não haver possibilidade de um acesso excepcional, ou seja, embora em tese se possa modificar o protocolo para que se possa interceptar mensagens, isso além de ser inútil pois informaria os comunicantes de que alguém está espreitando, abriria uma porta para invasões. Claro que essa opinião não é unânime, mas pareceu na pesquisa a mais bem embasada e popular entre os especialistas da área.

Restam, portanto, dois pontos que devem ser tratados: um de que qualquer ataque a criptografia em aplicativos de mensagens instantâneas gera uma instabilidade que destrói a confiança as segurança dos dados privados; em segundo lugar há uma forte tendência em não se querer que o Estado tenha acesso a dados privados comunicados nesses aplicativos, por força da desconfiança frente o Estado, confiança corroída em parte por culpa do próprio Estado, em parte pela inserção da ideia liberal que Bauman define como moto da nossa consumerista modernidade líquida.

É claro que, cada caso deve ser tratado de maneira concreta eis que estamos tratando de princípios de Direitos Fundamentais e, portanto, princípios com valores *prima facie.*

E esse foi o problema congênito das decisões judiciais que bloquearam o uso do WhatsApp. Foram desproporcionais ao ordenar a suspensão do serviço em todo território nacional, afetando mais de 100 milhões de brasileiros que se acostumaram (a alguns até dependiam) da comunicação via WhatsApp. Não me

recordo de uma decisão judicial de primeira instância que tenha afetado tantas pessoas ao mesmo tempo como essa.

Todas as decisões que cassaram as ordens de bloqueio utilizaram da argumentação da desproporcionalidade, que salta aos olhos e tergiversaram sobre o foco do problema.

O enfrentamento do problema, se o Estado deve ou não ter acesso às conversas privadas nos aplicativos de mensagens instantâneas no intuito de garantir a segurança pública, quebrando a criptografia de alguma forma, não foi enfrentado, porém algumas conclusões podem ser feitas.

O moto do presente trabalho é justamente investigar, dada as premissas básicas pesquisadas, a resposta que pareça mais adequada. Nesse ponto, pode-se ter ideia da natureza principiológica dos direitos fundamentais em conflito, conforme ensina Robert Alexy. Dessa forma, já afastamos soluções gerais como as do bloqueio geral do WhatsApp eis que há uma clara desproporcionalidade e também, a nosso ver, uma tendência de tratar como regra aquilo que é princípio, sem observar devidamente o caso concreto.

Note-se que a utilização da ponderação nos termos de Robert Alexy pareceu a mais adequada do ponto de vista metodológico pois a forma como o autor trabalha os conflitos no caso concreto, ponderando e valorando é compatível com a ideia de dinamismo da Sociedade da Informação e da modernidade líquida baumaniana, além de ser provavelmente uma das teorias mais populares no que tange a solução de conflitos entre princípios.

Em geral, o problema da quebra da criptografia dos aplicativos de mensagens instantâneas a fim de preservar a segurança pública pode ser resolvido utilizando-se a proporcionalidade ou ponderação de Alexy.

Temos dessa forma dois princípios fundamentais em conflito, levando-se em conta o caso concreto, como por exemplo o caso do uso do WhatsApp para comunicação entre membros de facções criminosas: A privacidade de todos os usuários do WhatsApp, protegida pela criptografia de ponta-a-ponta assimétrica e

a obrigação do Estado em proteger todos os cidadãos, oferecendo segurança pública e procedendo a persecução criminal desses membros de grupos criminosos.

A primeira premissa, de que todos os usuários do WhatsApp são protegidos pela criptografia ponta-a-ponta parece ser verdadeira de acordo com a pesquisa, assim como parece ser verdadeira a afirmativa de que a intervenção no protocolo de criptografia ou outro tipo de intervenção como o ataque do homem do meio causaria uma vulnerabilidade que comprometeria a privacidade de todos os usuários do WhatsApp. Ainda é verdadeira, como se viu, a premissa de que o WhatsApp não criptografa os metadados, apenas o conteúdo das conversas. Por outro lado, também é verdadeira a premissa de que o Estado precisa ter acesso às conversas ou, ao menos interceptar essas conversas para que se possas proceder com mais facilidade à persecução criminal, fazendo provas com o intuito e impedir que o a segurança pública seja violada. Não há, até hoje, espaço em que o Estado não possa atuar para garantir a Segurança Pública, sua obrigação constitucional.

Dessa forma, pode-se passar para uma análise sob o ponto de vista da proporcionalidade ou ponderação nos conflitos entre essas duas normas-princípios.

De acordo com a teoria da proporcionalidade o devemos examinar a adequação, a necessidade e a proporcionalidade propriamente dita (ponderação). E para tanto vamos utilizar como exemplo o princípio da Segurança Pública com prevalência sobre o Direito a Privacidade, como se o Estado pudesse quebrar a criptografia do WhatsApp para conseguir chegar a sua finalidade conseguir provas a fim de dar prosseguimento à persecução criminal (pode-se imaginar o caso real em que o Estado requisitou a interceptação das comunicações do WhatsApp para agir contra criminosos organizados).

No caso da adequação, dependendo do caso concreto variará a carga axiológica dos princípios em conflito, porém, *ab initio,* se usarmos o exemplo

acima, parece ser adequado o Estado requerer a quebra da criptografia para se garantir a segurança pública.

Passando ao segundo crivo, da necessidade a questão começa a se modificar. Se antes questionamos apenas a adequação, agora confrontamos os dois princípios questionando se há realmente a necessidade de se afastar um princípio em detrimento de outro. No exemplo utilizado, existem garantias de que é possível se proceder à persecução criminal sem que se tenha acesso ao conteúdo das mensagens, mas aos metadados, que não são criptografados. É claro que a interceptação do teor das mensagens seria muito mais útil para a Segurança Pública, porém o próprio princípio da defesa da Segurança Pública no caso concreto não é afastado totalmente. Porém, a quebra da criptografia por parte do Estado nesse caso também não pulveriza o Direito à Privacidade, apenas o mitiga. Esse mais apurado pode ser feito na terceira fase dessa ponderação.

Na proporcionalidade propriamente dita temos que quanto maior a invalidação de certo princípio, maior deverá ser a validação do outro princípio. E aqui nesse ponto é onde chegamos a uma conclusão mais profunda sobre o problema.

Se o pedido do Estado para que o WhatsApp fornecesse alguma forma de quebrar a criptografia fosse aceito (e possível), a insatisfação com a quebra da privacidade, em tese, de milhões de brasileiros, seria desproporcional à satisfação estatal em conseguir continuar a persecução criminal por esse meio.

Notemos que uma vez quebrada a criptografia, uma enorme gama de possibilidades se abre. A insegurança do sistema protetivo da criptografia poderia abrir a possibilidade para que hackers obtivessem dados privados, como ocorreu em casos com o do iCloud da Apple entre outros.

Por outro lado, se dermos prevalência ao Direito à Privacidade em detrimento ao da Segurança pública no caso concreto (ou seja, negar a quebra da criptografia para a interceptação de conversas entre membros do crime

organizado) claramente a insatisfação do último não será tão grande quanto a satisfação do primeiro.

Note-se que essa pesquisa leva em conta os dados disponíveis levantados, como o fato de que se houver uma violação da criptografia haverá séria falha de segurança, de que os metadados são uma ferramenta, ainda que menos eficientes, de efetivação da investigação e de que, de fato, não há possibilidade de se proceder a essa quebra da criptografia sem que haja um desmoronamento do sistema privado de proteção à privacidade dos usuários.

Dessa feita, a pesquisa demonstra, se utilizarmos a ponderação nesse caso concreto, que não seria satisfatória a quebra da criptografia para que o Estado pudesse proceder à sua função em relação à Segurança Pública, em especial por existirem outros meios disponíveis para que seja efetivado esse dever constitucional.

Existem outros pontos também que devem ser levados em conta, como a possível inutilidade de se romper com as defesas criptográficas eis que, ainda que se faça em relação, digamos, ao WhatsApp, outros aplicativos surgirão, nem que seja na Deep Web.

Do ponto de vista da possibilidade técnica, a audiência pública comprovou que apenas poucas formas seriam possíveis, como o ataque do homem do meio, pois existe uma limitação jurisdicional brasileira e tal ordem serviria apenas no território brasileiro o que criaria um impasse técnico na comunicação entre usuários brasileiros e estrangeiros. Haveria uma segregação dos usuários do WhatsApp brasileiro, senão um corte de comunicação.

Com isso pode-se afirmar que a criptografia nos aplicativos de mensagens instantâneas cumpre um papel de defesa do direito fundamental à privacidade e se adequa a esses novos tempos em que novas formas de se viver, agir e comunicar surgem na esteira da Sociedade da Informação, criando novas relações entre as pessoas e entre as pessoas e o Estado. Novos paradigmas são formados, a informação passa a ter uma importância cada vez maior em nossas vidas e o Estado deve entender que surgem novos espaços que, muitas vezes

serão impermeáveis, seja por uma questão técnica, seja por uma questão social, seja por uma questão jurídica.

Isso não quer dizer que o Estado deva se afastar de sua função de cumprir com sua obrigação positiva de, no caso, fornecer segurança e ordem pública, mas que existem espaços privados que o Estado não pode automaticamente romper. Com todo respeito ao Professor Tércio Sampaio, o problema não é que há um espaço em que o Estado não pode entrar, o problema é para quê o Estado quer entrar, se há outras formas do Estado atuar para atingir a mesma finalidade. Esse buraco negro de intervenção estatal não é propriamente ruim enquanto houver outras formas de se chegar a resultados semelhantes. Não é um mal em si pois o Estado tem como objetivo o bem comum, que muitas vezes, como os Direitos Humanos de primeira dimensão nos ensinou, passa pelo afastamento do Estado.

A modernidade líquida é uma realidade, gostemos ou não e o espírito dela é liberal. A privacidade hoje detém um status especial a ponto de termos várias legislações que tratam desse aspecto na rede mundial de computadores, conforme observamos no trabalho. A tendência é a valorização do espaço privado, um refluxo da ideia inicial baumaniana de sacrifício da privacidade para benefícios do mundo digital. Hoje os usuários estão cada vez mais conscientes dessa “barganha” e o sinal disso são as leis protetivas da privacidade de dados mencionadas há pouco. Há uma estabilização legislativa no sentido de proteger cada vez mais o “eu” digital frente a sanha e fome de terceiros, inclusive o Estado em se imiscuir da vida digital privada do indivíduo.

REFERÊNCIAS BIBLIOGRÁFICAS E ELETRÔNICAS

ALEXY, Robert. *El concepto y la validez del derecho***.** 2. ed. Barcelona: Gedisa, 1997

_____. *Teoria dos direitos fundamentais*. 5. Ed. São Paulo: Malheiros Edi

_____. *Direitos Fundamentais, Balanceamento e Racionalidade.* Ratio Juris. Vol. 16, n. 2, 2003

ANTUNES, Igor; KOWADA, Luis Antonio*. Explorando o Sistema de Criptografia Signal no WhatsApp*. Niterói: Instituto de Computação – Universidade Federal Fluminense, 2018. Disponível em: <http://portaldeconteudo.sbc.org.br/index.php/sbseg/article/view/4252/4183>. Acesso em 15 nov 2018.

ARENDT, Hannah. *A condição humana*. Trad. Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2008.

ASCENÇÃO, José de Oliveira. *Direito da Internet e da sociedade da informação*. Rio de Janeiro: Forense, 2002.

BARRETO JUNIOR, Irineu Francisco; LIMA, Marco Antonio*. Marco Civil da Internet: Análise das Decisões Judiciais que suspenderam o Aplicativo Whatsapp no Brasil–2015-16*. Revista de Direito, Governança e Novas Tecnologias, 2016, 2.2: 37-52. Disponível em: < http://indexlaw.org/index.php/revistadgnt/article/view/1484>. Acessado em 15 set. 2018.

BASTOS, Celso Ribeiro. *Hermenêutica e interpretação constitucional. São Paulo*: C. Bastos. 1997.

BAUMAN, Zygmunt. *A riqueza de poucos beneficia todos nós?*. Rio de Janeiro: Jorge Zahar, 2013

_____. *Modernidade líquida*. Rio de Janeiro: Jorge Zahar Ed., 2001.

_____. *Vida líquida*. Rio de Janeiro: Jorge Zahar 2ª Ed., 2005

_____. *Vigilância líquida: diálogos com David Lyon/Zygmunt Bauman*. Rio de Janeiro: Zahar, 2013

BITTAR, Carlos Alberto*. Os direitos da personalidade*. 6. ed. Rio de Janeiro: Forense Universitária, 2003.

BOBBIO, Norberto. A Era dos Direitos. Rio de Janeiro: Campus, 1992.

BOBBIO, Norberto, et. al. Dicionário de Política. Tradução de Carmem C. Varialle et al. 5a. edição. Brasília: Editora Universidade de Brasília, 2004

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: Titulo V, Da Defesa do Estado e das Instituições Democráticas. Capítulo III da Segurança Pública. Disponível em: <http://www.stf.jus.br/portal/constituicao/artigobd.asp?item=%201359>. Acesso em 20 jan de 2016

BRASIL. Lei Ordinária no 9.882, de 3 de dezembro de 1999. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9882.htm >. Acesso em: 10 out 2018

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403/SE – Sergipe. Relator: Edson Fachin. Pesquisa de Andamento Processual, Decisão Liminar. 2016a. Disponível em: < http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4975500 >. Acesso em: 20 jan. 2017

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403/SE – Sergipe. Relator: Edson Fachin. Audiência Pública. 2016b. Disponível em: < http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf>. Acesso em: 20 jan. 2017

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 4815/DF – Distrito Federal. Relator: Carmem Lúcia. 2015a. Disponível em:

<http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=4815&processo=4815>. Acesso em: 20 jan. 2017

BRASIL. Tribunal de Justiça do Rio de Janeiro. Apelação Cível 0122463-44.1997.8.19.0001/RJ– Rio de Janeiro. Relator: Des. Leila Mariano. 1997. Disponível em: <http://www4.tjrj.jus.br/ejud/ConsultaProcesso.aspx?N=200000122727>. Acesso em: 20 jan. 2017

BRASIL. Tribunal de Justiça de São Paulo. Mandado de Segurança 2271462-77.2015.8.26.0000/SBC – São Paulo. Relator: Des. Xavier de Souza. 2015b. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/wp-content/uploads/sites/41/2015/12/MS-2271462.pdf>. Acesso em: 20 jan. 2017

BRASIL, Tribunal de Justiça de Sergipe. Vara Criminal de Lagarto. Ação Penal _ Procedimento Ordinário nº 201655000183: Juíz: Marcel Maia Montalvão. Pesquisa de Andamento Processual, Decisão Liminar, 2016a. Disponível em: < http:// http://www.tjse.jus.br/portal/consultas/consulta-processual >. Acesso em: 20 jan. 2017

BRUIN, Nicholas.*The Evolution of Instant Messaging***.** 2018. Disponível em: < https://www.researchgate.net/profile/Nicholas_Bruin/publication/325411833_The_Evolution_of_Instant_Messaging/links/5b0cabd0a6fdcc8c253659e8/The-Evolution-of-Instant-Messaging.pdf> . Acessado em 19 out 2018.

CANOTILHO, Joaquim José Gomes. *Direito constitucional e teoria da constituição*. 7 ed. Coimbra : Almedina, 2010.

CASTELLS, Manuel. *A Era da Informação: Economia, Sociedade e Cultura. Fim do Milênio*. v.3, São Paulo: Paz e Terra, 2012.

CASTELLS, Manuel*. Compreender a Transformação Social.* Conferência de 4 e 5 de Março de 2005, em Portugal-Lisboa, sobre o título: Sociedade em Rede: do Conhecimento à Acção Política, organizado por Manuel Castells e Gustavo Cardoso.

CASTELLS, Manuel. A sociedade em rede. 8. ed. rev. ampl. São Paulo: Paz e Terra, 2005.

_____ A galáxia internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003

_____ Ruptura – A Crise da democracia liberal. Rio de Janeiro: Jorge Zahar, 2017

CORBATÓ, Fernando José et al. *The Compatible Time-Sharing System - A Programmer's Guide*. Cambridge, MA: The M.I.T. Press, 1963.

COSTA, Célia Maria Leite. *Intimidade versus interesse público: a problemática dos arquivos*. In: Revista Estudos Históricos, Rio de Janeiro, v. 11, n. 21, p. 189-200, jul. 1998. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/reh/article/view/2066/1205>. Acesso em: 17 Mar. 2018.

COUNCIL OF EUROPEAN UNION INTERINSTITUTIONAL FILE*. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Disponível em <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>. Acessado em 02/12/2017.

DINIZ, Maria Helena**. Código Civil Anotado,** 13ª Edição, São Paulo: Saraiva, 2008.

DINIZ, Maria Helena in FIUZA, Ricardo (coords.). **Novo Código Civil Comentado**. 5 ed. São Paulo, SP: Saraiva, 2006.

DONEDA, Danilo. ***Da privacidade à proteção dos dados pessoais***. Rio de Janeiro: Renovar, 2006.

DUROV, Pavel. *"The encryption of Signal (=WhatsApp, FB) was funded by the US Government. I predict a backdoor will be found there within 5 years from now".* Paris, 8 jun 2017. Twitter: @durov. Disponível em

<https://twitter.com/durov/status/872891017418113024>. Acesso em: 10 out 2018.

DWORKIN, Richard Myles. **É o direito um sistema de regras?**. Estudos Jurídicos, São Leopoldo, RS , v.34, n.92 , set./dez. 2001.

_____ *Levando os direitos a sério*. São Paulo: Martins Fontes, 2002.

FARIAS, Edilsom Pereira de. *Colisão de Direitos – A Honra, A Intimidade, A Vida Privada e a Imagem versus A Liberdade de Expressão e Informação*. 2ª ed. Porto Alegre: Ségio Antonio Fabris Editor, 2000

FAURE, Antoine; SANTOS, Marcelo. *Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption***.** Social Media+ Society. 2018. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/2056305118795876>. Acesso em: 15 nov 2018

FERRAZ JUNIOR, Tércio Sampaio et al. *O Desafio do WhatsApp ao Leviatã*, Folha de São Paulo, 16 ago. 2016. Disponível em: <http://www1.folha.uol.com.br/opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml>. Acesso em: 20 jan. 2017.

FERREIRA FILHO, Manoel Gonçalves. *Direitos humanos fundamentais*. 12 ed. rev. e atual. São Paulo : Saraiva, 2010.

FIORILLO, Celso Antonio Pacheco. *O marco civil da Internet e o meio ambiente digital na sociedade da informação*. São Paulo:Saraiva, 2015.

_____. *Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital*. São Paulo: Saraiva, 2015.

GANGULY, Manisha. *WhatsApp design feature means some encrypted messages could be read by third party***.** The Guardian, 2017. Disponível em:

<https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages> . Acesso em: 10 mar 2018.

GAY, Peter. *O século de Schnitzler: A formação da cultura da classe média: 1815 – 1914*, São Paulo: Companhia das Letras, 2002.

HERN, Alex. *May calls again for tech firms to act on encrypted messaging***.** The Guardian, 2018. Disponível em: <https://www.theguardian.com/technology/2018/jan/25/theresa-may-calls-tech-firms-act-encrypted-messaging> . Acesso em: 10 out 2018.

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua) - ACESSO À INTERNET E À TELEVISÃO E POSSE DE TELEFONE MÓVEL CELULAR PARA USO PESSOAL* 2016. Disponível em: <ftp://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_continua/Anual/Acesso_Internet_Televisao_e_Posse_Telefone_Movel_2016/Analise_dos_Resultados.pdf>. Acessado em: 15 nov 2018

KARASZ, Palko. *What Is Telegram, and Why Are Iran and Russia Trying to Ban It?.* The New York Times. 2018. Disponível em: <https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html>. Acesso em: 18 out 2018

KOPLIN, Klaus Cohen**.** *Em caso urgente, intimação pode ser feita por WhatsApp ou aplicativos do tipo*. 2016. In: Revista Consultor Jurídico Disponível em: <http://www.conjur.com.br/2016-fev-27/klaus-koplin-urgente-intimacao-feita-whatsapp>. Acesso em: 20 jan. 2017.

LÉVY, Pierre. **A inteligência coletiva. Por uma antropologia do ciberespaço***.* tradução de Luiz Paulo Rouanet., São Paulo, Folha de São Paulo, 2015.

LISBOA. Roberto Senise. **Direito na sociedade da informação**. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/direitonasociedadedainformacao.pdf>. Acesso em: 27 mai. 2018.

MARCACINI, Augusto Tavares Rosa. *Direito e Informática: uma abordagem jurídica sobre a criptografia*, São Paulo, 2010.

MARQUES, Garcia; MARTINS, Lourenço. *Direito da Informática*, 2ª Edição. Coimbra. Almedina, 2006.

MEIRELLES, Hely Lopes. *Direito administrativo brasileiro*. 37 ed. São Paulo: Malheiros, 2011.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet; COELHO, Inocência Mártires. **Curso de direito constitucional**. 9ª ed. São Paulo: Saraiva. 2014.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014.

MOTA, Antonio Marcos de Castro. **ANÁLISE DE SEGURANÇA SOBRE APLICATIVO DE MENSAGEM INSTANTÂNEA**. 22 f. Artigo (Especialização em Perícia Digital) – Universidade Católica de Brasília, Brasília, 2016. Disponível em: < https://core.ac.uk/download/pdf/48130918.pdf>. Acesso em: 2 set. 2018

NETO, Arthur Rezende Alves, et al.. **UFPR UNIVERSIDADE FEDERAL DO PARANÁ DEPARTAMENTO DE MATEMÁTICA PET PROGRAMA DE EDUCAÇÃO TUTORIAL**. Curitiba: Universidade Federal do Paraná, 2014.

PAESANI, Liliana Minardi. **Direito na Sociedade da Informação**. São Paulo: Atlas, 2007

PANORAMA MOBILE TIME/ OPINION BOX. **Mensageria no Brasil em Fevereiro de 2018.** 2018, Disponível em: < https://panoramamobiletime.com.br/pesquisa-mensageria-no-brasil-fevereiro-de-2018/>. Acessado em 15 nov 2018

PINHEIRO, Patricia Peck. Direito Digital: 6. ed. São Paulo: Saraiva, 2016.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 4. ed. São Paulo: Max Limonad, 2000

RODOTÀ, Stefano. (traduzido por: DONEDA, Danilo; MORAES, Maria Celina Bodin) **A Vida na Sociedade da Vigilância: A privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SANTOS, Dayane Silva dos. **Uso da criptografia como motivação para o ensino básico de matemátic***a.* 2016. 63 fls. Dissertação (Mestrado Profissional em MATEMÁTICA) – Programa de Pós-Graduação em MATEMÁTICA da Universidade Federal de Sergipe, Sergipe, 2016

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**. 6ª Edição, ver., atual. E ampliada. Porto Alegre: Editora Livraria do Advogado, 2006.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2ª Edição, Rio de Janeiro : Editora Lumen Juris, 2006,

SCHREIBER, Anderson*.* **Direitos da Personalidade: Revista e atualizada**. 3 ª Ed. São Paulo: Atlas, 2014

SILVA, José Afonso, *Curso de Direito Constitucional Positivo*, Malheiros Editores,9º edição 4º tiragem, 1994, São Paulo-SP.

_____. **Aplicabilidade das Normas Constitucionais***;* 8ª Edição, São Paulo: Malheiros, 2012

SILVEIRA, Alexandre Borba da. **Atitudes e intenções de adoção de internet móvel: uma análise do comportamento do consumidor jovem adulto**. 2012. 185 f. Dissertação (Mestrado em Administração) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2012. Disponível em: < https://core.ac.uk/download/pdf/48130918.pdf>. Acesso em: 2 set. 2018.

SIQUEIRA JÚNIOR, Paulo Hamilton. **Direitos humanos e cidadania digital**. In: DE LUCCA, Newton. SIMÃO FILHO, Adalberto. LIMA, Cíntia Rosa Pereira de (coords.). Direito & Internet III - Tomo I: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

STATISTA – THE STATISTICS PORTAL. **Most popular mobile messaging apps worldwide as of October 2018, based on number of monthly active**

users (in millions). 2018. Disponível em: < https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>. Acessado em: 21 nov 2018

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 1993

VAN VLECK, Tom. **The History of Electronic Mail**. 2001. Disponível em: < https://www.multicians.org/thvv/mail-history.html>. Acessado em: 20 set 2018

_____. **The IBM 7094 and CTSS**. 1995. Disponível em: < https://multicians.org/thvv/7094.html>. Acessado em: 20 set 2018

VASCONCELLOS, Eliane. **Intimidade das confidências**. Teresa: revista de literatura brasileira 8/9. Departamento de Letras Clássicas e Vernáculas, Faculdade de Filosofia, Letras e Ciências Humanas, USP. São Paulo, 2008. Disponível em: <http://www.revistas.usp.br/teresa/article/view/116762>, Acesso em :10 de mai. 2018.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, v. IV, n. 5, 1890. Disponível em: < http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf >. Acesso em: 20 jan. 2017.

WHATSAPP. **End-to-End encryption**. 2018. Disponível em: https://faq.whatsapp.com/en/android/28030015/. Acesso em 15 nov 2018

WYKES, Sean Michael, **Criptografia Essencial: A Jornada do criptógrafo**. Rio de Janeiro: Elsevier, 2016