Fronteiras Interdisciplinares do Direito
Interdisciplinary Boundaries of Law V1 N.1 2019

PROTEÇÃO E TRATAMENTO DE DADOS SOB O PRISMA DA LEGISLAÇÃO VIGENTE

CAROLINA DA SILVA LEME
ADVOGADA CRIMINALISTA. MESTRANDA EM DIREITO PENAL; ESPECIALISTA EM CORRUPÇÃO, CRIME ORGANIZADO E TERRORISMO, EM PROCESSO PENAL E CRIMES ECONÔMICOS E EM DIREITO PENAL ECONÔMICO.

RESUMO: O presente estudo tem como objetivo analisar os dados coletados pelos principais serviços de aplicação de internet à luz das legislações de proteção à dados pessoais. Partindo de análise histórica do surgimento da internet e das gerações de leis de proteção de dados, passaremos à análise do Marco Civil da Internet e da Lei Geral de Proteção de Dados (ainda não em vigor), bem como de seus alcances e efetiva proteção aos titulares de dados. Em seguida, passaremos à análise dos principais serviços de aplicação de internet e análise de seus termos de uso, concluindo pela ampla coleta de dados por mencionados serviços e a necessidade de aprofundamento legislativo no tocante ao processamento e compartilhamento de referidos dados.

PALAVRAS-CHAVE: PROTEÇÃO DE DADOS. INTERNET. MARCO CIVIL. PRIVACIDADE. LEI GERAL DE PROTEÇÃO DE DADOS.

PROTECTING AND PROCESSING DATA IN ACCORDANCE WITH BRAZILIAN LAW

ABSTRACT The objective of present study was to analyze the data collected by internet applications companies in the light of Brazilian data. Departing from a historic contextualization of internet and data protection generations, we intended to analyze the Internet Act and Brazilian Data Protection Law (which is not yet in effect), in order to verify if they are effective regarding user's protection. After that, we analyzed which data is collected and processed by the most famous internet application companies and we intended to conclude that a lot of sensitive data is shared between those companies and the need for deepening of legislation regarding the processing and sharing of such data.

KEYWORDS: DATA PROTECTION. INTERNET. INTERNET ACT. PRIVACY. BRAZILIAN DATA PROTECTION LAW.

I – BREVE HISTÓRICO DA INTERNET:

A Internet tem seu nascedouro atrelado à Guerra Fria, quando blocos militares capitaneados pelos Estados Unidos da América, temendo que um ataque destruísse seus meios de comunicação, iniciaram estudos acerca da criação de novos meios descentralizados de armazenamento de dados e

comunicação, evitando, desta forma, que apenas um ataque acarretasse a perda de todas as informações sigilosas e impossibilitasse a comunicação (MOSCHOVITOS, 1999. p. 11/14).

A primeira comunicação online, contudo, se deu em contexto acadêmico, quando o primeiro e-mail foi enviado de um professor da Universidade da Califórnia para um professor da Universidade de Stanford, datado de outubro de 1969[1]. Nas duas décadas que se seguiram, a internet permaneceu restrita ao meio acadêmico, consistindo em importante ferramenta de comunicação entre discentes e docentes, não havendo, contudo, grandes avanços em suas ferramentas ou alcance.

No início da década de 1990, Tim Berners-Lee, engenheiro inglês, criou o protocolo World Wilde Web (WWW), permitindo a criação dos websites com interações gráficas[2] e, em seguida, foram criados os navegadores, como o Windows Explorer da Microsoft e o Netscape, culminando a acelerada expansão da internet e seu alcance à população geral.

Na segunda metade da década de 90 temos o surgimento das diversas ferramentas que alteraram definitivamente a forma de realizarmos pesquisas acadêmicas, ouvirmos músicas, armazenarmos dados e nos comunicarmos, fazendo parte dessa revolução empresas como Google[3], Yahoo[4], Napster[5], ICQ[6] e Messenger[7].

Conforme evidenciado acima, a internet teve vertiginoso crescimento desde a sua criação. Contudo, não obstante os avanços com ela trazidos, importa destacar que a produção normativa não acompanhou referido ritmo.

No presente estudo, buscaremos demonstrar a evolução da legislação de proteção de dados no Brasil e quais dados são coletados pelos principais aplicadores de internet utilizados, a fim de analisar de a privacidade encontra-se respaldada pela legislação pátria ou se aperfeiçoamentos deverão ser propostos.

[1] https://cs.stanford.edu/people/eroberts/courses/soco/projects/distributed-computing/html/body_history.html.

[2] "It is to think the internet and the World Wild Web, or web, as the same thing. Sometimes the terms are used interchangeably, or as though one word means as the other. But the web and the Internet are actually very different things. The world wild web is a part of the Internet. The Internet is a huge network of network that connects millions of computers to share information. The web is a way to access that information". (NIVER, 2016. p. 5).

[3] https://www.google.com/about/our-story/

[4] https://www.britannica.com/topic/Yahoo-Inc

[5] https://www.britannica.com/topic/Napster

[6] http://icq-planet.com/the-history-of-icq/

[7] https://www.trutower.com/2013/01/10/microsoft-windows-live-messenger-retrospective/

II – As Gerações de Proteção de Dados:

A preocupação com a proteção de dados remonta ao final do século XIX, contudo seu delineamento passou a ser melhor traçado ao longo das últimas décadas, remontando ao início da internet, dessa forma, à Guerra Fria. Cientes de que os dados dos cidadãos consistem em valiosa informação para seu monitoramento e ordenação[8], e tementes de que a internet pudesse se tornar um meio de opressão à liberdade e privacidade, diversos países dispenderam esforços para criação de um banco de dados unificado, administrados por meio de concessões de autorização (BIONI, 2019, p. 111).

A segunda geração de proteção de dados, por sua vez, ocorre com a extensão da preocupação aos dados privados e à percepção de que o Governo não seria apto a administrar todos os bancos possíveis, de forma que a responsabilidade pela proteção de dados passa a ser de responsabilidade de seus titulares (BIONI, 2019, p. 112).

A transferência da responsabilidade para o titular dos dados traz consigo a terceira geração de proteção de dados, na qual passa a ter papel central o consentimento do indivíduo para coleta e processamento de seus dados (DONEDA, 2006, p. 372), uma vez que diversos serviços como bancários e afins coletavam dados sensíveis de seus clientes, sem informar precisamente de qual forma se daria seu processamento e utilização.

Nessa esteira de preocupação tem início a quarta geração de proteção aos dados, sanando as lacunas legislativas anteriores (BIONI, 2019, p. 113)., a fim de que o titular dos dados tenha ciência inequívoca da forma como seus dados serão coletados, armazenados, processados e compartilhados, fazendo parte dessa geração a Lei brasileira denominada Lei Geral de Proteção de Dados LGPD), analisada no tópico II.3 a seguir.

[8] Nesse sentido: "Em primeiro lugar, foi o Estado que se encontrou na posição de se utilizar largamente de informações pessoais. Os motivos são razoavelmente implícitos: basta verificar que um pressuposto para a administração pública eficiente é o conhecimento tão acurado quanto possível da população, do que decorre, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública, visando maior eficiência". (DONEDA, 2006, p. 8).

III. 1 – LEIS DE PROTEÇÃO DE DADOS NO BRASIL

A primeira proposta de legislação versando sobre atividades realizadas na internet foi realizada no ano de 1999, pelo então Deputado Federal Eduardo Azeredo[9]. O texto proposto, contendo 17 artigos, foi alvo de severas críticas e manifestos, sendo por alguns considerado o AI-5 da internet, em razão das disposições versando sobre atividades cotidianas e a criminalização de diversos atos praticados na internet. Em razão da manifestação contrária ao projeto de lei, este não foi sancionado.

Aos 24 de agosto de 2011 uma nova proposição de lei de regulamentação de dados e segurança da rede mundial de computadores foi apresentada no Congresso Nacional. O Projeto de Lei PL 2160/11[10], o qual inicialmente teve tramitação paulatina.

No ano de 2012, uma famosa atriz da Rede Globo de Televisão, Carolina Dieckmann, teve 36 (trinta e seis) imagens pessoais transferidas para o computador de invasores em uma assistência técnica. Após não ceder à extorsão pretendida, as fotos foram publicadas na internet, causando grande impacto na vida da vítima.

Nesse contexto, aproveitou-se o projeto de Lei 2793/2011 em trâmite na Câmara dos Deputados, tendo sido sancionada a Lei Federal 12.737/2012, a qual alterou o Código Penal Brasileiro, inserindo artigos que punem o cometimento de crimes cibernéticos.

No ano de 2013 um escândalo mundial ganhou a imprensa internacional: Edward Snowden, de apenas 29 anos, teria vazado informações sigilosas dos Estados Unidos da América, fornecendo ao mundo dados da espionagem do governo daquele país sob sua população e inclusive de líderes de Estado, como da então Presidente do Brasil, Dilma Rousseff, valendo-se de servidores de grandes empresas como Apple, Facebook e Google.

As declarações de Snowden acarretaram a sensação de insegurança mundial, culminando na aprovação de leis que preveem a proteção dos dados dos usuários. Foi nesse cenário que o retro mencionado Projeto de Lei 2160/11 foi aprovado na Lei Federal nº 12.965/14, conhecido como

[9]A íntegra da proposta pode ser acessada por intermédio do link: http://imagem.camara.gov.br/Imagem/d/pdf/DCD00199905110008200000.PDF#page=57, fls. 19975.
[10]A íntegra da proposta pode ser acessada por intermédio do link: https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255

"Marco Civil da Internet", o qual será melhor analisado no item II.2 abaixo (LEITE; LEMOS, 2014, p. 1).

Em 2018 um novo escândalo envolvendo a coleta e processamento de dados pessoais por uma empresa chamada *Cambridge Analytica*. Em suma, referida empresa foi acusada pelos jornais *The New York Times* e *The Observer* a utilizar-se de dados coletados de redes sociais para influir em campanhas eleitorais, auxiliando na eleição de Donald Trump à presidência dos Estados Unidos da América.

Os escândalos envolvendo dados pessoais impactou também o cenário legislativo internacional, tendo aos 25 de maio de 2018 entrado em vigor o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Vale destacar que referida legislação tem seu alcance para além das fronteiras do velho continente, vinculando sua aplicação a empresas que possuam filiais em algum dos 28 países da União Europeia ou que ofereçam serviços a pessoas que ali se encontrem. O GDPR prevê ainda requisitos para que haja a transferência internacional de dados entre empresas, nos quais o Brasil inicialmente não cumpriria os requisitos (MONTEIRO, 2018, p. 1).

Dentro desse contexto, aos 14 de agosto de 2018, o Brasil sancionou a Lei Federal nº 17.709/2018, denominada Lei Geral de Proteção de Dados, a qual altera as demais legislações e consolida a proteção de dados no Brasil. Referida Lei Federal sofreu clara influência do GDPR e será melhor analisada no item II.3 a seguir.

III. 2 – O MARCO CIVIL DA INTERNET

O nascedouro do Marco Civil da Internet remonta ao ano de 2011, quando da proposição do Projeto de Lei nº.2.160. Em referido ano a discussão pela privacidade de dados não se encontrava sob holofotes, culminando em paulatina tramitação do projeto. Após vir à tona a divulgação da espionagem de Governos, incluindo a então presidente brasileira Dilma Rousseff por Eduardo Snowden, a temática passou a ser centro de preocupações e, desta forma, amplamente debatida.

Importa destacar que o projeto de lei que deu origem ao Marco Civil da Internet não foi elaborado mediante proposta do Governo, mas sim uma discussão popular antecessora ao escândalo Snowden, a qual visava a debater a forma como seria regulamentada a internet no Brasil. Tangenciando a criminalização de atos praticados na rede, o Marco Civil da Internet teve início como um fórum (www.culturadigital.com/marcocivil), que primeiramente visou à delineação dos

princípios os quais a lei se calcaria, para, em seguida, haver o desenvolvimento do texto legal (LEITE; LEMOS, 2014, p. 5).

Conforme se infere do preâmbulo, o Marco Civil da Internet visa a estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, calcando suas diretrizes na privacidade, na proteção de dados pessoais e na liberdade de expressão dos usuários da rede mundial de computadores, conforme consta de seu artigo 3º (SANTOS; ARAÚJO, 2017. p. 48), tendo sua aplicabilidade limitada às relações entre usuários e provedores de conexão.

Abra-se um parêntesis, a fim de salientar que mencionada Lei Federal foi regulamentada no ano de 2015, por intermédio do Decreto Lei nº. 8771, o qual manteve e complementou as diretrizes de privacidade e liberdade de expressão, sendo possível depreender de seu conteúdo a preocupação com *"uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes*[11]".

Não se pretende no presente estudo o esgotamento da análise do Marco Civil da Internet, mas a sua aplicabilidade prática no tocante aos dados dos usuários dos aplicativos de redes sociais, mensageria e streaming, os mais utilizados pelos usuários brasileiros.

Nesse sentido, o Marco Civil da Internet impõe como obrigação aos aplicadores de internet o fornecimento de dados cadastrais de usuários que acessarem a internet em solo brasileiro[12], bem como os registros de acesso, também conhecidos por "IP Logs", coletados nos 06 meses anteriores ao recebimento da solicitação[13], mediante autorização judicial, salvo casos excepcionais oportunamente abordados.

Importa sublinhar que nem todos os aplicativos coletam dados como "Nome Completo", "RG", "CPF", "Endereço" para o cadastro dos usuários, de modo que o Decreto Regulamentador do Marco Civil facultou os dados coletados, impondo como obrigação a prestação da informação de quais dados são coletados pelo aplicador da internet à autoridade solicitante[14].

[11] **BRASIL.** Marco Civil da Internet. Artigo 13, IV.

[12] "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. **BRASIL.** Marco Civil da Internet. Artigo 11.

[13] O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento". **BRASIL.** Marco Civil da Internet. Artigo 15.

[14] "O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados." **BRASIL.** Decreto Lei nº. 8771/2015.Artigo 11, §1.

No que tange aos registros de acesso, a relevância de mencionado dado relaciona-se com a localização do usuário, já que, uma vez fornecido pelo aplicador de internet, é possível verificar junto à empresa provedora de internet (empresas de telefonia) a localização aproximada do usuário.

No tocante à coleta, armazenamento, tratamento e uso de dados pessoais, o Marco Civil da Internet prevê de maneira genérica a necessidade do consentimento expresso e inequívoco do usuário (GONÇALVES, 2017, p. 95), bem como a necessidade de que todas as informações de uso de dados sejam trazidas de forma clara e completa, sem quaisquer direcionamentos adicionais aos usuários[15].

Em termos práticos, da análise aprofundada da lei ora em estudo extrai-se a necessidade de coleta e armazenamento de duas espécies de dados: dados cadastrais ou de subscrição e os registros de acesso dos usuários[16], os quais deverão ser excluídos no término da relação entre as partes ou expirado o prazo legal.

Ocorre que, conforme a seguir melhor explanado, os aplicativos de redes sociais, mensageria e streaming coletam uma gama expressiva de dados, metadados e conteúdo dos usuários, ausente regulamentação no Marco Civil acerca de seu fornecimento, o que faz com que estudiosos do tema (SANTOS; ARAÚJO, 2017, p. 51) o classifiquem como intransigente, vez que submete o controle total dos dados às empresas prestadoras de serviços de internet, permanecendo o usuário em situação de passividade.

III.3 - A LEI GERAL DE PROTEÇÃO DE DADOS

Após aprovação da Regulamentação Geral de Proteção de Dados (GDPR) pela União Europeia e o escândalo da *Cambridge Analytica*, tornou-se ainda mais latente a necessidade de o Brasil editar legislação de proteção de dados mais aprofundada, visando a nortear a coleta, uso,

[15] "Em relação às informações claras e completas sobre dados de conexão e acesso a provedores de internet, o Marco Civil direcionou-se para uma questão aberta e que não será regulamentada por ele: Lei de proteção de dados pessoais. Quais as informações? Como serão guardadas? Quem são os responsáveis? Como o usuário se empoderará desses direitos? A quem reclamar quando não houver transparência e clareza no uso dos dados? Sem respostas a essas perguntas, o inciso é supérfluo e sem condições de se impor na prática". (GONÇALVES, 2017, p. 22).

[16] Note-se que no tocante ao conteúdo das comunicações há uma clara contradição com o encorajamento à utilização da encriptação como modelo de segurança recomendável, razão pela qual adotaremos no presente estudo o entendimento de que o conteúdo das comunicações privadas deverá ser fornecido uma vez que seja coletado pelo aplicador de internet. Ademais, insta salientar que conteúdo das comunicações não se confunde com interceptação das comunicações, sendo aquele dado estático e este dado produzido em tempo real.

armazenamento e processamento de dados entre entres públicos e privados, bem como se enquadrar no padrão internacionalmente exigido.

A aprovação de uma legislação específica de proteção de dados traz também relação com o intuito de o Brasil pleitear seu ingresso na Organização para a Cooperação e desenvolvimento Econômico (OCDE) (KUJAWSKI; THOMAZ, 2018, p. 1). Isso porque, mencionado órgão traz diretrizes e orientações acerca do tema desde 1980 e, em 2013, as atualizou para adequá-las ao nível de sociedade de informação atual. Embora as orientações da OCDE não tenham força de lei, consistem em requisitos para seu ingresso, sendo essencial para o Brasil a edição de norma mais robusta acerca do tema (MONTEIRO, 2017, p. 6).

Nesse contexto, aos 14 de agosto de 2018 foi sancionada a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), a qual se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", salvo exceções estipuladas em seu artigo 4º.

Antes de adentrarmos as especificidades e inovações da LGPD, importa salientar que a mesma ainda não se encontra em vigor. Conforme previsto em seu último artigo, seu *vacatio legis* será de 24 (vinte e quatro meses), ou seja, no dia 16 de fevereiro de 2020.

O primeiro ponto a ser destacado consiste nas definições de dados pessoais, contidas no artigo 5º, sendo classificados de forma separada os **dados pessoais**, consistentes em "*informação relacionada a pessoa natural identificada ou identificável*"[17] e **dados sensíveis**, consistentes em "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*". O tratamento de dados pessoais somente poderá ocorrer mediante a autorização prévia, gratuita, informada e inequívoca do titular (KUJAWSKI; THOMAZ, 2018, p. 3) e, em se tratando de dados sensíveis, referido consentimento deverá ainda constar em cláusula própria, apartada das demais[18]

[17] Note-se que o conceito de dado pessoal na LGPD é mais extensivo que o conceito adotado pelo Marco Civil da Internet, não se limitando a dados de subscrição ou nome, endereço, CPF.

[18] Referida formalidade poderá ser dispensada nas seguintes hipóteses, insculpidas no art. 11, II, da LGPD: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

No que tange aos dados a serem coletados pelas empresas, a LGPD é expressa quanto à necessidade, isto é, as empresas deverão coletar os dados dos titulares que sejam necessários para a execução de suas finalidades, o que também se aplica ao compartilhamento de dados entre empresas, salvo em caso de "legítimos interesses do controlador", prevalecendo os direitos e liberdades fundamentais dos titulares[19].Conceito importado do GDPR, o "legítimo interesse" tem sido amplamente debatido no cenário internacional em razão de sua forma genérica, havendo receio de que hipóteses diversas se encaixem em referida exceção, de modo a torna-la regra no lugar do consentimento do usuário.

Mister se faz destacar a sensibilidade do consentimento para coleta e compartilhamento de dados. Conforme mencionado, esse deve ocorrer de maneira prévia, gratuita, informada e inequívoca por parte de seu titular, contudo, estudos demonstram que 91% dos usuários confirmam os termos de uso sem sequer ler seu conteúdo (MCDONALD; CRANOR, 2008, p. 565)[20].

A causa do desinteresse decorre principalmente do tamanho dos termos e da complexidade com que se encontram estruturados, conforme outra recente pesquisa divulgada, a qual demonstrou que a leitura dos termos de uso dos oito principais serviços acessados demandaria aproximadamente quatro horas e meia[21].

Inspirada no GDPR, a LGPD trouxe a definição de duas figuras distintas, de agentes de dados: o controlador e o operador. O controlador consiste em "*pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"* e o operador em "*pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".*

No curso de suas funções, os agentes de dados deverão realizar as seguintes funções: definir e documentar a base para o processamento de dados pessoais; garantir a implementação de

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

[19] "Destaca-se a positivação da base legal conhecida como "legítimo interesse", que permitiria o uso dos dados para finalidades além daquelas originalmente autorizadas pelos seus titulares ou as que ensejaram a sua criação. Por meio de um teste de proporcionalidade que leva em consideração os interesses dos responsáveis pelo tratamento e os direitos dos titulares, essa hipótese permitiria novos usos, o que a torna essencial em tempos de big data, inteligência artificial, machine learning e modelos de negócio inovadores baseados no uso de dados pessoais". (MONTEIRO, 2017, p. 6.).

[20] Conclusões semelhantes quanto à falta de leitura destas informações são trazidas por diversos outros estudos, tal como: "A Deloitte survey of 2,000 consumers in the U.S found that 91% of people consent to legal terms and services conditions without reading them. For younger people, ages 18-34 the rate is even higher with 97% agreeing to conditions before reading". (CAKEBREAD, 2017, p. 11).

[21] https://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-45-horas.shtml.

mecanismos para cumprir os direitos dos titulares de dados; informar violações de dados e incidentes à agencia nacional de proteção de dados e, em alguns casos, aos titulares de dados afetados; executar a privacidade avaliações de impacto quando requerido pela autoridade nacional; e nomear um oficial de proteção de dados responsável pelo tratamento de dados pessoais dentro da organização[22].

Destaca-se ainda o empoderamento conferido ao titular dos dados, o qual poderá, a qualquer tempo, obter e/ou requerer do controlador, dentre outros, o acesso aos seus dados coletados, exclusão de dados coletados além do disposto na LGPD, informações das entidades públicas e privadas cujos dados foram compartilhados, bem como revogar o consentimento previamente fornecido, impedindo a continuidade do tratamento de seus dados por aquele ente[23].

Assim como o GDPR, a LGPD prevê a possibilidade de transferência internacional dos dados, desde que o país ou organismo internacional destinatária possua leis de proteção de dados com os mesmos padrões de segurança por ela assegurados; quando o controlador comprovar estar de acordo com os padrões da LGPD; em casos de cooperações jurídica internacional; proteção à vida ou incolumidade do titular ou terceiro, com autorização expressa do titular; ou em casos excepcionais previstos no corpo da lei[24].

Ainda, importa salientar que, assim como o GDPR a LGPD possui alcance extraterritorial, uma vez que sua aplicabilidade se estende às empresas que tiverem filial no Brasil e aos serviços prestados fora do Brasil por empresas que coletem dados de pessoas residentes ou aqui em trânsito.

No tocante à autoridade nacional de proteção de dados, destaca-se o veto no ato em que a LGPD foi sancionada pelo então Presidente da república, Michel Temer, o que veio a ocorrer somente no final de seu mandato, aos 28 de dezembro de 2018.

IV– A ERA DIGITAL E A PUBLICIDADE:

Os dados pessoais consistem em informações coletadas por provedores e aplicadores de internet e, conforme acima estudado, devem ser coletados no limite da necessidade para a prestação do serviço final. Isso porque, além da discussão acerca da invasão à privacidade e à intimidade do

[22] "In addition, data controllers shall make easily accessible to the data subject a fairly detailed privacy notice, stating clear, adequate and ostensive information on the purposes of the data processing; form and duration of the data processing; contact information of the controller; information regarding the shared use of personal data by the controller; responsibilities of the processing agents; and data subjects' rights." (KUJAWSKI; THOMAZ, 2018, p.5).
[23] **BRASIL.** Lei Geral de Proteção de Dados. Artigo 18.
[24] **BRASIL.** Lei Geral de Proteção de Dados. Artigo 33.

titular (SANTOS; ARAÚJO, 2017, p. 43/52), os dados são valiosos ferramentais para promoção de bens de consumo (marketing) e sua promoção (publicidade) (BIONI, 2019, p. 11).

Dentre as formas de publicidade, importa mencionar no presente estudo a chamada *publicidade comportamental online*, a qual é a responsável por identificar padrões de consumo, personalizando as ofertas apresentadas aos internautas de acordo com seus acessos. Conforme explicação do *expert* Demi Getschko[25], ao visitar websites, os usuários são "carimbados" de forma a facilitar o reconhecimento em caso de novo acesso, o que se dá por meio dos "*cookies"*, sendo possível, dessa forma, inferir suas preferências de consumo.

Além de referida modalidade de coleta, os registros de acesso igualmente possibilitam um mapeamento de acessos realizados pelos titulares dos dados, tornando-se possível um mapeamento de suas preferências e, com isso, a personalização da publicidade que lhe será apresentada ao acessar novamente a internet (BIONI, 2019, p. 19). Em termos mais práticos, o mapeamento dos registros de acesso possibilita que o usuário realize uma pesquisa de uma viagem a ser realizada pelo seu celular e, ao acessar sua rede social via computador lhe apareça uma publicidade acerca do site de viagens e do destino consultados.

Atualmente muito se fala em "Internet das Coisas", que consiste na possibilidade de aparelhos de uso comum, como refrigeradores, televisores e afins coletarem dados do usuário, realizarem seu mapeamento e sugerirem ou mesmo efetivarem compras quando o usuário necessitar, em conformidade com seu perfil de consumo.

À título de exemplo, importa relembrar o caso de Ross Compton de Ohio: Após ter sua casa incendiada, a companhia de seguros conseguiu uma autorização para acessar os dados do marca-passo utilizado por Compton, vislumbrando que seus batimentos cardíacos eram incompatíveis com a descrição de ação e fuga por ele narrado, resultando na instauração de procedimento para averiguar os crimes de incêndio e fraude contra a seguradora[26].

Não obstante às facilidades e ônus trazidos à rotina dos usuários, importa verificar quais dados são atualmente coletados pelos serviços mais utilizados por usuários brasileiro, a fim de analisar se essa coleta está de acordo com o Marco Civil da Internet e com a Lei Geral de Proteção de Dados, que entrará em vigor no próximo ano.

[25] https://link.estadao.com.br/blogs/demi-getschko/privacidade-na-web-isso-ainda-existe/
[26] https://www.conjur.com.br/2017-fev-12/marca-passo-revela-tentativa-fraude-seguro-incendio

IV.1 DADOS COLETADOS PELOS APLICADORES DE INTERNET:

Conforme acima explicitado, a internet teve vertiginosa expansão a partir da década de 90, não sendo possível, sobretudo para as novas gerações, imaginar a vida cotidiana sem a utilização dessa importante ferramenta.

Atualmente, o método mais comum de acesso à internet pelos brasileiros se dá por meio de seus aparelhos celulares, denominados Smartphones[27] e os principais serviços acessados são aplicativos de redes sociais, mensageria e streaming (assistir vídeos)[28.]

Dentro desse contexto, o presente estudo traz como metodologia a análise dos aplicativos mais utilizados pelos brasileiros em referidas categorias: Facebook, WhatsApp e Youtube, respectivamente.

IV.2 – WHATSAPP

O WhatsApp é hoje o principal aplicativo instalado nos Smartphones dos brasileiros, tendo aproximadamente 130 milhões de usuários. Segundo pesquisa realizada pelo Mobile Time em julho de 2018, 97% dos brasileiros detentores de smartphones possuem e utilizam o aplicativo, tendo 92% destes usuários afirmado que acessam o aplicativo diariamente[29].

Ao acessar a política de privacidade do WhatsApp, percebe-se uma distinção no tratamento de dados dos usuários: Os residentes em países Europa têm seus dados tratados pelo *WhatsApp Ireland* e os residentes nos demais países tem seus dados tratados pelo *WhatsApp Inc*. Vale aqui mencionar que tanto o GDPR quanto a LGPD têm alcance extraterritorial, o que não justificaria o tratamento por empresas distintas. Contudo, não há informações suficientes na política de privacidade que nos permitam inferir que a distinção possui base legislativa[30].

Adiante, o aplicativo de mensageria explica que a coleta de dados se dá para "*funcionar, fornecer, melhorar, compreender, personalizar, apoiar e publicitar os nossos Serviços*", permitindo

[27] https://www1.folha.uol.com.br/tec/2018/07/celular-e-mais-utilizado-do-que-computador-para-acessar-internet-no-brasil.shtml
[28] http://www.ibope.com.br/pt-br/noticias/Paginas/WhatsApp-e-o-aplicativo-mais-usado-pelos-internautas-brasileiros.aspx
[29] http://www.panoramamobiletime.com.br/
[30] https://faq.whatsapp.com/general/26000121/

inferir que são coletados dados que visem a possibilitar o mapeamento dos usuários com finalidade publicitária.

O WhatsApp, assim como grande parte dos aplicativos de mensageria não requer dados cadastrais para registro dos usuários, sendo coletados, segundo dados disponíveis nos termos de uso do aplicativo ora em estudo, dados de subscrição[31]. Além de mencionados dados, o WhatsApp ainda coleta os registros de acesso dos usuários, bem como agenda de contatos, lista de grupos que os usuários fazem parte e cookies[32].

Há o mapeamento da utilização do aplicativo pelo usuário, informando a empresa coletar dados de diagnóstico, sendo possível aferir hora, frequência, durabilidade e funcionalidades utilizadas nos acessos dos usuários, com o intuito de melhorar a prestação do serviço.

No tocante ao compartilhamento de dados com outras empresas, os termos de uso do WhatsApp afirmam fazer parte das empresas Facebook e informa que, dentre as razões para o compartilhamento está a publicidade. No entanto, não é possível inferir dos termos de uso do aplicativo quais são os dados partilhados, qual tratamento dado a esses dados antes do compartilhamento e a validade que referidos dados permanecem armazenados[33].

No que diz respeito ao consentimento, o WhatsApp se faz claro quanto aos dados coletados, bem como informa que, em consonâncias às diretrizes do GDPR, o consentimento do usuário poderá ser alterado ou revogado a qualquer momento[34].

Importa salientar que o WhatsApp afirma não coletar o conteúdo das mensagens trocadas entre seus usuários, em razão do sistema de criptografia ponta-a-ponta utilizada na prestação dos serviços. Referido sistema realiza a encriptação da mensagem no celular do usuário, de forma que ela passa pelos servidores de forma indecifrável, sendo decriptada apenas no celular do receptor, por meio de um sistema chave-fechadura de chaves de encriptação.

---

[31] Número do Telefone; Informações acerca do aparelho utilizado; informações acerca do sistema operacional utilizado; informações acerca dos serviços utilizados (agenda de contatos ou se faz parte de grupos); informação de Status; informação de conexão ("visto última vez").

[32] https://www.whatsapp.com/legal/?lang=pt_pt#privacy-policy-affiliated-companies

[33] Nesse sentido, destaca-se o tópico: Como parte das Empresas do Facebook, o WhatsApp recebe e partilha informações com as mesmas. Podemos utilizar as informações que recebemos das mesmas e estas podem utilizar as informações que partilhamos com elas para nos ajudar a operar, prestar, melhorar, compreender, personalizar, apoiar e publicitar os nossos Serviços e as respetivas ofertas. Isto inclui a melhoria dos sistemas de infraestrutura e entrega e a compreensão de como os nossos Serviços ou os serviços daquelas são utilizados, o que nos ajuda a oferecer-lhe uma forma de contactar com empresas e sistemas de segurança. Também partilhamos informações com o intuito de impedir spam, ameaças, abusos ou infrações e para promover a segurança em todos os Produtos das Empresas do Facebook".

[34] https://www.whatsapp.com/legal/?eea=1#how-we-process-your-information

Abra-se um parêntesis a fim de salientar que a utilização da encriptação é encorajada pelo Decreto Regulamentador do Marco Civil da Internet, como um dos mecanismos de segurança que devem ser adotados pelas empresas de mensageria. Contudo, sob a afirmativa de que as interceptações telefônicas passaram a ser inócuas após o uso do WhatsApp diversas autoridades passaram a impor multas que superam os dois bilhões de reais[35], bem como houve casos de determinação de retirada do aplicativo do ar, razão pela qual a discussão acerca da legalidade da utilização do sistema de criptografia ponta-a-ponta[36] se encontra atualmente em discussão perante o Supremo Tribunal Federal, por intermédio das Ações Constitucionais ADI 5527[37] e ADPF 403[38].

Ultrapassada a questão do conteúdo, verifica-se que o aplicativo de mensageria ora em análise coleta dados diversos de seus usuários, a fim de garantir a melhor prestação do serviço, bem como para permitir a publicidade dos serviços. Dessa análise, concluímos que à luz da LGPD o WhatsApp deveria inserir em seus termos de uso quais dados são compartilhados e com quais empresas do Facebook, a fim de assegurar a transparência de sua política e a garantia da capacidade de determinação informativa do titular ou demonstrar que o compartilhamento se enquadra na possibilidade de dispensa do consentimento em razão do "legítimo interesse" da empresa, conforme disposto na legislação que vigorará a partir do próximo ano.

IV.3 – FACEBOOK

O Facebook foi criado no ano de 2004 por Mark Zuckerberg, Dustin Moskovitz e Chris Hughes, então alunos da universidade de Harvard. Então com o intuito de conectar alunos daquela faculdade, o Facebook teve rápida adesão, sendo hoje a rede social mais utilizada para interligar pessoas conhecidas ou com afinidades similares, contando com 500 milhões de usuários inscritos.

Seguindo a metodologia do presente estudo, analisamos os termos de uso do Facebook[39], a fim de verificar quais dados são coletados, armazenados e compartilhados. Constata-se que a rede

[35] https://tecnoblog.net/238480/facebook-multa-brasil-quebra-sigilo-whatsapp/, https://www.gazetadopovo.com.br/economia/nova-economia/whatsapp-e-multado-em-r-21-bilhoes-por-nao-colaborar-com-investigacao-de-trafico-de-drogas-eukq04c8ic44gg630os47caok/

[36] Importa ressaltar que não apenas o WhatsApp utiliza-se de referida tecnologia, a qual provém de protocolo público e disponível na internet denominado signal, mas também aplicativos como Telegram, Skype, dentre outros.

[37] http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282

[38] http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500

[39] https://www.facebook.com/about/privacy

social coleta uma gama de dados mais expressiva e complexa que o aplicativo de mensageria anteriormente analisado.

No que tange aos dados do usuário, o Facebook informa coletar metadados, bem como faz um *disclaimer* acerca da coleta de dados sensíveis e a proteção especial hoje em vigor pelo GDPR. Quanto aos dados, mediante aceite dos termos de uso o usuário autoriza a coleta do conteúdo das comunicações[40], de seus registros de acesso, localização em que fotos foram tiradas, data em que um arquivo foi criado, imagens capturadas pela câmera.

A interação com usuários, grupos, páginas e *hashtags* igualmente é coletada pela rede social, sendo analisada a frequência com que o usuário acessa ao Facebook, quando foi seu último acesso e quais publicações, vídeos e conteúdos foram acessados. Cumpre salientar que essas mesmas informações são coletadas quando usuários compartilham publicações com referência a outros usuários.

Ademais dos dados coletados dos usuários, há ainda a coleta de dados dos dispositivos (computadores, telefones, TVs conectadas e outros dispositivos conectados à web) utilizados para acessar a rede social, tais como i) Marca e Sistema operacional do dispositivo, ii) versão do software ou sistema operacional utilizado; iii) informações sobre operações e comportamentos realizados no dispositivo, como em que plano está a aba com o Facebook e o movimento do cursor do mouse; iv) Identificadores do dispositivo; v) Sinal de Bluetooth e pontos de wi-fi utilizados; vi) cookies.

Insta sublinhar que tem se tornado cada vez mais comum a utilização do Facebook como "*Application Programming Interface*" (API), o que consiste no usuário se conectar a um serviço ou plataforma por intermédio de outro[41]. Mencionada plataforma fornecerá ao Facebook informações sobre suas atividades, inclusive informações sobre seu dispositivo, os sites acessados, as compras realizadas, os anúncios visualizados. Vale destacar que a transmissão dessas informações independe de o usuário ter ou não uma conta ou de estar conectado ao Facebook.

A coleta expressiva de dados tem como função a personalização dos serviços prestados pelo Facebook, permitindo sugestões quanto a pessoas, locais, compras e demais interações baseadas no mapeamento desses dados coletados. Ademais, há compartilhamento dos dados com empresas

[40] Ao contrário do WhatsApp, o Facebook Messeger permite, em regra, a coleta do conteúdo das conversas mantida entre os usuários, salvo a opção de conversas em sites que se vale da encriptação de ponta-a-ponta.
[41] À título de exemplo, a identificação de um usuário na plataforma Waze (aplicativo que permite ao usuário calcular rotas de deslocamento com análise do tráfego), por intermédio de seu Facebook.

parceiras, a fim de que avaliem a eficácia e a distribuição dos respectivos anúncios e serviços, e delinear o perfil de usuários que se utilizam desses serviços e como interagem com os sites, aplicativos e serviços deles.

Importa sublinhar ainda que, em meados de 2014 o Facebook Inc. se tornou acionista do WhatsApp Inc., de modo que, conforme previsto em ambos os termos de uso, há intercâmbio das informações coletadas acerca dos usuários entre as empresas. Infere-se ainda o compartilhamento de dados com empresas estranhas ao grupo Facebook, a fim de que haja melhorias e ampliações tanto da rede social como dos parceiros, tais como serviços de análise, anunciantes, pesquisadores. Por fim, prevê-se o compartilhamento com acadêmicos e em resposta a pedidos de autoridades. Insta sublinhar que não há em referida sessão quais dados dos usuários do Facebook são compartilhados com empresas terceiras.

A análise dos termos de uso do Facebook nos permite concluir que uma gama extensa e complexa de dados é reiteradamente coletada de seus usuários. No tocante ao compartilhamento de dados, seja com empresas do grupo ou com empresas terceiras, não é possível depreender quais desses dados são alvos do intercâmbio, de forma que resta igualmente maculada a transparência dos termos de uso e o consentimento do usuário frente ao "legítimo interesse da empresa".

A preocupação com a amplitude de dados coletados pelo Facebook foi um dos impulsionadores da edição da LGPD, uma vez que referida empresa esteve diretamente envolvida no escândalo da empresa *Cambridge Analytcs.* Em referida circunstância, a empresa teve acesso não autorizado a dados de 50 (cinquenta) milhões de usuários do Facebook, utilizando-os de modo indevido para influenciar na eleição do atual presidente norte-americano, Donald Trump. Em decorrência de mencionado escândalo, Mark Zuckberg foi convocado e compareceu ao Senado americano para prestar esclarecimentos.

IV.4 – YOUTUBE

O Youtube foi criado no ano de 2005 por Chad Hurley, Steve Chen e Jawed Karim. Já no ano seguinte, após rápida ascensão da plataforma, a gigante Google adquiriu o Youtube em transação de 1,65 bilhões de dólares.

Nesse contexto, não é possível identificar os dados coletados exclusivamente pelo Youtube, uma vez que se faz necessário criar uma conta no Google para utilizar-se da plataforma. Desta

forma, recorremos à política de privacidade do Google[42], a fim de identificar quais dados são coletados dos usuários.

No tocante aos dados dos usuários, no ato de subscrição são fornecidos nome, endereço de e-mail e um número de telefone. Ademais, o Google coleta todo o conteúdo criado, subido ou baixado, vídeos salvos e comentários realizados em vídeos assistidos.

O Youtube rotineiramente é acessado via diversos dispositivos, tais como celulares, tablets ou televisores com função compatível. Referidos dispositivos fornecem ao Google seus registros de acesso, seus identificadores, as informações do software ou sistema operacional, localização via GPS ou wi-fi e bluethooth; e data, hora e URL acessada. No que tange ao conteúdo, o Google coleta os termos pesquisados, vídeos assistidos, visualizações e interações com conteúdo e anúncios, atividades em sites parceiros e cookies.

Segundo informações do Google, as informações dos usuários são compartilhadas com empresas e serviços não pertencentes ao grupo com o consentimento do titular, para processamento externo por empresas ou pessoas "confiáveis" aos olhos do Google, bem com o para atender à requisição de autoridades.

A análise dos termos de uso dos serviços prestados pela Google nos permite inferir que não há o compartilhamento de dados com empresas terceiras para fins de publicidade e mapeamento de consumo, salvo nos casos em que há o consentimento do usuário. Nessa esteira, não obstante a gama de dados coletados, não vislumbramos em primeira análise nenhum ponto de sensibilidade frente às legislações de proteção de dados.

V – CONCLUSÃO

O presente estudo teve o escopo de analisar o surgimento da internet e sua vertiginosa expansão nas últimas décadas. Ademais, buscou-se analisar as duas recentes leis que versam sobre proteção de dados: o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

Da análise do Marco Civil da Internet concluímos que este possui restrito alcance a usuários e provedores ou aplicadores de internet, no ambiente virtual, determinando quais dados devem ser coletados, por quanto tempo e resguardando sobretudo a privacidade e a liberdade de expressão.

[42] https://policies.google.com/privacy?hl=pt

A Lei Geral de Proteção de Dados, por sua vez, foi inspirada em legislação europeia (GDPR) e possui alcance mais amplo, atingindo empresas públicas e privadas, no ambiente físico ou virtual. Em referida lei encontramos novo e extensivo conceito de dados pessoais, distinguidos de dados sensíveis. Abordamos com enfoque o consentimento do usuário para a coleta e compartilhamento de dados, bem como as excepcionalidades a esse consentimento, em especial o "legítimo interesse das empresas".

A partir da análise legislativa, adotou-se estudo empírico, analisando nos termos de uso dos três principais aplicadores de internet acessados pelos brasileiros e quais dados são efetivamente coletados e de qual maneira são tratados e compartilhados, buscando em tal análise compreender a adequação às legislações estudadas.

Conclui-se do presente estudo que os aplicadores de internet coletam expressiva quantidade de dados de seus usuários, não sendo possível, contudo, vislumbrar em suas políticas quais dados são compartilhados, não sendo possível inferir se é necessário o consentimento do titular ou se há o devido enquadramento nas exceções legais, de modo que há evidente limitação da capacidade de determinação informativa do usuário.

Nesse diapasão, correto afirmar que a legislação traz em seu corpo lacunas e termos genéricos que possibilitam a ausência de transparência nos termos de uso dos aplicadores de internet, mantendo o usuário no *status quo* de insegurança quanto às informações compartilhadas e a forma como tais informações influem no seu mapeamento de compras, em sua geolocalização e na sua privacidade de forma geral.

REFERENCIAS BIBLIOGRAFIAS

BIONI, BR. **Proteção de dados pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Marco Civil da Internet.

BRASIL. Decreto Lei nº. 8771/2015.

BRASIL. Lei Geral de Proteção de Dados.

CAKEBREAD, C. You're not alone, no one reads terms of service agreements. **Business Insider**. Nov/2017.

DONEDA, D. **Da Privacidade A Proteção De Dados.** Rio de Janeiro: Renovar, 2006.

GONÇALVES, VHP. **Marco Civil da Internet comentado**. São Paulo: Atlas 2017.

KUJAWSKI, FF; THOMAZ, ACE. **The Privacy, Data Protection and Cybersecurity**. Law Review 5th Edition, October/2018.

LEITE, GS; LEMOS, R (coord.). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

"MCDONALD, AM.; CRANOR, LF. The Cost of Reading Privacy Policies. *Journal of Policy for Information Society*, Vol. 4, 2008.

MENDES. LS. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MONTEIRO, RL. **Lei Geral de Proteção de dados**: **análise**. www.baptistaluz.com.br, 2018.

MOSCHOVITOS, CJP. **History of the Internet: A Chronology**, **1843 to the Present**. ABC-CLIO, 1999.

NIVER, H. **Tim Berners-Lee**: **Inventor of the World Wide**. Web. New York: Rosen Publishing, 2016.

PECK. P. **Direito Digital**. Ed.6. São Paulo: Saraiva, 2016

PUPO. ACP. Privacidade, liberdade de expressão e proteção de dados pessoais: uma perspectiva brasileira com base na jurisprudência do Supremo Tribunal Federal. Dissertação (Mestrado em Direito Civil) – **Pontifícia Universidade Católica de São Paulo**. São Paulo, 2017.

SANTOS. MCC; ARAUJO, M. **Tribunal do Futuro e o futuro dos tribunais**. Curitiba: Appris 2017.

LINKS CONSULTADOS.

http://icq-planet.com/the-history-of-icq/
http://imagem.camara.gov.br/Imagem/d/pdf/DCD00199905110008200000.PDF#page=57,
https://cs.stanford.edu/people/eroberts/courses/soco/projects/distributed-computing/html/body_history.html
https://link.estadao.com.br/blogs/demi-getschko/privacidade-na-web-isso-ainda-existe/
https://policies.google.com/privacy?hl=pt
https://www.britannica.com/topic/Napster
https://www.britannica.com/topic/Yahoo-Inc
https://www.conjur.com.br/2017-fev-12/marca-passo-revela-tentativa-fraude-seguro-incendio
https://www.google.com/about/our-story/
https://www.trutower.com/2013/01/10/microsoft-windows-live-messenger-retrospective/
https://www.whatsapp.com/legal?eea=1#key-updates
https://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-45-horas.shtml
https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-