



APARECIDO VIANA DA CRUZ JÚNIOR

A AMPLITUDE DO CONCEITO DE PRIVACIDADE COM O BIG DATA

Ji-Paraná
2019

APARECIDO VIANA DA CRUZ JÚNIOR

A AMPLITUDE DO CONCEITO DE PRIVACIDADE COM O BIG DATA

Artigo apresentado no curso de graduação em Direito do Centro Universitário São Lucas 2019, como requisito parcial para obtenção do título de Bacharel.

Orientador: Mestre Aroldo Bueno de Oliveira

Ji-Paraná
2019

C957n

Cruz Júnior, Aparecido Viana da

Um Novo conceito de privacidade com o big data / Aparecido Viana da Cruz Júnior. Ji-Paraná: Centro Universitário São Lucas, 2019.

22 p. il.

Trabalho de Conclusão de Curso (graduação) - Centro Universitário São Lucas, Curso de Direito, Ji-Paraná, 2019.

Orientador: Prof. Me. Aroldo Bueno de Oliveira

1. Privacidade. 2. Intimidade. 3. Big Data. 4. Coleta de Dados Pessoais. 5. Tecnologia. I. Oliveira, Aroldo Bueno de. II. Um Novo conceito de privacidade com o big data. III. Centro Universitário São Lucas.

CDU 340

Ficha catalográfica elaborada pelo bibliotecário José Fernando S Magalhães
CRB 11/1091

Aparecido Viana da Cruz Júnior

A AMPLITUDE DO CONCEITO DE PRIVACIDADE COM O BIG DATA

Artigo apresentado no curso de graduação em Direito do Centro Universitário São Lucas 2019, como requisito parcial para obtenção do título de Bacharel.

Orientador: Mestre Aroldo Bueno de Oliveira

Ji-Paraná ____ de ____ de 2019

Resultado:

BANCA EXAMINADORA

Resultado:

Titulação e nome

Centro Universitário São Lucas

Titulação e nome

Centro Universitário São Lucas

Titulação e nome

Centro Universitário São Lucas

A AMPLITUDE DO CONCEITO DE PRIVACIDADE COM O BIG DATA

Aparecido Viana da Cruz Júnior

RESUMO: O presente trabalho teve como objetivo verificar as transformações que ocorrem na sociedade, principalmente, novas revoluções tecnológicas, que trouxeram consigo uma mudança no entendimento fundamental sobre privacidade e intimidade. Informações pessoais são distribuídas em larga escala na internet e passou a ser de interesse de empresas o manejo dessas informações para alavancarem vendas através de dados importantes sobre seus clientes. Assim, foi constatado a fragilidade dos usuários diante de sistemas de *Big Data* e a importância do surgimento de leis que passaram a proteger as informações pessoais e regulamentar como as empresas devem se portar antes, durante e depois da coleta de informações pessoais. Ao final constatou-se o surgimento de uma nova cultura, a divulgação da privacidade de forma espontânea contemporaneamente ao desejo de proteger dados pessoais dos usuários que utilizam serviços na internet.

Palavras-chaves: Privacidade. Intimidade. Big Data. Coleta de Dados Pessoais. Tecnologia.

EXTENSION OF PRIVACY CONCEPT WITH BIG DATA

ABSTRACT: This paper aims to verify the transformations that occur in society, especially new technological revolutions, which can cause a change in the fundamental understanding of privacy and intimacy. Personal information is widely distributed on the Internet and has become of interest to companies or managing this information to leverage sales through important data about their customers. Thus, the fragility of users after Big Data systems and the importance of data processing that protects personal information and regulate how companies should be behaved before, during and after the collection of personal information was noted. In the end, a new culture is discovered or emerging, the spontaneous disclosure of privacy immediately contemporary to the desire to protect personal data of users who use services on the Internet.

Keywords: Privacy. Intimacy. Big data. Collection of Personal Data. Technology.

Gráfico I



Gráfico usando palavras chaves do artigo feito com a ferramenta:

www.wordclouds.com/

1. INTRODUÇÃO

As pessoas nascidas no não tão distante século passado talvez sintam-se incomodadas com a afirmação "um novo conceito de privacidade"; o que de fato acontece é que a humanidade passa por ciclos que renovam e transformam conceitos estabelecidos como a privacidade.

A nova geração participante dessa nova "etapa evolutiva da privacidade" não se incomoda com a divulgação de dados como: nome, idade, gênero, ideologia; prova disso é que na maioria dos serviços de mídia sociais a coleta de dados não é feita de maneira abrupta, pois os próprios usuários dispõe dados pessoais e informações sobre o que gostam, com quem andam, por onde andam e até o que

comem livremente em suas redes sociais, o que as empresas como Facebook e Google fazem é armazenar essas informações traçando perfis que possam ser disponibilizados para anunciantes, sem informar aos anunciantes informações como nome, e-mail e documentos pessoais. Entretanto, é preciso analisar com cautela essa nova etapa.

Hodiernamente, cada ato online é coletado e arquivado, fazendo com que tenhamos uma identidade de conduta online e nossas preferências e gostos pessoais passam a dizer muito sobre nós, cada detalhe pessoal sobre os internautas pode ser arquivado e comercializado.

Hoje um em cada quatro habitantes do planeta usa algum serviço do Facebook que é dono de serviços como a rede social Instagram e o aplicativo de mensagem instantânea WhatsApp, segundo matéria do Estadão. (CAPELAS, 2019)

A privacidade é objeto inerente à vida humana ao qual todos necessitamos para mantermos nossa individualidade e escolhas como modo de vida, hábitos, comunicação livre de censura, segredo de quaisquer espécies, intimidade, relacionamentos, segurança etc., entretanto, ocorre que, ao mesmo tempo necessitamos de acesso sem restrições à internet, tornando-se, segundo declaração da Organização das Nações Unidas (ONU) um direito humano, tal sua importância nos dias atuais. Ocorre um certo paradoxo, queremos todo o avanço tecnológico que possamos ter sem abrir mão da nossa privacidade. (EURONEWS, 2016)

A tecnologia proporciona avanços sociais e até jurídicos, a pergunta que deve ser feita é: como garantir que direitos existentes no mundo físico permaneçam *online*.

2. PRIVACIDADE E MODERNIDADE

Segundo o dicionário *online* de língua portuguesa, privacidade é:

Qualidade do que é privado, do que diz respeito a alguém em particular: não se deve invadir a privacidade de ninguém. Intimidade pessoal; vida privada, particular. (DÍCIO, 2019)

É possível entender que privacidade é algo íntimo, particular e que é algo que não deve ser invadido. Legalmente, tem-se esses direitos assegurados em na Carta Política de 1988, mais precisamente em seu art. 5º, inciso X, versando sobre a inviolabilidade da intimidade, prevendo ainda indenização caso haja o descumprimento da lei.

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; (BRASIL, 2019)

Entretanto, o grande desafio jurídico atual é perceber que assim como a sociedade avança em suas percepções de como as coisas são, seguramente, pelo advento do avanço tecnológico, assim, as novas normas jurídicas devem evoluir para acompanhar os avanços a sua época além de ter a ambição de assegurar uma integração segura e harmônica entre pessoas e o mundo tecnológico.

A privacidade não é mais uma norma social, pelo menos não como conhecemos um dia.

Nossos celulares possuem aplicativos que aprenderão nossos hábitos e se aperfeiçoarão para uma melhor experiência do portador deste, poderá traçar o trajeto da sua casa até o trabalho, informar qual trajeto será mais rápido até o destino final, mapear suas localizações preferidas, quem são seus familiares e seus melhores amigos, acompanhar quantas horas de sono você tem entre diversas outras funcionalidades.

A vida moderna está repleta de novas funcionalidades e facilidades que não existiam há poucas décadas atrás, assim, nos tornamos pessoas sondáveis, ou seja, informações sobre nós estão disponíveis em serviços na internet e, nós escolhemos isso todos os dias ao ligar nossos smartphones, televisores, carros etc.

A vida moderna traz consigo uma nova percepção sobre princípios fundamentais como privacidade. A geração dos nossos pais não se expunha tanto quanto nós o fazemos hoje e assim será com a geração dos nossos filhos, princípios

como privacidade e intimidade são transformados conforme o entendimento da geração que a vive.

3. BIG DATA: O PETRÓLEO DO SÉCULO XXI

Big Data nada mais é do que o sistema que estuda e desenvolve maneiras de armazenar e manejar grandes quantidades de informações e analisá-las da maneira mais rápida possível, para extrair valor de um grande volume de dados, provenientes de uma variedade de fontes.

A importância e o alto valor desses dados para a economia está no cruzamento dessas informações que podem fazer com que lojistas conheçam os hábitos de consumo de seus clientes, preferências e interesses, podendo oferecer produtos com um alto índice de conversão em compras, pois anunciam o produto certo para a pessoa certa através de interesses armazenados e cruzados com *Big Data*, para exemplificar podemos citar o famoso caso da rede americana *Target*, quando em 2010 a empresa fez uma campanha onde suas clientes preenchiam um formulário informando entre algumas questões se estavam grávidas e a data do nascimento da criança. Assim, a varejista sabia que além de um futuro consumidor a caminho, os pais também aumentavam consideravelmente o consumo de certos produtos voltados para cuidados pessoais de mulheres. Com os dados em mãos fizeram o cruzamento de dados das compras de novos clientes assim, perceberam que havia similaridade em certas ações e após alguns meses de gravidez as clientes consumiam produtos como loções ou cremes hidratantes sem cheiro e nos últimos meses passavam a adquirir produtos de reposição vitamínica. (AGOSTINI, 2012)

Com os dados dos possíveis clientes, conseguiram aumentar em cerca de 30% as vendas dos produtos para gestantes, prevendo o consumo delas e as fidelizando durante e depois da gravidez. (AGOSTINI, 2012)

O *Big Data* pode ser usado em qualquer área atualmente, tanto *on-line* ou *off-line*, economia ou segurança pública, desta forma, no carnaval de 2019, o Estado da Bahia adotou o sistema de reconhecimento facial e cadastraram mais de 60 mil

registros no banco de dados da Secretaria da Segurança Pública, na lista integram pessoas que têm ou já tiveram dívidas com a Justiça. Com o sistema ativo em Salvador, um homem fantasiado de mulher foi reconhecido e mesmo fantasiado o sistema apontou 94% de similaridade entre a imagem capturada pela câmera e o banco de dados da polícia. (MUNIZ, 2019)

O uso do *Big Data* nesses casos, funciona como um mapeamento facial, transformando o rosto do indivíduo em algoritmos, ou seja, números codificados que como uma impressão digital traçam singularidades do rosto humano como formato do crânio, distância entre nariz, boca, orelhas etc. (MUNIZ, 2019)

No Brasil estão sendo investidos recursos em sistemas de Segurança Pública com *Big Data*, segundo o Ministério da Justiça e Segurança Pública serão investidos 32 milhões de reais em ferramentas de tratamento de dados que utilizam *Big Data*, o intuito é o monitoramento e a prevenção de práticas delituosas. A polícia, poderá com o tratamento de dados, traçar perfis de criminalidade das pessoas que tiverem seus registros no banco de dados, analisar os locais frequentados e traçar geograficamente lugares com maior índice de criminalidade, enfim, as possibilidades para o uso dessa tecnologia são infinitas, o que fará com que a polícia não só tenha uma orientação mais eficaz sobre onde e como os crimes ocorrem, mas também, em alguns casos prevenir atividades delituosas com base nos dados colhidos dessas regiões. (BRASÍLIA, 2019)

O cuidado nesses casos deve estar na preocupação sobre a assertividade do sistema de reconhecimento pois, o reconhecimento errôneo pode gerar danos a inocentes, e também, o cuidado da população civil em preocupar-se com o controle Estatal sobre os hábitos das pessoas, ocorrendo grave lesão aos princípios individuais caso o Estado espione indivíduos indiscriminadamente.

Caminhamos a passos largos para uma nova revolução, agora, uma revolução tecnológica e o direito deve estar atento a todas as mudanças que ocorrerem, desta forma, garantir que todos os usuários da internet tenham seus direitos garantidos e preservados.

4. TERMOS DE PRIVACIDADE NA INTERNET

Atualmente, plataformas *on-line* precisam de páginas informando os usuários sobre a coleta e uso dos dados que conseguem colher com o acesso em suas plataformas, essas informações precisam estar disponíveis de forma esclarecida para os usuários para que possam fazer o manejo dos dados, desta forma as plataformas evitam problemas jurídicos, trazendo segurança para o consumidor e credibilidade para a empresa que colherá as informações. (CENDÃO, 2017)

Pode ser verificado como mudanças sociais ou jurídicas fazem com que Microsoft e Google mudem suas políticas de privacidade e fiquem sempre atualizando seus termos de uso e privacidade. Essas empresas disponibilizam um histórico de alterações nas suas políticas de privacidade, com isso pode ser visto com qual frequência essas duas empresas alteram seus termos de uso. Segundo o histórico dos termos de privacidade do Google, desde 1999 até 2019 foram feitas 30 atualizações, são 1,5 atualizações por ano. Já a Microsoft de 2015 que é a data mais antiga disponível até 2019 foram feitas 24 atualizações totalizando cerca de 6 atualizações por ano. Mesmo que haja avisos aos usuários que ocasionalmente ocorrem mudanças conforme a necessidade de cada plataforma, é de extrema importância que as pessoas verifiquem os termos de uso e privacidade antes aceitos por elas esporadicamente para analisarem se ainda concordam em terem seus dados colhidos e tratados. Com esse cuidado os usuários evitam serem lesados, além de terem a possibilidade de simplesmente mudar de ideia sobre a coleta e armazenamento de suas informações por essas plataformas ou até mesmo para obterem esclarecimentos sobre seus próprios dados e o que cada empresa faz com eles.

Nem todas as atualizações nos termos dessas duas empresas versam sobre coleta de dados, elas mantem uma política ativa sobre manter seus usuários informados sobre mudanças em seus termos de uso e privacidade, todavia, podemos analisar como conceitos e diretrizes mudam conforme a necessidade atual, como pode ser visto no gráfico a seguir a rapidez de tais mudanças feitas pelo Google e Microsoft e as datas de cada mudança.

Gráfico II

Atualizações Google	Atualizações Microsoft
Versão atual (2019)	Setembro de 2019
25 de maio de 2018	Agosto de 2019
18 de dezembro de 2017	Junho de 2019
2 de outubro de 2017	Maio de 2019
17 de abril de 2017	Abril de 2019
1 de março de 2017	Março de 2019
29 de agosto de 2016	Novembro de 2018
28 de junho de 2016	Outubro de 2018
25 de março de 2016	Agosto de 2018
19 de agosto de 2015	Maio de 2018
30 de junho de 2015	Abril de 2018
5 de junho de 2015	Fevereiro de 2018
1 de maio de 2015	Outubro de 2017
25 de fevereiro de 2015	Setembro de 2017
19 de dezembro de 2014	Agosto de 2017
31 de março de 2014	Junho de 2017
20 de dezembro de 2013	Março de 2017
24 de junho de 2013	Fevereiro de 2017
27 de julho de 2012	Novembro de 2016
1 de março de 2012	Setembro de 2016
20 de outubro de 2011	Agosto de 2016
3 de outubro de 2010	Janeiro de 2016
11 de março de 2009	Outubro de 2015
27 de janeiro de 2009	Julho de 2015
7 de agosto de 2008	
14 de outubro de 2005	
1 de julho de 2004	
4 de janeiro de 2001	
20 de setembro de 1999	
9 de junho de 1999	

Gráfico feito pelo autor com informações colhidas nos domínios:
<https://policies.google.com/privacy/archive?hl=pt-BR> (GOOGLE 2019) e
<https://privacy.microsoft.com/pt-br/updates> (MICROSOFT 2019)

5. MARCO CIVIL DA INTERNET

Decretada em abril de 2014 o Marco Civil da Internet (MCI), lei nº 12.965/2014, rege normas e princípios que versam sobre a utilização da internet no território federal, regulando pessoas físicas e jurídicas tanto de direito privado e público na internet. Quando foi sancionada, havia um debate mundial sobre a neutralidade na internet e sem regulação havia abusos tanto dos usuários em publicar conteúdos inadequados quanto de empresas que poderiam excluir conteúdo publicado em suas plataformas sem prévio aviso ou não excluir quando solicitado pelo poder público o conteúdo publicado que pode ter gerado um dano a outrem. (PRETTO, 2019)

Com a neutralidade, o Brasil figura entre os primeiros países a garantir a neutralidade na internet, garantindo sem distinção a mesma qualidade de acesso para todos os usuários, mas, não é só sobre neutralidade que fala a lei, ela trata sobre mais três importantes princípios existentes na rede de internet: a neutralidade da rede a liberdade de expressão dos usuários e a privacidade. (VALENTE, 2017)

Segundo André Carbette, editor do site Nexojornal são pontos importantes abordados pelo Marco Civil da Internet; principalmente a garantia ao acesso a uma rede de internet neutra, sendo garantido aos usuários um provedor de internet que não deve definir que tipo de site ou aplicativo o usuário visita, tão pouco controlar a velocidade da conexão em qualquer endereço acessado. Também, deve ser proibido, por exemplo, negar o acesso a um devido aplicativo e permitir outro segundo a vontade do provedor, como por exemplo permitir a Netflix e negar o Spotify, dar uma velocidade de acesso a determinada plataforma e outra velocidade a outra plataforma segundo critérios do provedor, como por exemplo conceder maior velocidade de acesso ao Facebook e ceder menos velocidade ao acessar o YouTube ou qualquer plataforma ou site disponível. A ideia é que o usuário tenha acesso a toda a internet, e não a aplicativos, serviços ou sites pré-determinados pelo provedor forçando o usuário a acessar determinados sites ou plataformas ou o obrigando a pagar pacotes maiores de internet para ter acesso total. (CABETTE, 2019)

Liberdade de expressão: Quem responde por um conteúdo é quem o postou. O Youtube, por exemplo, não precisa controlar os vídeos colocados ali. A empresa só é responsabilizada se mantiver algo no ar, mesmo após a Justiça mandar tirar. É um jeito de proteger a liberdade de expressão, já que é proibido definir previamente o que pode e o que não pode ir para o ar. Há casos específicos, porém, em que é preciso agir sem motivação judicial, como no caso de pornografia infantil.

Privacidade: Os provedores de internet só podem guardar registros de conexão dos usuários por no máximo um ano. Também é proibido armazenar e monitorar informações pessoais e histórico de navegação. Já empresas, nacionais ou estrangeiras, como WhatsApp e Google, devem armazenar informações por no máximo seis meses. Autoridades só podem acessar dados pessoais com ordem judicial. (CABETTE, 2019)

O Marco Civil da Internet também contribuiu para assegurar uma rede de internet mais democrática, pois, garantiu o acesso sem limites aos usuários, garantia que já esteve ameaçada no passado quando o então ministro da Ciência, Tecnologia, Inovações e Comunicações Gilberto Kassab havia dito que os planos de internet ilimitados chegariam ao fim no país, pouco tempo depois houve mudanças nos planos divulgados, porém essa preocupação nunca foram esquecidas pelos usuários temendo terem o direito de acesso à internet limitado pelo Estado. O Brasil não é o primeiro país a tentar limitar os planos de internet, países como Estados Unidos já oferecem planos limitados aos seus usuários, existindo também planos ilimitados. (MONTEIRO, 2017)

A internet tornou-se um ambiente plural, amplamente democrático e garantiu o livre acesso a informação aos seus usuários de maneira ilimitada, surgindo assim a era de livre acesso a informação. Qualquer pessoa pode adquirir conhecimento sobre qualquer assunto pois, em uma rede livre e ilimitada basta alguns cliques e todo o conhecimento é transmitido, tornando antigos veículos de informação e de ensino em instituições ultrapassadas e pouco inovadoras, além de tirar o monopólio da transmissão de ideias e transmitir esse poder a todas as pessoas que tenham acesso à internet e algo a ensinar. Desta forma, o Marco Civil e outros mecanismos jurídicos asseguram a inovação em todos os aspectos sociais que envolvem a liberdade de acesso à internet.

6. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), veio estabelecer normas mais específicas quanto ao tratamento de dados pessoais para empresas e entes públicos. Versa sobre os direitos dos titulares das informações e as obrigações de quem processa os dados, regulando a atividade e sobretudo trazendo segurança jurídica para os usuários de plataformas *on-line* pois, anteriormente o titular dos dados não sabia quais informações estavam sendo colhidas e para que seriam usadas, agora o titular poderá ter acesso a todas as informações além de ter o poder de escolha quanto a permanência das suas informações em bancos de dados de determinadas empresas.

A Lei entra em vigor em de agosto de 2020, por ser uma regulação extensa e abrange toda a internet além de qualquer manejo de dados pessoais *on-line* e *off-line* no território nacional e empresas estrangeiras que oferecem seus serviços no Brasil, o legislador entendeu que esse tempo de *vacatio legis* era o tempo necessário para que empresas e entes dos setores públicos possam ter seus serviços adequados a nova legislação. (AGÊNCIA SENADO, 2019)

A lei é inspirada na legislação europeia (UE) 2016/679 Regulamento Geral sobre a proteção de Dados (RGPD) que já regulamenta tratamento de dados. (COMISSÃO EUROPEIA, 2019)

A distinção entre a legislação europeia e a brasileira é que no Brasil a lei tem um alcance maior, atingindo empresas públicas e não apenas o setor privado, segundo informação da Agência Senado:

A LGPD regulamenta o tratamento de dados e informações pessoais, inclusive em meios digitais, por entes públicos e privados. A lei é inspirada na regulamentação já utilizada na Europa, com uma diferença importante: no Brasil as empresas públicas também estão sujeitas à lei. Empresas que não se adequarem às exigências poderão pagar multa de até R\$ 50 milhões, entre outras sanções. (AGÊNCIA SENADO, 2019)

Até a LGPD entrar em vigor em 2020 as empresas e usuários ainda precisam respeitar as regulamentações existentes como o Marco Civil da Internet e, em casos específicos, buscar amparo aos mecanismos já em vigor no País como o Código de Defesa do Consumidor lei nº 8.078 de 1990. (BRASIL, 2019)

Desta forma, o maior benefício da LGPD é a cultura do respeito à proteção dos dados pessoais e a privacidade das pessoas. Está sendo criada uma nova mentalidade com as novas regulamentações no mesmo momento em que o compartilhamento da intimidade é algo comum na internet.

Todavia, existem certas categorias de dados pessoais que recebem uma proteção maior, pois, são informações que podem identificar um usuário e, portanto, foi criada a categoria denominada “dado sensível” quando contém informações relacionadas a documentos que identifiquem o usuário ou sua etnia, religião, opinião política, opção sexual e até mesmo estado de saúde, desta forma, a lei busca evitar formas de discriminação. (VALENTE, 2019)

Existem princípios na lei que tentam promover uma proteção maior ao usuário atingido pelo Big Data e o manejo de dados para que esse não seja o elo mais fraco na relação entre empresa fornecedora de serviço ou plataforma e usuário, são aspectos fundamentais para que a aplicação da lei seja de maneira que ocorra o bem-estar social do titular e podemos observar, tais aspectos nos incisos do artigo 6º da LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e

os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL 2019)

Estabelecidos os princípios o próximo passo é dar atenções às previsões legais necessárias para que haja justificção quanto ao interesse do tratamento das informações dos usuários, assim, as empresas que trabalham com o manejo de dados precisaram ter objetivo certo e claro quanto à coleta e uso das informações, estando assim justificados quanto ao uso de *Big Data*, desta forma, deverão ter seus objetivos analisados em conjunto ao artigo 6º, analisado anteriormente, e 7º apresentando tais requisitos adiante:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2019)

Fica claro logo no inciso I do artigo 7º da LGPD que o titular tem o poder de decisão quanto à disponibilidade das suas informações pessoais. No direito civil temos o princípio do consensualismo nas relações contratuais onde existe o vínculo, dentre outras formas, o desejo de firmar um acordo, desta forma, acordo entre as partes acerca do objeto do contrato, como acontece no contrato de compra e venda, objeto do artigo 482 do Código Civil.

Art. 482. A compra e venda, quando pura, considerar-se-á obrigatória e perfeita, desde que as partes acordarem no objeto e no preço. (BRASIL, 2019)

Portanto, sendo um acordo de vontades ele pode ser externado por meio verbal, escrita, expressa ou tácita.

Já na Lei Geral de Proteção de Dados Pessoais encontramos o seguinte dispositivo acerca do consentimento do titular do dado:

Art. 5º Para os fins desta Lei, considera-se:
[...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...] (BRASIL, 2019)

O artigo 5º da LGPD deixa claro que para existir consentimento o titular deverá expressar requisitos específicos não podendo ser simplesmente o entendimento de vontade ou, após o consenso, o silêncio de uma das partes não poderá ser considerado consentimento, todavia, a lei também não exige necessariamente o consentimento do usuário por meio escrito, poderá ser por um clique do botão no *pop-up* de alguma plataforma ou site para a aceitação dos termos

de uso ou qualquer outro meio que demonstre fisicamente ou virtualmente o interesse de vontade do titular como pode ser observado no caput do artigo 8º:

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (BRASIL, 2019)

O consentimento é um dos principais objetos que dará permissão ao agente que pretende tratar as informações do titular, mas, não é causa de exclusão de observância dos demais requisitos da lei, todavia, deverá ser contextualizada diante dos outros critérios necessários para o consentimento, não deixando o titular o dado desprotegido mesmo após ter consentido o tratamento das suas informações pessoais pela empresa ou plataforma interessada. (FRAZÃO, 2018)

Outro ponto a ser destacado acerca da coleta de informações diz respeito à motivação da empresa, como vemos no inciso IX do artigo 7º da LGPD:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses
[...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; [...] (BRASIL 2019)

Assim, o inciso IX estabeleceu um termo que deverá ser analisado com cautela pois pode ter diferentes interpretações que é o legítimo interesse, por isso, a importância de se estabelecer os princípios a serem seguidos, para que qualquer previsão do artigo 7º, seja regido pelos princípios do artigo 6º que dá ao titular um lugar de segurança quanto ao tratamento de dados pessoais realizado. Desta forma, a autoridade competente deverá fiscalizar o legítimo interesse para proteger os direitos dos titulares, tendo algum princípio ferido da lei, a empresa que estiver realizando o tratamento dos dados perderá permissão obtida pela caracterizada pelo legítimo interesse, também a empresa gestora dos dados deverá apresentar um plano de contingência para sanar o erro e apresentar formas de proteção para

as informações armazenadas em seu banco de dados. (COTS, 2019)

Assim, deverão ser comprovadas certas situações para que estejam caracterizadas para o tratamento de dados o objetivo concreto, finalidade legítima, preservação dos direitos do titular, benefícios ao titular, necessidade e transparência que terão previsibilidade legal para o tratamento de informações pessoais. Sendo assim, as empresas que queiram trabalhar com tratamento de dados pessoais precisaram cumprir alguns requisitos citados acima conforme sua necessidade, portanto, estabelecidos esses princípios os titulares ficam resguardados quanto à proteção de seus dados pessoais e adquirem certo poder de decisão sobre como e quais dados serão coletados e se permitirão ou não, podem decidir quanto a confirmação da coleta do dado, quanto ao acesso, correção, anonimização, eliminação do dado do banco de dados quanto ao seu compartilhamento, negativa de consentimento, revogação do consentimento concedido e a portabilidade dos seus dados para outra empresa de seu interesse como prevê os artigos abordados. (AGÊNCIA SENADO 2019)

7. SANÇÕES ADMINISTRATIVAS DA LGPD

Big Data e tratamento de dados pessoais é um assunto sobre tecnologia e inovação, porém, antes de mais nada, é um assunto jurídico pois versa sobre informações pessoas que garantem a intimidade de cada indivíduo, ou seja, princípio protegido e assegurado pela Carta Magna Brasileira, portanto, é preciso existir penalidade em seus descumprimento.

Desta forma, foi criado o órgão que fiscalizara o cumprimento dos requisitos da lei, e fiscalizar os procedimentos para tratamentos de dados pessoais, com a publicação da Lei 13.853 de julho de 2019 que alterou a Lei Geral de Proteção de Dados Pessoais criou-se a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL, 2019)

A lei criada pela medida provisória 869/2018, estabelece que o Órgão Federal ANPD cuidará especificamente da aplicabilidade e interpretação da LGPD como também de sanções para coibir descumprimento da lei, e terá natureza transitória

podendo ser transformada em autarquia vinculada à Presidência da República após dois anos, a critério do governo. (AGÊNCIA SENADAO, 2019)

Após vetos e mudanças as sanções ficaram estabelecidas da seguinte forma:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração; [...]

(BRASIL, 2019)

A Lei Geral de Proteção de Dados Pessoais trouxe segurança para usuários da rede mundial de internet que possam ter seus dados pessoais armazenados e comercializados por terceiros, tendo seu direito à privacidade e garantia à intimidade preservados, pois, têm autonomia de escolha acerca da disponibilidade dos seus dados estarem em poder de empresas e plataformas *on-line* e *off-line*. E também poder buscar esclarecimento quanto ao uso de tais informações.

A informação pessoal de cada usuário é muito valiosa tanto para o titular quanto para a empresa que faça o manejo de *Big Data*, portanto, deve haver segurança jurídica na relação pois, antes de mais nada existe uma relação de consumo e as partes devem estar equiparadas para não acontecer excessos de nenhuma das partes. Portanto, a LGPD é um passo importante pois, no atual momento histórico da vida humana, relações de consumo estão cada vez mais presentes no mundo digital.

8. CONCLUSÃO

As relações sociais e comerciais estão em transição, passando do mundo

físico para o mundo digital, portanto, é preciso ficar atento com que tipo de informação pessoal está disponível sobre nós na internet. Assim, fez-se necessário o acompanhamento jurídico para garantia de princípios individuais para que o avanço tecnológico traga com sigilo o respeito ao indivíduo, priorizando o tratamento humano dos usuários de serviços na internet.

Desta forma, a legislação acerca de *Big Data*, coleta e tratamento de dados, mesmo sendo muito recente no País, não pode ser negado que é um grande avanço no cenário da segurança de dados pessoais, visto que é a primeira lei a lidar com o assunto de maneira específica. Garantindo o direito do usuário de proteger seus dados pessoais e também, a legislação preocupou-se em manter o desenvolvimento tecnológico do assunto abordado, principalmente quando estabeleceu o termo *legítimo interesse* na coleta de dados, pois em situações concretas e certas não é necessário a liberalidade do usuário, porém, sempre deve ser observado princípios que beneficiem o dono do dado coletado.

A lei busca assegurar ao usuário o controle de seus dados pessoais e proporciona a ele autonomia em sua decisão, através de normas claras que estabelecem princípios de como devem ser tratadas informações pessoais e quais são os direitos do usuário, podendo este, voltar atrás nos consentimentos e pedir esclarecimentos sobre uso e finalidade dos dados pessoais para as empresas e órgãos públicos que colheram suas informações.

Por fim, reconhecendo a relação bilateral de consumo, as legislações estão visando assegurar aos indivíduos uma proteção jurídica quando estiverem conectados à rede de internet.

REFERÊNCIAS

Agostini, Renata, Revista Exame. **A nova indústria da espionagem explora o consumo.** Disponível em: <https://exame.abril.com.br/revista-exame/a-nova-industria-da-espionagem>. Acessado em: 31 ago. 2019.

Dicionário da Língua Portuguesa, **Significado de Privacidade.** Disponível em: <https://www.dicio.com.br/privacidade/>. Acessado em: 12 out. 2019

Capelas, Bruno, O Estado de S. Paulo. **Temos de proteger a privacidade e a saúde mental das pessoas', diz Mark Zuckerberg.** Disponível em: <https://link.estadao.com.br/noticias/empresas,temos-que-proteger-a-privacidade-e-a-saude-mental-das-pessoas-diz-mark-zuckerberg,70003026190>. Acessado em: 31 ago. 2019.

Muniz, Tailane, **Reconhecimento facial já prendeu 35 na Bahia; 3 mil são alvos da polícia.** Disponível em:

<https://www.correio24horas.com.br/noticia/nid/reconhecimento-facial-ja-prendeu-35-na-bahia-3-mil-sao-alvos-da-policia/>. Acessado em: 31 ago. 2019.

Feitosa, Alessandro, **Gizmodo Brasil, Sistema de reconhecimento facial ajuda polícia baiana a prender homem procurado por homicídio**. Disponível em: <https://gizmodo.uol.com.br/reconhecimento-facial-bahia-prender-homem/>. Acessado em: 31 ago. 2019.

Cots, Márcio; Oliveira, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. Editora Revista dos Tribunais. São Paulo. 2018.

Frazão, Ana, Jota Info. **Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018>. Acessado em: 7 set. 2019.

Valente, Jonas, Agência Brasil Brasília. **Lei de Proteção de dados traz desafios a empresas, cidadãos e governo**. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo>. Acessado em: 7 set. 2019.

União Europeia. **Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)?**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt. Acessado em: 7 set. 2019.

Carbette, André, Nexo Jornal. **A aplicação do Marco Civil da Internet, 5 anos depois**. Disponível em: <https://www.nexojornal.com.br/expresso/2019/04/22/A-aplica%C3%A7%C3%A3o-do-Marco-Civil-da-Internet-5-anos-depois>. Acessado em: 29 set. 2019.

Monteiro, Larissa, Grupo Abril. **Sim, pode ser que sua internet seja limitada pelo governo**. <https://veja.abril.com.br/tecnologia/sim-pode-ser-que-sua-internet-seja-limitada-pelo-governo/>. Acessado em: 29 set. 2019.

Valente, Jonas, Agência Brasil Brasília. **Entenda o que é neutralidade de rede e como é o seu funcionamento no Brasil**. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-12/entenda-o-que-e-neutralidade-de-rede-e-como-e-o-seu-funcionamento-no-brasil>. Acessado em: 29 set. 2019.

Pretto, Nelson, Comitê Gestor da Internet no Brasil. **Neutralidade da rede no marco civil da internet.** Disponível em: <https://marcocivil.cgi.br/contribution/neutralidade-da-rede-no-marco-civil-da-internet/139>. Acessado em: 29 set. 2019.

Cendão, Fabio, Parceiro Legal. **Política de privacidade: O que é e Porque é tão Importante para Seu Site.** Disponível em: <https://parceirolegal.fcmlaw.com.br/politica-de-privacidade/politica-de-privacidade/>. Acessado em: 29 set. 2019.

Euronews, **Acesso à internet é um direito humano diz ONU.** Disponível em: <https://pt.euronews.com/2016/07/05/acesso-a-internet-e-um-direito-humano-diz-onu>. Acessado em: 15 out. 2019.

Andrade, Marcio Roberto, Conta Azul, **LGPD Brasil: como se adequar à Lei Geral de Proteção de Dados Pessoais.** Disponível em: <https://blog.contaazul.com/lgpd-lei-geral-protecao-dados-pessoais>. Acessado em: 15 out. 2019.

Redação, Agência Senado, **País deve se preparar para Lei de Proteção de Dados Pessoais, aponta debate.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/08/08/pais-deve-se-preparar-para-lei-de-protecao-de-dados-pessoais-aponta-debate>. Acessado em: 15 out. 2019.

Redação, Agência Senado, **Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos>. Acessado em: 15 out. 2019.

Redação, Agência Senado, **MP que cria a Autoridade Nacional de Proteção de Dados ainda aguarda instalação de comissão mista.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/03/12/mp-que-cria-a-autoridade-nacional-de-protecao-de-dados-ainda-aguarda-instalacao-de-comissao-mista>. Acessado em: 15 out. 2019.

BRASIL. Lei Geral de Proteção de Dados nº 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Palácio do Planalto Presidência da República,** Brasília, DF, 14 de agosto de 2018. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.
Acessado em: 12 set. 2019.

BRASIL. Marco Civil da Internet nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Palácio do Planalto Presidência da República**, Brasília, DF, 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em: 12 set. 2019.

BRASIL. Medida Provisória nº 869/2018 de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 27 de dezembro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm >. Acessado em: 12 set. 2019.

BRASIL. Conversão da Medida Provisória nº 869, de 2018, Lei 13.853 de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm. Acessado em: 12 set. 2019