CENTRO UNIVERSITÁRIO UNA

A NOVA LEI DE PROTEÇÃO DE DADOS E SUA INTERFACE COTIDIANA COM A PRIVACIDADE DOS CIDADÃOS

Vitor Hugo Alves Januario

Renan Fernandes Nunes

Betim

2021

Vitor Hugo Alves Januario
Renan Fernandes Nunes

A NOVA LEI DE PROTEÇÃO DE DADOS E SUA INTERFACE COTIDIANA COM A PRIVACIDADE DOS CIDADÃOS

Trabalho de conclusão do curso apresentado ao curso de Direito, como parte dos requisitos necessários à obtenção do título de Bacharel em Direito do Centro Universitário UMA – Betim. Orientador: Wagner Vilaça
Área de Concentração: Direito Constitucional e Direito

Betim
2021

A NOVA LEI DE PROTEÇÃO DE DADOS E SUA INTERFACE COTIDIANA COM A PRIVACIDADE DOS CIDADÃOS

Trabalho aprovado. Betim, junho de 2021.

_____

Wagner Vilaça Orientador

_____

Professor Convidado 1

_____

Professor Convidado 2

RESUMO:

Esta pesquisa apresenta a perspectiva do direito à proteção de dados pessoais e sua interface cotidiana com a privacidade dos cidadãos. Trata-se de uma discussão dicotômica entre a liberdade de autodeterminação informativa do cidadão e o dever de proteção de dados e da fiscalização do tratamento desses dados por parte do Estado, garantindo-se a privacidade do cidadão. Essa complexa análise exige uma harmonização entre o desenvolvimento tecnológico e a proteção de direitos fundamentais, franqueando ao cidadão o controle de seus dados pessoais e, ao mesmo tempo, exige uma fiscalização e tratamento legítimo, adequado e razoável dos dados por parte dos entes públicos e privados envolvidos. A pesquisa bibliográfica documental foi realizada pelo método dedutivo.
Palavras-chaves: direitos à privacidade; proteção de dados; sociedade da informação; Lei Geral de Proteção de Dados.

ABSTRACT:

This research presents the perspective of the right to protection of personal data and its daily interface with citizens' privacy. It is a dichotomous discussion between the citizen's freedom of informative self-determination and the duty of data protection and inspection of the processing of these data by the State, guaranteeing the citizen's privacy. This complex analysis requires a harmonization between technological development and the protection of fundamental rights, giving the citizen the control of their personal data and, at the same time, it demands a legitimate, adequate and reasonable inspection and treatment of the data by public and private parties involved. The bibliographic documental research was carried out by the deductive method.
Keywords: privacy rights; data protection; information society; General Data Protection Law

SUMÁRIO

1. INTRODUÇÃO

O objetivo do presente artigo consiste em investigar a nova lei de proteção de dados e sua interface cotidiana com a privacidade dos cidadãos. É que a vida em sociedade vem exigindo novas reestruturações sociais e novas gamas protetivas com a conectividade massiva da população. A exposição em redes sociais e na própria internet em si acaba por obrigar o usuário a fornecer determinados dados, que são coletados e recebem tratamentos diversificados e, por vezes, ilegítimos e ilegais.

A Lei de Proteção de Dados de 2018 vem com o intuito de proteger essas informações e o tratamento dado a elas. Contudo, ela perpassa sobre o direito à privacidade do indivíduo. A divulgação massiva de dados e a tutela do direito à vida privada tornou-se uma emblemática no Direito, pois de um lado há um interesse do cidadão em expor-se nas redes e manter-se conectado, exercendo sua liberdade positiva de autodeterminação informativa e, por outro lado, há um interesse estatal e privado no uso desses dados para fins políticos, econômicos e sociais. E, paralelamente, há o dever do Estado em garantir e fiscalizar o uso adequado desses dados.

A temática da proteção de dados vem chamando a atenção dos governos e da sociedade civil face aos diversos escândalos acerca do uso indevido desses dados e os riscos que essas informações podem acarretar aos envolvidos, aos países e ao mundo. Em paralelo a isso há ainda a discussão acerca de uma sociedade totalitária em que predomina a busca do desenvolvimento tecnológico em desfavor da tutela do direito à privacidade.

Assim, a presente pesquisa busca evidenciar a necessária harmonização entre o desenvolvimento tecnológico e a preservação dos direitos fundamentais, sobretudo do direito à privacidade mediante o uso da liberdade positiva informativa e uma legítima utilização e tratamento desses dados por parte dos entes estatais, empresas privadas, organizações civis e da própria sociedade a partir dos parâmetros estabelecidos pela LGPD e pelos mandamentos constitucionais.

A pesquisa bibliográfica-documental, por meio do método dedutivo, parte da premissa macro de a privacidade e a tutela de dados representarem direitos fundamentais da pessoa humana em direção a uma análise micro acerca de como esse direito será resguardado diante do desenvolvimento das plataformas e otimização de dados a partir da Lei Geral de Proteção de Dados.

2. O DIREITO FUNDAMENTAL À PRIVACIDADE

A privacidade representa uma ideia cultural introduzida enquanto direito fundamental por fatores sociais, políticos e econômicos diante uma necessidade humana de resguardar determinados elementos de sua vida particular. Essas transformações transcorridas durante o processo evolutivo da sociedade perpassa a relação entre o ser humano e seu habitat de convivência.

Esses espaços de convivência são definidos historicamente entre o público e o privado. Na antiguidade grega, a sociedade dividia-se nesses domínios público-privado, no qual os cidadãos livres mantinham relações entre si na denominada *polis* (esfera política) e também interagiam com os membros de sua família de modo mais privado na chamada esfera familiar. Assim, a pessoa exercia sua função política na *polis* e também em campo familiar, numa inserção privada ou público-política. (HABERMAS, 2014). Contudo, somente indivíduos considerado livres exerciam essa relação patriarcal, já que não se considerava cidadão os estrangeiros, escravos e mulheres. (CARDOSO JÚNIOR, 2014).

Assim, havia autonomia entre as esferas públicas e privadas, mas a primeira era o local no qual o cidadão apresentava sua liberdade de pensamento e, perante seus familiares apresentava sua individualidade. Com a descentralização de poder pós queda do Império Romano, a esfera pública passa a ser representada na pessoa do senhor feudal, ficando o domínio público equidistantes do indivíduo comum, mas, ao mesmo tempo, há uma valorização da esfera privada fortalecendo-se os ambientes familiares a partir de estratégias política e social. (CHAPAPUZ, 2006).

A modernidade acabou por acentuar a promoção do social, de modo que a seara pública tornou-se instrumento de sociabilidade para proteger a esfera privada da riqueza e da propriedade da casa. Assim, na mutação da esfera privada a propriedade adquire um significado especial por assegurar um lugar próprio e seguro ao indivíduo, de modo que o privado passa a ter supremacia e invade o domínio público. (CARDOSO JÚNIOR, 2014).

O direito à privacidade, assim como os demais direitos fundamentais passaram a ter uma importância maior pós Segunda Guerra Mundial em virtude da valorização de determinados direitos após os horrores trazidos pela Segunda Guerra. Houve uma participação

maior do Estado na vida dos cidadãos transitando do Estado Liberal para o chamado Estado de Bem Estar Social. (DONEDA, 2006).

O direito à privacidade refere-se a um direito fundamental, cujo caráter universal lhe é peculiar. Trata-se de um direito inerente à pessoa humana, requisito para sua titularidade enquanto direito perpétuo, inato e indisponível. O ordenamento jurídico pátrio reconhece o direito à privacidade como direito fundamental tanto na perspectiva constitucional quanto na esfera civilista por meio das terminologias vida privada e intimidade. A Constituição reconhece tal direito em ser art. 5º, incisos X, XI e XII da CR/88 (BRASIL, 2021) e, o Código Civil em seu art. 21 do Código Civil (BRASIL, 2020).

Silva (2009, p. 206) define a privacidade como:

> (...) o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem isso pode ser legalmente sujeito. A esfera da inviolabilidade assim, é ampla, abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos e, bem assim, as origens e planos futuros dos indivíduos.

Assim, a vida privada do indivíduo referenda um direito fundamental não apenas para se opor ao público, mas como extensão de seu direito à personalidade, Essa concepção contemporânea com a "(...) a evocação da privacidade supera o tradicional quadro individualista e se dilata em uma dimensão coletiva, no momento em que deixa de considerar o interesse do indivíduo enquanto o tal, porém como membro de um determinado grupo social." (RODOTÁ, 2008, p. 27).

A privacidade representa, pois, um direito categorizado como bem coletivo merecendo tutela estatal em todos os parâmetros e não somente na relação indivíduo-estado. Assim, o direito à privacidade traduz uma dimensão negativa, no sentido de garantia de não intervenção estatal, e também numa dimensão positiva, no sentido do Estado de garantir esse direito em face de condutas de terceiros.

Com a globalização e a intensificação da internet, o direito à privacidade assumiu novos contornos. A sociedade passou a receber informações instantaneamente e a tutela da privacidade tornou-se um fato primordial, um direito fundamental da pessoa humana. Atualmente, para participar da esfera social, como forma de garantir o ideal de felicidade contemporânea o indivíduo deve estar sempre conectado.

Como reflexo disso, essa interseção entre a vida real e as redes sociais acabam por introjetar no indivíduo uma vontade patológica em apresentar conteúdos no facebook, instagram e outras redes. Trata-se de uma realidade social em que a digitalização do cotidiano na internet implica em ser integrante da sociedade. Vale dizer a "(...) divulgação de grande parte do ambiente privado como uma forma de participar da sociedade do espetáculo" (CARDOSO JÚNIOR, 2014, p. 85)."

Essa hiperconexão representa um marco de uma sociedade fluída, digitalizada cuja exposição da vida íntima constitui um fator essencial, quase que vital, para a vida da pessoa. Assim, essa exposição massiva na internet, nas redes sociais acaba por expor inúmeros dados dos indivíduos, o que enseja uma série de questões a serem analisadas, inclusive do direito da proteção de dados pessoais. Essa dicotomia entre tecnologia e privacidade acaba por ensejar o direito à proteção de dados pessoais como um direito fundamental como extensão do direito à privacidade.

3. DADOS PESSOAIS NA ERA DIGITAL: QUARTA REVOLUÇÃO

O desenvolvimento e a difusão das tecnologias digitais nas últimas décadas, especialmente nos últimos anos, vem propiciando grandes transformações sociais e, por derradeiro, vem mudando a forma como se produz e consome dados. Trata-se de uma era focada no consumo instantâneo de informações que foi acelerada com a chamada Quarta Revolução Industrial e, também, com os efeitos da pandemia da Covid-19. Essa crise sanitária acelerou ainda mais a chamada " informacionalização da sociedade" e seus reflexos atingem a vida cotidiana da população como um todo e acaba por impactar na seguridade dos dados dispostos na internet.

O mundo nunca esteve tão conectado. Esse termo "informacionalização da sociedade" ou "sociedade da informação" vem sendo utilizado para se referir a esse contexto temporal hodierno em que o acesso e uso de informações tornaram-se o eixo central da sociedade. Conquanto não há uma origem clara do termo, ele vem sendo utilizado em debates acadêmicos americanos e em países asiáticos para explicar as mudanças sociais provocadas por essas novas tecnologias que propiciam a fluidez em alta velocidade das informações. (CASTELLS, 2011).

Segundo Takahashi (2000), essa formação e desenvolvimento pode ser atribuído a alguns fatores como: a convergência da base tecnológica, a dinâmica da indústria e o crescimento da internet¨ A convergência de dados implica na possibilidade de se processar qualquer informação de forma digital apenas. O primeiro fator se refere à possibilidade de se processar qualquer tipo de informação a partir de uma única forma, qual seja, a digital. Assim, palavras, imagens ou outros meios de dados podem ser transmitidos e estarem disponíveis em celulares, computadores, tablets.

Como reflexo disso, a indústria trouxe uma dinâmica de queda nos preços e aprimoramentos tecnológicos que permitiu a difusão dos meios eletrônicos à população que foi potencializado pela rapidez de propagação de dados pela internet. Logo, o termo "sociedade da informação" acaba por resultar num paradigma social que estabelece novos rumos para a sociedade em termos econômicos, políticos e sociais, sobretudo numa era epidêmica em que o mundo digital tem sido a plataforma de vivência da sociedade.

Nesse atual contexto, a informação revela-se como um instrumento essencial, como uma matéria prima primordial das novas tecnologias. E, pelo fato da informação constituir parte integrante da atividade humana, os aparatos tecnológicos apresentam-se como fatores essenciais que moldam o processo de existência social e coletiva. (CASTELLS, 2011). Hoje, a maioria da população consegue acessar cada vez mais meios tecnológicos de informações de forma instantânea, realizando desde diálogos simples a transações bancárias e ou negociações comerciais por meio digitais.

Entretanto, todo esse arcabouço de informações deixa rastros que podem ser convertido em armazenamento de dados dos indivíduos. Esses mesmos dados podem facilitar a vida do cidadão, mas, paralelemente, empresas e governos podem fazer essa coleta de dados pessoais em massa e utilizar para diversos mecanismos. Trata-se de um efeito colateral da mudança de paradigma trazida pela chamada "Quarta Revolução Industrial:

> A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela "Quarta Revolução Industrial", cujo tom é dado pelo fenômeno da "informacionalização da sociedade", iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico empresarial,quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações. (BOFF; FORTES e FREITAS, 2018, p. 13).

Essas perspectivas de mudança social abrupta e radical denominada como quarta revolução industrial mudou a maneira como a sociedade compra, utiliza os meios bancários, modificando grande partes das atividades cotidianas dos cidadãos. Em razão disso, os dados pessoais dos indivíduos resultaram em elementos a serem explorados na rede mundial de computadores e, consequentemente, transformaram-se em ferramentas essenciais nesse novo formato de economia, inclusive com a monetização de dados e informações pessoais dos indivíduos.

A primeira revolução industrial ocorreu entre 1760 e 1840 por meio da produção mecânica realizada nas ferrovias e máquinas a vapor ao passo que a segunda revolução industrial ocorreu entre o final do século XIX e início do século XX impulsionada pela invenção da eletricidade e pela organização da indústria em linhas de montagem. Já a terceira revolução industrial transcorreu entre 1960 e 1990 a partir das tecnologias digitais com a criação de computadores, computação pessoal e da internet. (SCHWAB, 2016).

Nesse processo de criação da terceira revolução industrial que a chamada sociedade da informação se desenvolve e cria aparatos para o desenvolvimento e fomentação de uma quarta revolução industrial. Esta se baseia em processo de revolução digital que concilia diversas tecnologias que promovem uma evolução em ritmo acelerado, profundo e com forte impacto sistêmico, representando uma nova etapa no cotidiano humano. (SCHWAB 2016).

Essa quarta revolução acabou por permear o surgimento de dossiês digitais acerca da população mundial, com uma riqueza detalhada de aspetos individuais da pessoa. Essa composição de conteúdo individuais são extensos e são utilizados de forma que afeta profundamente a vida das pessoais em múltiplos fatores da sua vivência. E a adaptação à essa evolução, apesar de complexa, representa uma alternativa, quiçá, a única, para a própria evolução e inovação da sociedade:

> A 4ª Revolução, marcada pela convergência de tecnologias digitais, físicas e biológicas, afetará o mercado, pois os homens terão que se adaptar às transformações, que certamente serão complexas, pois estarão ligadas diretamente à velocidade, ao alcance e aos impactos, portanto, as Organizações devem estar aptas para evoluir e inovar (MOLINA; SANTOS, 2020, p.40).

A ubiquidade trazida pela Internet revela esse cenário de impossibilidade ao *status quo* anterior. Isso porque a Internet está presente em diversos aparelhos domésticos, além dos automóveis, relógios e na própria residência por meio das inteligências artificiais. Essa última permite o processamento de dados para fins diversos e cada vez mais avançados, promovendo uma verdadeira ruptura com o contexto social que a antecede:

> Ao permitir "fábricas inteligentes", a quarta revolução industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível. Isso permite a total personalização de produtos e a criação de novos modelos operacionais. A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos nessa revolução, as tecnologias emergentes e as inovações generalizadas são difundidas muito mais rápida e amplamente do que nas anteriores, as quais continuam a desdobrar-se em algumas partes do mundo. A segunda revolução industrial precisa ainda ser plenamente vivida por 17% da população mundial, pois quase 1,3 bilhão de pessoas ainda não têm acesso à eletricidade. Isso também é válido para a terceira revolução industrial, já que mais da metade da população mundial, 4 bilhões de pessoas, vive em países em desenvolvimento sem acesso à internet. O tear mecanizado (a marca da primeira revolução industrial) levou quase 120 anos para

> se espalhar fora da Europa. Em contraste, a internet espalhou-se pelo globo em menos de uma década. (SCHWAB, 2016, p. 19-20).

Essa conjunto de informações trazidas pela quarta revolução industrial apresenta inúmeras modificações tecnológicas como as chamadas tecnologias industriais extensíveis e a inteligência artificial que se valem de quantidade massivas de dados como mecanismo proliferador. Com isso, a questão é como o uso do *Big Data* impacta nas decisões de empresas e do governo. Trata-se de uma mudança radical cuja preocupação alarmeia os cidadãos em virtude dos estabelecimentos de perfis individuais a partir dessa coletânea massiva de dados pessoais.

Esse termo *Big Data* não apresenta uma conceituação única, ao revés, converte-se de inúmeros fatores para defini-lo. Ele pode ser referir ao alto crescimento na disponibilidade e utilização de informação como às massificações de dados produzidas por fontes distintas e na velocidade de processamento e variação dos dados. Assim, a expressão *Big Data* alude tanto aos grandes bancos de dados alicerçados pelos governos e empresários como a toda tecnologia de captura de dados, crescimento, disponibilidade e uso de informações estruturadas ou não que são difundidas por meio eletrónico (SIMÃO FILHO, A.; SCHWARTZ, 2018).

Assim, a partir desse sistema torna-se possível o cruzamento de diversos dados em alta velocidade cujos fins não necessariamente são explicados por empresários ou governos. Com isso, o processo de datificação, o qual possibilita a medição e armazenamentos de dados para fins de análise, tornou-se mais sintético com a quarta revolução industrial, com o armazenamento e análise de fatores indistintos de dados. (SIMÃO FILHO, A.; SCHWARTZ, 2018).

Percebe-se essa integração de dados nos dispositivos de geolocalização de *smartphones*, o que redunda não só na localização da pessoa como também de seus dados comportamentais tal como ocorre nas redes sociais e sites específicos. Não se trata mais de algo estático, com uma coleta única. Os dados se tornaram modelos de comércio e negócio, um ativo económico vital para criação e utilização constante em todos os tipos de serviços. Mas essa datificação dos mais variados aspetos da realidade e do comportamento humano acaba por atrair uma lógica de vigilância, já que as empresas acabam por buscar mais e mais informações para fins de compreensão do comportamento humanos e consequentemente questões negociais.

Esse cenário de monitoramento e medição de comportamento humano realizado tanto pelo governo quanto por empresas é chamado de “Sociedade da Vigilância” por Stéfano Rodotá (2008). Segundo o autor há uma erosão na privacidade do indivíduo em que ele passa a ceder informações de forma compulsória para usufruir de eventuais oportunidades apresentadas na sociedade de informação. Esclarece o autor que “a pessoa é obrigada expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito.” (RODOTÁ, 2008, p. 113).

Nessa perspectiva, surge a emblemática a respeito do volume e da velocidade da geração de dados e a privacidade do indivíduo. São inúmeros os desafios a serem analisados no tocante ao acesso à difusão de dados na rede de computadores e a manipulação e mineração desses dados por parte das empresas e governos. Com isso, com esses avanços teconológicos e desenvolvimento da economia digital, torna-se necessárias leis que regulamentem esse mercado para se garantir maior transparencia no processo de coleta e tratamento desses dados pessoais, para se assegurar a proteção à privacidade.

4. CONTEXTUALIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

A internet, enquanto fator social de caráter essencial, não foi objeto de reconhecimento expresso no texto constitucional, não havendo um reconhecimento expresso de sua extensão por meio da privacidade dos dados pessoais, ficando a encargo da legislação infraconstitucional esse âmbito de proteção. Contudo, há que se ressaltar que o habeas data constitui um remédio constitucional viável, mas muito limitado, para garantir a proteção de dados. Isso porque ele assegura o acesso às informações dos bancos de dados públicos, mas limita a proteção em domínio privado (FORTES, 2016).

Infraconstitucionalmente, a tutela de dados pessoais teve início com o Código de Defesa do Consumidor, Lei nº 8.070/90, mais precisamente em seu artigo 43, § 4º, alude que os registros de dados dos consumidores de qualquer espécie se equiparam ao registros de caráter público, além de garantir acesso, ele equipara os registros de dados dos consumidores de qualquer gênero àqueles de caráter público. Além disso, o código consumerista garante ainda acesso às fichas de registro e comunicação por escrito de abertura de cadastro, registros e fichas quando não houver sua autorização prévia.

Assim, o CDC (BRASIL, 1990) tratou dos dados com foco no inadimplemento do consumidor para fins de concessão de crédito, resguardando a vulnerabilidade do consumidor perante os os bancos de dados forjados para fins creditícios. (POLIDO *et al,*) E também há ainda um conjunto de princípios basilares, como de acessibilidade e qualidade dos dados, da transparência no processo de formação da base de dados e da imperiosidade de limitação do armazenamento de dados negativos pelo prazo de cinco anos. (MENDES, 2014).

Em 2002, o Código Civil previu expressamente, em seu artigo 21 (BRASIL, 2020), a inviolabilidade da vida privada da pessoa humana, consagrando o direito à privacidade como direitos da personalidade, o qual se fundamenta como direito fundamental e guarda todas as características inerentes ao tais direitos, tais como inalienabilidade, imprescritibilidade relatividade, irrenunciabilidade, historicidade e universalidade.

Preventivamente o código civilista expressou ainda a necessidade de inviolabilidade do direito à privacidade ao prevê no mencionado dispositivo a autorização para o juiz evitar o dano (BRASIL, 2020). Esse caráter preventivo é importante pois uma vez que determinada coisa é divulgada na internet há uma probabilidade de nunca mais ser excluída, podendo se tratar de um dano irreversível à pessoa, atingindo inclusive o processo de formação de sua personalidade. Sob essa conjuntura, não se trata apenas de uma temática voltada à ideia de indenização, mas, sobretudo, de conceito de prevenção da vida privada em si. (CACHAPUZ, 2006).

A proteção constitucional e infraconstitucional do direito à privacidade estende-se à proteção de dados, vez que ambos se correlacionam intrinsecamente, não havendo como se referir à vida privada resguardada em redes sociais e na nternet em si sem se falar em uma legítima proteção de dados. A Lei de Acesso à informação, Lei nº 12.737/2012 (BRASIL, 2012), adveio de uma consulta pública *on line* realizada no ano de 2009, sendo a legislação que, de fato, impulsionou a proteção de dados pessoais.

O processo de criação dessa norma teve uma intensa participação da sociedade civil por meio de empresas, organizações sociais, ativistas e especialistas em tecnologia. Como resultado disso, o projeto foi reconhecido internacionalmente em virtude dessa participação da sociedade em que se equilibrou responsabilidades e direitos dos usuários, governos e corporações de rede.

Já a Lei nº 12.965 de 2014, Marco Civil da Internet (MCI), disciplina a tutela de proteção de dados, dispondo sobre a a aplicação a toda operação relativa à coleta, armazenamento e tratamento de dados pessoais dos usuários e provedores de internet, trabalhando diversos setores ligadas à governança da internet. Essa legislação trouxe tanto princípios como garantias e direitos no uso da internet tutelando a privacidade. Essa norma conferiu mais eficácia aos direitos fundamentais já consagrados.

O Marco Civil não disciplina de forma completa toda a proteção de dados, já que essa regulamentação viria com a lei, conforme art. 3º (BRASIL, 2014). Mas ele trouxe medidas clássicas em matéria de tutela de dados pessoais como o: i) consentimento, disposta no art. 7º, incisos VII e IX e art. 16º, inciso I; II) a transparência prevista no art. 7°, incisos VI, VIII e XI; iii) a segurança da informação e dos sistemas, dispostas no art. 2º, inciso V, e art. 10, §4º; e artigo ***45; iv)*** o respeito ao contexto - compatibilidade com o contexto de coleta dos dados para a sua utilização, estabelecido no art. 7º, inciso VIII. E trouxe também

medidas inovadoras como: a) o controle das práticas abusivas, no caso uso e compartilhamento de dados de forma incompatível com as finalidades do contrato inicial, assim como a garantia da confidencialidade da comunicação além da garantia da confidencialidade no armazenamento da nulidade de cláusulas contratuais previstas no rt. 8° e da vedação da guarda de registros de acesso a serviços de internet para provedores de conexão disposta no art. 14.

Anteriormente à legislação do Marco Civil, o acesso a dados e registros de usuários na rede munidial de computadores não possuíam qualquer regulamentação específica, permitindo um arsenal de abusos e violações de direitos, uma chamada “terra sem lei”. Daí a importância da Lei do Marco Civil no paranorama legislativo brasileiro, estabelecendo fundamentos a princípios constitucionais já consagrados, como a liberdade de expressão, comunicação e manifestação do pensamento, inviolabildiade da vida privda. E, ainda, resguardou-se a preservação, segurança e funcionalidade e neutralidade de rede por meio de aparatos técnicos similiares aos aparatos internacionais (FORTES, 2016)

Contudo, a Lei 12.965/14 (BRASIL, 2014), não se limitou a apresentar tutela criminal às violações ocorridas na internet. Ao revés, ela apresentou um conjunto de direitos e liberdades civis que traduzissem princípios fundamentais prevista na legislação brasileira, estabelecendo proteções mínimas para a tutela dos usuários brasileiros na utilização de redes sociais, da internet como um todo.. Mas, esses princípios não resguardaram especificamente acerca das coltas de dados e o tratamento a ele dados, ainsa sendo uitilizado o art. 43 do CDC como mecanismo de proteção (CANCELIER, PILATI, 2017).

Assim com essa insegurança, o Brasil ainda carecia de uma efetiva proteção de dados e mediante razões de ordem econômica para adequação brasileira aos padrões internacionais e, consequemente relacões negociais e/ou diplomáticas, a matéria de proteção de dados pessoais tornou-se medida emergencial e culminou na criação da Lei Geral de Proteção de Dados.

5. A REGULAÇÃO DOS DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD), Lei 13.709/18 foi objeto de um longo processo legislativo. Em seu artigo 1º, deduz seu objeto: tratamento de dados pessoais, tanto nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, com o escopo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa. (BRASIL, 2018),

Já o artigo segundo admite que a tutela os dados pessoais tem como meio de resguardar os direitos da privacidade, autodeterminação informativa, liberdade de expressão, de informação, comunicação, inviolabilidade da intimidade, imagem, honra, bem como o desenvolvimento econômico e tecnológico e a livre iniciativa, livre concorrência e a defesa ao consumidor ao mesmo tempo em que promove a defesa da autodeterminação informativa e a proteção dos direito humanos. (BRASIL, 2018).

A sistemática da LGDP volta-se à proteção de dados pessoais e também dos meios digitais, bem como do tratamento deles efetuado tanto pela pessoa natural quanto pela jurídica de âmbito privado e público, aplicando-se a norma desde que: a) ela ocorra em território nacional; b) a atividade de tratamento, tenha o fim na oferta, ou nofornecimento de bens, serviços, ou tal tratamento seja de indivíduos localizados noterritório nacional; e c) o campo de coleta dos dados pessoais utilizados no tratamento esteja no território nacional, conforme dispõe art. 3º (BRASIL, 2018).

O dispositivo 4º refere-se às situações em que a lei não se aplica ao tratamento de dados pessoais, destacando-se quando nos casos em que for realizado: a) por pessoa natural para fins exclusivamente particulares e não econômicos; b) para fins exclusivamente jornalísticos e artísticos ou acadêmicos; c) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais; d) fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que esse país também proporcione grau de proteção adequado à lei brasileira.

Já no art. 5º há uma definição de conceitos chaves, especialmente nesse último dispositivo:

Art. 5º Para os fins desta Lei, considera-se:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: 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;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> (...) (BRASIL, 2018).

Os princípios basilares da norma estão expressos no art. 6º: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Dentre esses destaca-se a finalidade e não discriminação. O primeiro estabelece que Deles, destaca-se o da finalidade e não discriminação. O primeiro estabelece que a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (art. 6, inc. I). Já o princíprio da "não discriminação pauta-se na impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (art. 6, inc. IX). (BRASIL, 2018).

A LGPD, em seu art. 7º, enumera as hipóteses em que o tratamento de dados poderá ser efetuado: a) autorização do titular mediante consentimento; b) cumprimento de obrigação legal ou regulatória, do controlador; c) utilização pela administração pública, para fins específicos, como tratamento e uso compartilhado de dados para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; d) estudos por

órgão de pesquisa; e) execução de contrato ou de procedimentos preliminares relacionados a contrato em que o titular seja parte e a seu pedido; f) exercício regular de direitos em processo judicial, administrativo, ou arbitral, conforme Lei de Arbitragem; g) proteção da vida ou da incolumidade física própria ou alheia; h) proteção da saúde, realizado por profissionais desta área ou por entidades sanitárias; i) interesses lícitos do controlador ou de terceiro, salvo a prevalência de direitos e liberdades fundamentais do titular que requeiram a proteção dos dados pessoais; ou j) proteção creditícia. (BRASIL, 2018).

O consentimento do titular deve ser realizado por meio escrito ou outro meio idôneo que demonstre a vontade do indivíduo no fornecimento de dados (art. 8º), devendo, no primeiro caso, haver uma cláusula destacada das demais (art, 8º, § 1º). O ônus da prova cabe ao controlador (art. 8º, § 2º), sendo vedado o tratamento mediante vício de consentimento (art. 8º, § 3º). Note-se ainda que o consentimento deve ser específico, para finalidades determinadas, sendo as autorizações genéricas nulas (art. 8º, § 4º), podendo o consentimento ser revogado a qualquer momento, excepcionados alguns casos (art. 8º, § 5º). E, no caso de alteração de informação, o controlador deverá informar o titular que poderá revogar o seu consentimento na hipótese de não acordar com as modificações (art. 8º, § 6º). (BRASIL, 2018).

Resguarda-se ao titular acesso facilitado às informações a respeito do tratamento de seus dados, especialmente acerca: a) da finalidade específica do tratamento; b) da forma e duração do tratamento, observados os segredos comercial e industrial; c) da identificação do controlador; d) dos dados de contato do controlador; e) de eventual uso compartilhado de dados pelo controlador e finalidade; f) da responsabilidade dos agentes que realizarão o tratamento; (art. 9º). (BRASIL, 2018).

Note-se que a LGPD optou por criar uma tripartição dos dados, de modo que cada qual gozasse de um nível diferente de proteção. Assim, os dados sensíveis possuem um grau maior de proteção, posteriormente vem os dados pessoais e por último os dados anônimos ou anomizados como são chamados.

Os dados pessoais sensíveis são enumerados taxativamente no art. 11 do dito diploma O titular ou o seu ou seu representante legal deve consentir expressamente o uso e para quais finalidades específicas. Contudo, independente de consentimento, quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador além de ser vedado a a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis no tocante à saúde com o objetivo de obter vantagens econômicas. Obviamente nos casos em que a portabilidade de dados for consentida pelo titular ou na necessidade de comunicação para a adequada prestação de serviços de saúde suplementar elas serão permitidas. (BRASIL, 2018).

A anomização e pseudonimização remota a conceitos importante da LGPD, trazidos, respectivamente, em seus artigos 12 e 13. O primeiro aduz que os dados anonimizados não serão considerados dados pessoais para os fins da norma apresentando algumas exceções. Já a pseudonimização "refere-se ao tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro." (art. 13, §4º). (BRASIL, 2018).

O tratamento de dados pessoais de crianças e adolescentes também foi objeto da LGPD, se o qual os dados deverão ser realizados no melhor interesse dos menores, devendo haver o consentimento específico e em destaque por pelo menos um dos pais ou pelo responsável legal (art. 14). Já o art. 15 estipula que o término do tratamento de dados pessoais poderá se dar quando: a) a finalidade tiver sido alcançada ou os dados tiverem deixado de ser necessários; b) no caso de dar o fim do período do tratamento. D) houver comunicação do titular, "inclusive no exercício de seu direito de revogação do consentimento"; d) a autoridade nacional assim determinar, quando houver violação ao disposto na LGPD. (BRASIL, 2018).

O artigo 16 trata dos dados pessoais deverão ser eliminados após o término do seu tratamento, contudo eles poderão ser conservados para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) estudo por órgão de pesquisa, "garantida, sempre que possível, a anonimização dos dados pessoais"; c) transferência a terceiro, uma vez observados os requisitos legais para tanto; e d) "uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

Os direitos dos titulares de dados pessoais são tratados nos artigos 17 a 23 da LGPD. Resguarda-se a titularidade dos dados sob a tutela dos direitos fundamentais de liberdade, de intimidade e de privacidade, bem como, a qualquer momento do direito a: a) obter do controlador a confirmação da existência de tratamento; b) ter o acesso aos dados; c) correção de dados incompletos, inexatos ou desatualizados, como visto; d) anonimização, o bloqueio ou a eliminação de dados desnecessários, dentre outros (art. 18). Lembrando que a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular (art. 19) que poderá solicitar a revisão de decisões que foram tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, (art. 20). (BRASIL, 2018).

O tratamento de dados pessoais pelo poder público é regulamentado na LGPD nos artigos 23 a 30. Esse tratamento de dados poderá ser feito por pessoas jurídicas de direito público, tendo os serviços notariais e de registro esse mesmo tratamento (art. 23), tais como os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de

Contas, e Judiciário e do Ministério Público, além de autarquias, fundações e empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, pelos Estados, Distrito Federal e Municípios. Já os artigos 31 2 32 da LGPD tratam da responsabilidade acerca do tratamento de dados pelos órgãos públicos. (BRASIL, 2018).

A transferência internacional de dados pessoais é regulamentado nos artigos 33 e 34 da LGPD. Já os artigos 37 a 45 tratam dos agentes de tratamentos de dados pessoais, especificando acerca do controlador e operador, do encarregado pelo tratamento de dados pessoais, da responsabilidade e ressarcimento de danos. Nessa última situação estabelece-se que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo." (art. 42) (BRASIL, 2018).

Já a adoção segurança e do sigilo de dados e das boas práticas e da governança são normas dispostas nos artigos. 46 a 51. O art. 46 impõe aos agentes de tratamento a obrigação de se adotarem medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados, inclusive evitando-se qualquer forma de tratamento inadequado ou ilícito. Quanto às boas práticas e à governança, os sistemas utilizados para o tratamento de dados pessoais devem atender a essas condições, juntamente com os requisitos de segurança, observando-se, ainda, os princípios gerais previstos na lei e as demais normas regulamentares pertinentes (art. 49). No tocante à fiscalização, as sanções administrativas são tratadas no art. 52 a 54. E do art. 55 adiante discute-se sobre a criação, sem aumento de despesa, da Autoridade Nacional de Proteção de Dados – ANPD e da Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e disposições finais e transitórias. (BRASIL, 2018).

6. PROTEÇÃO DE DADOS E SUA INTERFACE COTIDIANA COM A PRIVACIDADE DOS CIDADÃOS

O controle de informações representa a ideia de manutenção de poder e o contexto histórico hodierno acaba por permear esse cenário. Com o mundo globalizado e a instantaneidade dos meios de comunicação, o direito à privacidade acaba tomando uma relevância ainda maior diante da exposição de dados nas redes sociais e na internet em si. É que nessa sociedade pós-moderna, a pessoa quer interagir, se conectar aos artefatos midiáticos expostos na rede mundial de computadores.

Então para participar dessa esfera social torna-se necessário expor ao público dados de sua privacidade numa busca insana de admiradores virtuais, numa espécie de ideal de felicidade moderno. Essa digitalização do cotidiano impõe uma necessidade patológica de publicar, de enunciar ao mundo a sua prática cotidiana. Essa nova faceta de comunicação estabelecida pela internet abriu novas formas de comunicação, novos formatos de interatividade dos seres humanos.

A hiperdocumentação do cotidiano no atual século cresce exponencialmente na medida em que o indivíduo passa cada vez mais tempo no espaço virtual, mantendo-se uma interface diária entre a vida *online* e *off-line*. As redes sociais, como o Facebook, *Instagram,Twiter e whatssap* não representam somente um passa tempo da sociedade atual, eles apresentam-se como verdadeiras ferramentas de trabalho, lazer e interatividade simultaneamente. Funcionam, pois, numa espécie de apresentação curricular do indivíduo, no qual se expõe atributos, ainda que não realísticos, vida social e diversas situações cotidianas.

Essa exposição massiva em uma sociedade hiperconectada exige uma proteção desses dados, não podendo o cidadão ser um mero fornecedor de "fornecedor de dados" aos órgãos públicos e entidades privadas em uma contrapartida dos benefícios de usar dos serviços por eles oferecidos, devendo ele ser efetivamente capaz de exercer controle sobre

seus dados. Rodotà (2008) evidencia essa necessidade de uma infraestrutura informativa cada vez mais ampla e justificada, de uma garantia efetiva e da expansão dos direitos individuais ligados à privacidade e proteção de dados, não podendo o Estado e a sociedade fecharem os olhos para esse novo contexto.

Assim, a conceituação hodierna de privacidade deve abarcar um núcleo comum entre todas as situações que envolvem esse direito fundamental, sobretudo os dados dos cidadãos. Deve haver um conceito plural de privacidade, de modo que se atenda tanto as situações clássicas de invasão de privacidade quanto às novas situações advindas desse atual fluxo de informações. (LEONARDI, 2012).

Na visão de Rodotà (2008), essa atual noção de privacidade e suas novas características abarca as seguintes situações: a) o direito a ser deixado ou estar só transpassa ao direito de manter controle sobre as informações que digam respeito ao indivíduo; b) a busca pela privacidade torna-se uma verdadeira autodeterminação informativa; c) a privacidade é vista como mecanismo garantidor de não-discriminação; d) busca-se proteção ao sigilo, passando-se a buscar o controle de dados e informações, públicos ou não.

Com isso, a compreensão tradicional de privacidade deveria conviver com essa nova dimensão, com uma espécie de intercâmbio entre as tutelas estática e dinâmica do direito à privacidade, não se tratando o direito à proteção de dados como uma era evolução do direito à privacidade e sim como uma categoria autônoma. (BIONI, 2019). Assim, enquanto categoria autônoma não se limita à dignidade humana:

> O direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade. Pelo contrário, demandase uma correspondente ampliação normativa que clareie e não empole a sua tutela. (BIONI, 2019, p. 126).

Nessa perspectiva, tornou-se cada vez mais evidente uma necessária proteção de dados. Por óbvio foi preciso um escândalo em países desenvolvidos para que os governos e entes privados começassem a agir em prol da tutela de dados. Em 2013, com o escândalo do caso Snowden versus a Agência de Segurança Nacional Americana, a tutela à privacidade e a proteção de dados ficaram em evidência. Na situação fática, Edward Snowden, ex-assistente técnico da CIA criou um dossiê e o entregou ao jornalista Gleen Greenwald, que obviamente publicou o material em jornais de grande circulação, no caso o jornal britânico The *Guardian* e o american *The Washington Post.* A matéria expôs toda a espionagem americana promovida em massa pelo governo americano por meio de um programa denominado com o codinome PRISM. Esse instrumento garantia a NSA acesso

direto aos servidores das empresas *Microsoft, Yahoo, Google, Facebook, PalTalk, UOL, Skype, YouTube* e Apple, de modo que foram extraídos uma enorme quantidade de dados, como fotos, registros e emails, que permitiam ao governo americano traçar planos estratégicos. (G1, 2014, BOHRER, 2019).

Após esse episódio fatídico, surgiram outros casos, como *Cambrigde Analytica*, divulgado pelo *New York Times* no mês de março de 2018, o qual refere-se acerca das desinformações espalhadas pelas *Fake News* nas redes sociais no ano da eleição americana em 2016, expondo a vulnerabilidade dos dados pessoais dos usuários nas redes sociais. Cerca de 87 milhões de usuários tiveram seus dados informados ilegalmente à dita empresa sob a perspectiva de construção de campanhas eleitorais mais eficientes, manipulando o comportamento dos eleitores de acordo com o tipo deconteúdo que lhe era direcionado. (G1, 2018, BOHRER, 2019). Inclusive alguns veículos de imprensa chegaram a veicular que essa estratégia também foi utilizada no Brasil na campanha eleitoral de 2018, mas não teve investigação nem alardeamento como no caso americano.

Recentemente, o Supremo Tribunal Federal manifestou acerca do direito fundamental à proteção de dados pessoais. Em maio de 2020, o STF julgou a ADI 6387, relatoria da Ministra Rosa Weber, no qual foram julgadas cinco ações diretas de inconstitucionalidade propostas pelo Conselho Federal da Ordem dos Advogados do Brasil e pelos partidos políticos PSB, PSDB, PSOL e PCdoB. (BRASIL, STF, 2020). Da ementa da decisão extrai-se:

> EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida

> Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (BRASIL, STF, 2020).

A decisão suspendeu a eficácia da Media Provisória n. 954, de 17/04/2020 que dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadores de serviço público para fins de suporte à produção estatística oficial durante a situação de emergência pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020". (BRASIL, STF, 2020).

A decisão retrata que não existem mais dados neutros ou insignificantes, vez que esses bancos de dados podem identificar pessoas e que essas poderão ser usadas como forma invasiva, invadindo a esfera privativa dos cidadãos. Ademais, a relatora argui que o uso de dados tanto por entes estatais quanto por entes privados devem se dar de forma legítima mediante observação dos parâmetros estabelecidos pelos titulares dos dados, como a finalidade e o modo de utilização dos dados objeto da norma. (BRASIL, STF, 2020).

No caso julgado pelo STF, a relatora evidenciou que poderia haver uma ameaça à própria democracia na medida em que o aumento do poder de vigilância pode criar um enfraquecimento dos direitos e garantias fundamentais, não sendo legítimo e viável o compartilhamento dos dados dos usuários, devendo ser resguardada a necessidade, a adequação e proporcionalidade, de modo a se ter

clareza e transparência quanto à compatibilidade do tratamento com as finalidades informadas e a sua limitação ao mínimo necessário para alcançar as suas finalidades. (BRASIL, STF, 2020).

Ademais, não se poderia conceder a medida pleiteada ante a ausência de garantias de tratamento adequado e seguro dos dados compartilhados, pois isso compromete a responsabilização dos agentes de tratamento por eventuais danos ocorridos em virtude do tratamento de dados pessoais, o que vai de desencontro aos ditames da LGPD. Ainda que o caso verse sobre a necessidade da coleta de dados para fins epidemiológicos da Covid, essa excessiva coleta de dados pessoais e com o poder computacional dos sistemas automatizados poderiam desencadear modelos de negócios escusos e práticas ilegais que são rentabilizadas pelo uso de indevido dos dados, tal como ocorreu nos casos Cambridge Analytica.

E, esse cenário de medidas excepcionais poderiam se estender, como de fato tem ocorrido com a pandemia no Brasil, e correria um risco de uma vigilância permanente com o acesso a dados em períodos e contextos muito diferentes daqueles em que foram concedidos, o que afetaria as liberdades fundamentais e poderia criar uma verdadeira ditatura digital. (BRASIL, STF, 2020). Inclusive, nesse julgado o STF reconheceu o direito à proteção de dados como um novo direito fundamental, destacado e independente do direito à privacidade, sob o contexto de identificação das liberdades individuais, tal como defende Bioni (2019), entendimento do qual se comunga.

Essas situações evidenciam a realidade hodierna: como proteger os dados dos indivíduos nesse cenário massivo de informações veiculadas na internet? Como respeitar o espaço público-privado do indivíduo sem ferir-lhe o seu direito fundamental à privacidade? Essas emblemáticas contemporâneas apresentam uma enorme dificuldade devido ao fato da sociedade contemporânea valorizar extremamente a exposição e o interesse pelo íntimo numa eterna busca por notoriedade. Consequentemente há um intenso movimento de evasão da privacidade a qual, ainda que voluntária, merece tutela.

Por certo que o direito à privacidade tem sido historicamente articulado com base na dicotomia entre as esferas públicas e privadas. A habitação privada estabeleceria os contornos e demarcaria o refúgio no indivíduo em seu lar. Lá os indivíduos pensariam e refletiriam sobre as situações para retornar à esfera pública e se manifestar, o que evitaria que os indivíduos sofressem um nivelamento social e até mesmo a instalação de visões totalitárias. (BIONI, 2019).

Contudo, no contexto atual, a busca pela exposição tem sido a essência de vida de inúmeros cidadãos, de modo que postar as atividades cotidianos tornou-se uma necessidade e a grande dificuldade enfrentada pauta-se na separação entre as esferas públicas e privadas de cada indivíduo, do que se deve ou não estar disponível nos ambientes virtuais.

Por certo que o direito à privacidade é basilar à própria democracia, construindo-se numa "condição essencial ao livre desenvolvimento da personalidade dos cidadãos. Somente com a fuga da

“pressão social”, os indivíduos conseguiriam desenvolver cada qual a sua subjetividade para, posteriormente, projetá-la em meio à sociedade.” (BIONI, 2019, p. 124).

A emblemática é ainda maior quando se passa a analisar o fato de que essa sociedade da informação vem imprimindo uma nova dinâmica de proteção de dados da pessoa humana, com a monetização desses dados. Esses dados apresentam-se como uma nova forma de prolongamento da pessoa, interferindo na sua esfera relacional e daí reclama uma proteção de dados, com direito de acesso e retificação dos dados e oposição a decisões automatizadas, discriminatórias. (BIONI, 2019).

Note-se que até a aprovação da LGPD, o Brasil contava com leis esparsas acerca da proteção de dados, que não cobria diversos setores da economia, além de direitos basilares da população, o que acaba por gerar uma assimetria e uma insegurança não somente nos cidadãos, mas também nas relações governamentais e internacionais:

> Era uma verdadeira “colcha de retalhos” que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para: a) que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; b) a formulação de políticas públicas e parcerias público-privadas igualmente dependentes desse intercâmbio de dados; e c) o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público 256 . Sendo a proteção do consumidor e a dignidade da pessoa humana erigidas como princípios da ordem econômica pela Constituição Federal (art. 170, caput e inciso V, da Constituição Federal) que conformam a li-vre-iniciativa 257 , mostra-se ainda mais pertinente o diagnóstico dessa dupla faceta de leis gerais de proteção de dados pessoais, especialmente para se cumprir com o que foi programado em termos de ordem econômica pelo texto constitucional. (BIONI, 2019, 134).

A LGPD adveio com essa missão de proteção dos dados e consequentemente proteger os direitos fundamentais, perpassando para disciplinar aspectos econômicos e desenvolvimento tecnológico. Por certo que a dicotomia entre tecnologia e privacidade não corresponde ao melhor meio de resolução dos questionamentos outrora proposto. Deve-se haver uma harmonização entre o desenvolvimento tecnológico e a preservação dos direitos fundamentais dos indivíduos.

A LGPD vem de encontro a esses objetivos, vez que em suas disposições preliminares enunciam que a disciplina da proteção de dados pessoais tem como fim o proteger os direitos fundamentais e o livre desenvolvimento da personalidade (art. 1º) em paralelo com o desenvolvimento econômico-tecnológico e da inovação (art. 2º). Há, assim, uma dialética normativa de conciliação entre todos esses elementos na lei geral de proteção de dados.

Mendes(2014) traça um paralelo entre essa hamornização entre o desenvolvimento tecnológico e a preservação dos direitos fundamentais do indivíduo, fazendo uma analogia entre a

dicotomia vivenciada entre o desenvolvimento econômico e preservação ambiental, que nas décadas de 50 e 60 era vista como inevitável, buscando-se um caminho com o desenvolvimento sustentável. Na visão da autora esse mesmo entendimento deve ser aplicado às inovações tecnológicas e o resguardo da privacidade e a proteção de dados pessoais.

O triste cenário é que, ainda, hoje, a discussão entre desenvolvimento econômico e preservação ambiental, embora tenha chegado a um nível de discussão altíssimo, ainda encontra-se muito aquém de um desenvolvimento sustentável satisfatório. E, se a dicotomia entre proteção de dados e desenvolvimento econômico for no mesmo viés, o direito à privacidade em alguns anos será ainda objeto de muita discussão em níveis alarmantes e preocupantes.

Com isso, o principal vetor para alcançar uma harmonização entre essas esferas dicotômicas seria franquear ao cidadão controle sobre seus dados pessoais. Note-se que essa estratégia vai além do consentimento do titular dos dados, da sua autorização de uso, pois, tão importante quanto esse elemento volitivo encontra-se o resguardo protetivo do fluxo informacional que esse ato de vontade gera. (BIONI, 2019).

Logo, não basta meramente que a norma proteja seus dados, ela deve atender às suas legítimas expectativas e, sobretudo, não constituir-se em elemento corrosivo ao livre desenvolvimento da sua personalidade. É que o processo de receber e utilizar a informação promove um processo do ajuste às contingências do meio ambiente e do efetivo viver nesse meio, de modo que a harmonização entre o desenvolvimento tecnológico e a garantia de proteção de dados deve seguir por um caminho racional.

Habermas (1997), evidencia que:

> Neste Universo, a tecnologia proporciona igualmente a grande racionalização da falta de liberdade do homem e demonstra a impossibilidade "técnica" de ser autônoma, de determinar pessoalmente a sua vida. Com efeito, esta falta de liberdade não surge nem irracionalmente nem como política, mas antes como sujeição ao aparelho técnico que amplia a comodidade da vida e intensifica a produtividade do trabalho. A racionalidade tecnológica protege assim antes a legalidade da dominação em vez de a eliminar e o horizonte instrumentalista da razão abre-se uma sociedade totalitária de base racional. (HABERMAS, 1997, p. 92)

Como forma de buscar eliminar uma sociedade totalitária em que predomine a busca do desenvolvimento tecnológico numa racionalidae extrema em desfavor da tutela do direito à privacidade, tem-se que ponderar que a privacidade constitui um fator fundamental à formação e desenvolvimento da personalidade da pessoa humana e também funciona como um vetor que promove a liberdade e autonomia.

Trata-se de um interesse coletivo, já que a privacidade deve ser trabalhada também nessa perspectiva diante do fato de a sociedade contemporânea valorizar a exposição e o interesse pelo íntimo e, como reflexo disso, acaba por promover um intenso movimento de invasão de privacidade como reflexo da própria digitalização do cotidiano. Esse novo espaço de convivência do espaço *on line* deve promover determinadas garantias de tutela ao indivíduo, já que o texto constitucional, embora enalteça a liberdade de expressão, também veda a censura e declara inviolável a intimidade.

Desse modo, a tutela da privacidade no tocante à proteção de dados deve reprimir sua violação além de garantir eventual indenização ao dano ocasionado, já que, a partir do momento em que determinada informação deixa o âmbito privado, sendo objeto de veiculação em ambiente virtual não há como retomar essa posição, devendo o juiz tomar providências com o fito de impedir que o dano ocorra.

Por certo que o direito à privacidade na rede mundial de computadores implicará em sopesamento com outros direitos fundamentais, como a liberdade de expressão, dentre outros. Contudo, ainda que as benesses advindas da privacidade tenha cunho pessoal e emocional intangíveis, cuja mensuração será complexa, o sopesamento desse bem face a outros direitos fundamentais demonstra-se igualmente relevante. Assim, a ausência de um sistema eficaz de avaliação e comparação dos bens em conflito não impede uma tomada de decisão judicial razoada e proporcional diante do caso concreto.

Isso porque o próprio julgado do STF apresentou uma mudança de entendimento concebendo a autonomia do direito fundamental à proteção de dados, como um direito derivados da própria dignidade da pessoa humana, da intimidade, reconhecendo o habeas data como instrumento de tutela material do direito à autodeterminação informativa. (BRASIL, STF, 2020). E, por mais que essa última apresente uma perspectiva subjetiva, será através desse viés de autonomia que os cidadãos poderão ser protegidos contra eventuais ingerências estatais e empresas privadas no âmbito de sua privacidade. Trata-se, pois, de uma dimensão objetiva, que exige do Estado obrigações positivas como forma de garantir desse direito, tanto nas relações com o poder público, quanto nas relações privadas.

Portanto, o direito fundamental à proteção de dados pessoais exige um tratamento específico, baseando-se em medidas necessárias, adequadas e razoáveis, de modo a se conceber tais medidas somente para fins legítimos, devendo ser exigido uma fiscalização por parte de uma autoridade de proteção de dados independente. Essa nova hermeneutica do STF trazida no jugado analisado evidencia a necessidade de compreensão dos direitos fundamentais a partir do contexto social contemporâneo e numa constante atualização deles em face da acelerada evolução tecnológica.

CONSIDERAÇÕES FINAIS

O direito à privacidade refere-se a um direito fundamental inerente à pessoa humana. Trata-se de um conjunto de informações acerca do indivíduo, cujo sigilo ou divulgação deveria ficar a encargo do próprio. Mas, com os aparatos tecnológicos e o uso massivo da internet em todos os âmbitos da vida comum acabou por diagnosticar uma proteção maior desse direito face a exposição de dados nas redes sociais e na internet em si.A hiperdocumentação do cotidiano com a divulgação massiva de dados por meio de redes sociais e na internet na qual o indivíduo transforma-se em um fornecedor pessoal de dados acaba por exigir uma tutela maior do Estado, no sentido de reguardar ao indivíduo a proteção de seus dados e consequentemente do seu direito à privacidade.

A proteção desse direito fundamental em si já enfrenta inúmeros obstáculos no contexto contemporâneo diante da massificação de dados e a exposição frenética nas redes sociais em meio ao ideal de felicidade. E ela se torna ainda mais emblemática com o fato de a sociedade de informação monetizar esses dados. A posse dessas informações implica numa relação de poder extrema, num contexto em que o cenário pode modificar com o uso indevido desses dados. Os exemplos de Snowden versus a Agência de Segurança e o caso *Cambrigde Analytica* evidenciam essa emblemática, sendo esse último utilizado em campanha eleitoral americana com a exposição massiva de dados de milhões de estaunidenses e divulgação de *fake news* que, segundo alguns analistas, podem ter influenciado nessas eleições.

Esse cenário é devastador e implica em consequências de âmbito mundial. Daí a necessidade extrema da proteção de dados e tutela do direito à privacidade. Isso porque não existem mais dados neutros ou insignificantes, vez que esses bancos de dados podem identificar pessoas e que essas poderão ser usadas como forma invasiva, invadindo a esfera privativa dos cidadãos e para outros propósitos ainda mais obscuros.

Logo, o uso de dados por entes estatais, empresas privadas, organizações civis e da própria sociedade devem se dar de forma legítima mediante observação dos parâmetros estabelecidos pelos titulares dos dados, como a finalidade e o modo de utilização dos dados objeto da norma, como enuncia o texto da LGPD. Caso contrário, poderia haver uma ameaça à própria democracia se a divulgação desses dados não observar critérios de adequação, proporcionalidade e razoabilidade. Deve-se haver uma harmonização entre o desenvolvimento tecnológico e a preservação dos direitos, franqueando ao cidadão controle sobre seus dados pessoais e exigindo-se do estado uma intensa fiscalização e criação de meio protetivos que garantam ao usuário efetiva proteção do uso de seus dados, resguardando-se a sua privacidade.

REFERÊNCIAS

BOHRER, Igor Graeff. **A proteção de dados como direito da personalidade e seu risco diante do on line proffiling.** Monografia. Centro de Ciências Jurídicas – Universidade Federal de Santa Catarina. Florianópolis, 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado, 2021.

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. **Código Civil.** Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm . Acesso em: 10 mai. 2020.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 02 jun. 2021.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 02 jun. 2021.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso em: 02 jun. 2021.

BRASIL, **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 02 jun. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Declaratória de Inconstitucionalidade 6387**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil x Presidente da República. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629 Acesso em: 02 jun. 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites doconsentimento. Rio de Janeiro: Editora Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias nasociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.

CANCELIER, Mikhail Vieira de Lorenzi. *Infinito Particular:* Privacidade no Século XXI e a Manutenção do Direito de estar só. Rio de Janeiro: Lumen Juris, 2017.

CANCELIER, Mikhail Vieira; PILATI, José Isaac. *Privacidade, Pós-Modernidade Jurídica e Governança Digital:* ***O Exemplo Do Marco Civil Da Internet Na Direção De Um Novo Direito***. v. 18, n. 1, p. 65-82, jan./abr. Joaçaba. 2017. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/7252. Acesso 26 mai 2021.

CASTELLS, Manuel. *A Sociedade em rede*. São Paulo: Paz e Terra, 2011.

CARDOSO JÚNIOR, Nerione Nunes. **Hannah Arendt e o declínio da esfera pública.** Brasília: Senado Federal, Coordenação de Edições Técnicas, 2014.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo Código Civil brasileiro:** uma leitura orientada no Discurso Jurídico. Porto Alegre: Sergio Antonio Fabris Ed., 2006.

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

FORTES, Vinicius Borges. **Os direitos de privacidade de dados pessoais na internet.** Riode Janeiro: Lumen Juris, 2016.

HABERMAS, Jürgen. **Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa**. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014

HARBEMAS. *Direito e Democracia:* entre facticidade e validade, vol. I/ J***ü***rgen Habermas. Trad. Flávio Beno Siebeneicher. Rio de Janeiro: Ed. Tempo Brasileiro, 1997

G1.Entenda o caso de Edward Snowden que revelou espionagem nos EUA. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. São Paulo, 02/07/2013, 14h25 - Atualizado em 14/02/2014 07h29Acesso em 01 junho. 2021.

G1. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC News. {S.l.], 20/03/2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml, 07h29 Acesso em 01 junho. 2021.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

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

MOLINA, Letícia Gorri; SANTOS, Juliana Cardoso dos. **Gestão da Informação e a 4a Revolução Industrial.** Novas práticas em informação e conhecimento, 8(2), 39 – 48, 2019. Disponível em: https://revistas.ufpr.br/atoz/article/view/65784. Acesso em: 19 mai. 2021

POLIDO, Fabrício B. Pasquot et al. *GDPR e suas repercussões no direito brasileiro:* Primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade, 20 jun. 2018. Belo Horizonte: Iris, 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-nodireito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf>. Acesso em: 19 mai. 2021

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradutores Danilo Doneda e Luciano Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHWAB, Klaus. *A quarta revolução industrial.* Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016,

SIMÃO FILHO, A.; SCHWARTZ, G. A. D. Big Data em tempos de internet das coisas. In: PARENTONI, L.; GONTIJO, B.M.; LIMA, H.C.S. *Direito, Tecnologia e Inovação* . Belo Horizonte: D'Placido, cap. 2.2, p. 217-246. v. I. 2018

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 32 ed. Sâo Paulo, Malheiros, 2009.