ISSN 1982-0496

A PROTEÇÃO DE DADOS SENSÍVEIS NO SISTEMA NORMATIVO BRASILEIRO SOB O ENFOQUE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – L. 13.709/2018

THE PROTECTION OF SENSITIVE DATA IN THE BRAZILIAN NORMATIVE SYSTEM UNDER THE FOCUS OF THE GENERAL DATA PROTECTION LAW (LGPD) – L. 13.709 / 2018

Gabrielle Bezerra Sales Sarlet

Pós-Doutora em Direito pela Universidade de Hamburgo- Alemanha (2019) e igualmente pela Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS (2018). Doutora em Direito pela Universidade de Augsburg-Alemanha (2013). Mestre em Direito pela Universidade Federal do Ceará-UFC (2002). Especialização em Neurociências e Ciências do Comportamento (2020) Pesquisadora visitante e bolsista do Max-Planck-Institut für ausländisches und internationales Privatrecht - Hamburg-Alemanha (2018), Professora do curso de graduação e no PPGD em Direito da Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS.

Regina Linden Ruaro

Pós-Doutora pela Universidad San Pablo - CEU de Madri (2008). Doutora em Direito pela Universidad Complutense de Madrid (1993). Professora titular e Decana Associada da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS. Lidera o Grupo de Pesquisa cadastrado no CNPq: Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação no Estado Democrático de Direito. Advogada e Consultora na Área de Proteção de Dados Pessoais.

Resumo

Consiste em pesquisa bibliográfica e exploratória acerca dos institutos do ordenamento brasileiro que tocam à proteção de dados pessoais, especificamente ancorada na Lei Geral de Proteção de dados(LGPD), voltando-se para os dados sensíveis em razão do seu potencial discriminatório e, nesse sentido, para o reconhecimento de um direito

DOI: 10.25192/issn.1982-0496.rdfd.v26i22172

fundamental ao tratamento apropriado das informações imprescindíveis para a estruturação, para a proteção da identidade e para o livre desenvolvimento da personalidade da pessoa humana no contexto informacional tendo em vista a preservação do regime democrático.
PALAVRAS-CHAVE: Consentimento Informado. Dados Sensíveis. Direitos humanos e fundamentais. Identidade digital. Privacidade. Proteção de dados pessoais

Abstract

It consists of bibliographical and exploratory research about the Brazilian law system that deal with the protection of personal data, specifically anchored in the General Data Protection Law (LGPD), turning to sensitive data due to their discriminatory potential and, in this sense, for the recognition of a fundamental right to the appropriate treatment of the information essential for structuring, for the protection of identity and for the free development of the personality of the human person in the information context with a view to preserving the democratic regime.
KEY WORDS: Informed consent. Sensitive Data. Human and fundamental rights. Digital identity. Privacy. Protection of personal data

1. CONSIDERAÇÕES INICIAIS

Atualmente há uma inconteste hipertrofia (HENNING, 2019, p. 137) do ambiente digital/virtual (SCHMIDT; COHEN, 2014). Na sociedade informacional, importa ressaltar de antemão, os limites da vida privada têm se fragilizado, sobretudo em razão da infinidade de dados pessoais postados nas redes sociais e, consequentemente, da produção irreflexiva de pegadas/rastros digitais. Esse ambiente virtual/digital se constitui como um espaço compartilhado (ZENNER, 2018, p. 117), ou seja, implica em uma forma de participação instantânea.

É neste ambiente[1], ao qual também pode ser chamado de "meio ambiente digital/virtual", em que se inserem os dados pessoais coletados, produzidos e transferidos pelos indivíduos (KROHM , 2012, p. 19-20). Dito de outro modo, trata-se de um ambiente permeado pela Volatilidade, pela Incerteza, pela Complexidade e pela Ambiguidade. Devendo-se ressaltar que os dados pessoais, em suma, consubstanciam a vida das pessoas humanas atualmente.

[1]"**O ciberespaço** (que também chamarei de 'rede') é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo (LÉVY, 2008. p 17).

Com efeito, a contemporaneidade aponta para uma tendência de sociedade estruturada sob a forma de rede, gerando infinitas oportunidades de controle e de vigilância em dependência radical das redes de informação; volumes excessivos de informação em proporção ao decréscimo da produção de conhecimento; hiperaceleração e hiperexposição (GRABOSCH, 2019, p. 27-29).

A introdução desse modelo informacional alterou a gramática cultural da sociedade de forma radical na medida em que suas estruturas foram transformadas e, assim, foram engendrados novos comportamentos, tornando mais complexos os outrora conhecidos e, simultaneamente, encetando novos conceitos, novas demandas e conflitos ainda isentos de exaustiva e de apropriada regulamentação jurídica em razão de seu vanguardismo.

A segurança e a proteção do indivíduo no âmbito digital, no que afeta aos inúmeros usos dos dados pessoais e, de modo especial, no contexto da internet, ainda carece de maior atenção no Brasil, muito embora já se tenha desde 2014 um marco civil que, dentre outros pilares, expressamente previu como princípio estruturante a privacidade, delegando, no entanto, a proteção de dados pessoais a uma legislação específica que se concretizou por meio da promulgação da Lei Geral de Proteção de Dados, Lei 13.709/2018 (doravante LGPD), atualmente em *vacatio legis*.

Não se pode desconhecer que, curiosamente, o meio ambiente virtual apresenta facetas muito singulares, vez que as suas dimensões não se circunscrevem ao espaço e tampouco ao tempo. Outro aspecto relevante encontra-se diretamente relacionado com a capacidade de avanço e de incremento da tecnologia e, dessa maneira, deve ser considerada a impermanência desse ambiente, pois constantemente se altera o próprio conceito de dados pessoais, sobretudo quando se analisa as condições e os graus de identificabilidade que mudam rapidamente em razão de novos modos de armazenamento, de tratamento e de reidentificação dos dados.

Com efeito, as tecnologias de informação e de comunicação (vulgo TIC) estão em todas as áreas, forjando um panorama atual em que as corporações privadas se sobrepuseram em relação à atuação dos Estados. Deste modo, elas encetaram algumas situações que consistem em uma dinâmica de desobrigação do ser humano de decidir sobre sua vida cotidiana e, assim, quanto maior a desobrigação, mais afetada resta a capacidade de refletir, de anuir, de deliberar, ou seja, de uma atuação consciente e emancipada, sequer responsável.

Um dos principais desafios que se impõe, portanto, é a análise do giro copernicano imposto pela realidade aumentada, pela virtualização, pela personificação de robôs e de avatares, pela invenção de novas trocas simbólicas, pela superexposição da vida privada nas redes sociais, pelo excesso de informações, em particular de informações pessoais de caráter identitário e a consequente discriminação algorítmica (MENDES, 2019, p. 39), pela

reestruturação das transações comerciais e pela necessidade de respostas rápidas e precisas que não encontram precedente algum na civilização ocidental e que determinam o apelo inclusive por uma nova modalidade de juridicização, ou seja, advindos inclusive dos reflexos da digitalização da identidade (LE BRETON, 2018, p. 65) e, consequentemente, demandam um redimensionamento da efetiva proteção da personalidade no ambiente digital.

Emerge, nesses termos, uma nova qualidade de atenção voltada para as exigências do campo da ética, da filosofia dos valores e para a garantia de *compliance*. Para uma melhor apreciação do estado da arte, deve-se, todavia, realçar a possibilidade de uma espécie de *algoritmização (*HOFFMANN-RIEN, 2019, p. 16-18) [2] da realidade cotidiana e, consequentemente, do vasto potencial discriminatório de sua utilização em conjunto com Inteligência artificial e *Big Data*.

Em rigor, os algoritmos são, de fato, imprescindíveis para a contemporaneidade, ou seja, se prestam para a tomada de decisões com base na produção de prognósticos produzidos a partir do cálculo de probabilidades, particularmente quando se refere ao grandioso volume das comunicações via internet. Quanto à ontologia dos algoritmos, deve-se advertir que consistem em discursos em linguagem digital, isto é, se expressam em uma estrutura definida e mecanicamente processável (MENDES, 2019, p. 42-43).

Na contemporaneidade cada vez mais os algoritmos influenciam as decisões enquanto precarizam mais ainda o conhecimento da realidade mediante a filtragem de informações, atuando na manutenção ou na alteração do *status quo* na medida em que se prestam ao papel de postes/postos de vigilância e, em igual intensidade, têm sido empregados na criação de novos produtos, de serviços e na produção de *scores* amplamente aplicados, enquanto transmutam e afetam a efetivação das garantias elementares dos direitos humanos e fundamentais (OTTO Y PARDO, 1988, p. 110).

Relevante ainda mencionar o padrão atual de crescente emprego de *Big Data* que, em rigor, persiste ainda como uma espécie de ponto cego no sistema protetivo, ou seja, no mosaico legal brasileiro apesar da nova legislação. *Big Data*, não custa rememorar, é em um conceito primordial na atual conjuntura. Consiste, em suma, em um bloco algorítmico emulado para o tratamento de grandes quantidades de dados, que visa reconhecer padrões e obter novas percepções a partir deles, caracterizando-se pela abundância, pela diversidade de dados e pela rapidez com que são coletados, analisados e reintroduzidos no sistema (SALES; MOLINARO, 2019, p. 188).

Oportuno afirmar que em razão dos riscos, da irreversibilidade e, em particular, do grau

[2]O autor esclarece, a partir do conceito e do atual emprego dos algoritmos, um modelo de governança, inclusive orientando que se trata de uma prática de estabelecer políticas, procedimentos e padrões para o desenvolvimento da chamada infosfera, sobretudo levando em conta uma perspectiva ética *(*HOFFMANN-RIEN, 2019, p. 16-18).

da vulnerabilização das pessoas torna-se imprescindível a proposição de parâmetros jurídicos com intuito de, sobretudo, garantir a coexistência da eficácia dos direitos humanos e fundamentais (SARLET, 2017, p. 405-406) constitucionalmente consagrados, compatibilizando-os entre si, vez que resultaram de um longo processo histórico para a sua afirmação. E, nestes termos, recai um enfoque redobrado sobre os dados pessoais sensíveis.

O presente artigo é, dessa maneira, fruto de uma análise científica, mediante emprego de pesquisa bibliográfica e exploratória, acerca dos institutos (SILVA, 2014, p. 130) jurídicos já existentes no ordenamento brasileiro que tocam ao direito à proteção de dados, trabalhando com a atenção voltada para os dados sensíveis e, nesse sentido, para o tratamento de informações imprescindíveis para a estruturação e para a proteção da identidade (ECHTTERHOFF, 2010, p. 42) e, de modo mais geral, do livre desenvolvimento da personalidade da pessoa humana no contexto informacional sob o enfoque da LGPD.

Reafirma-se a imprescindibilidade do princípio da responsabilidade quando se trata dessa temática. Com base na revisão literária realizada até o presente estágio da investigação, já se pode antever que, no meio ambiente digital/virtual, em específico no que afeta ao tratamento de dados sensíveis, torna-se igualmente elementar a aplicação dos princípios da precaução[3] e da prevenção como pilares de uma constelação jurídica que tem como vetor primordial a proteção da dignidade da pessoa humana, dentro e fora do ambiente digital.

De todo modo, pretende-se empreender uma reflexão tendo-os como base para analisar a LGPD e, em razão disso, tangenciar a noção de privacidade, de governança algorítmica e das formas de anonimização de dados, para então revisitar o conceito de consentimento livre, informado e esclarecido no intuito de encetar uma percepção ampla e factível dos dispositivos legais no panorama atual (CASTELLS, 1999 p. 21). Diante disso, urge relembrar que a proteção de dados pessoais é, em síntese, a proteção da pessoa humana, mormente quanto ao resguardo do livre desenvolvimento de sua personalidade e, em particular, por meio da centralidade da garantia da sua autodeterminação informacional consoante o artigo 1º da LGPD.

2. A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS

A Finalidade, a Adequação, a Necessidade, o Livre acesso, a Qualidade dos dados, a Transparência, a Segurança, a Prevenção e a Não Discriminação permeadas pelo princípio

[3]No que concerne ao princípio da precaução, ele está previsto no artigo 1º da Lei de Biossegurança – 11.105/05, onde está expresso sua conexão com o meio ambiente. Vê-se que o princípio da precaução compõe o sistema jurídico no meio ambiente físico. O princípio da precaução vincula a ação humana não só com o presente, mas também com o futuro, atua prospectivamente.

da boa-fé, perfazem a constelação principiológica da LGPD que, por óbvio, é emoldurada pelos princípios constitucionalmente previstos pela Carta de 1988 e se ampara em instrumentos jurídicos previstos em outras searas, para além do direito digital, como a civil, a penal e a consumerista. Assim, em uma análise mais pormenorizada dos dispositivos desse instrumento legal, podem ser apontados como desdobramentos do direito à proteção de dados, dentre outros, os direitos: ao livre acesso, à qualidade dos dados, à transparência, à segurança, à prevenção e à não discriminação.

A promulgação dessa lei colocou o Brasil no rol de mais de 100 países que hoje podem, em certa medida, serem considerados adequados para proteger a privacidade e o uso de dados, vez que possuem institutos voltados para essa área sendo que, em regra, estão integrados aos demais países que atuam em rede, inclusive no que afeta às cautelas em relação à transferência de dados no contexto mundial. A LGPD cria uma regulamentação para o uso, para a proteção e, notadamente, para a transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são as suas atribuições, as responsabilidades e as penalidades no âmbito civil – que podem chegar a multa de 50 milhões de reais em decorrência de algum incidente ocorrido.

Em linhas gerais, a LGPD assegura a integralidade da proteção à pessoa humana na medida em que consagra a obrigatoriedade do gerenciamento seguro do início até ao fim da operação que envolve os dados pessoais. Importa salientar que o resguardo dos dados pessoais, particularmente os dados sensíveis, embora inicialmente tomados como personalíssimos, nunca tem apenas uma dimensão individual, vez que estão intrinsecamente atrelados ou podem ser atrelados aos dados de outrem.

De acordo com o artigo 5º, I e II, da LGPD, os dados pessoais são, então, em princípio, todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular, enquanto os dados sensíveis são aqueles que, à guisa de exemplo, tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos. Os dados sensíveis são, em vista disto, nucleares para a prefiguração e para a personificação do sujeito de direito no contexto atual[4].

O conjunto dessas informações[5] compõe os perfis ou as identidades (MURAT, 2015,

[4]Segundo Castells, “no informacionalismo, as tecnologias assumem um papel de destaque em todos os segmentos sociais, permitindo o entendimento da nova estrutura social – sociedade em rede – e consequentemente, de uma nova economia, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos”, pois “a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder”. De sorte que a informação passou a ser a matéria prima mais valiosa (CASTELLS, 1999, p. 21).

[5]EXEMPLOS DE DADOS DISPONIBILIZADOS – desde os dados que perfazem o registro civil, resultados de exames médicos, dados fornecidos em consultas, regularidade de consultas médicas, frequência e especificidade de exames e de procedimentos clínicos, dados escolares, históricos

p. 52) digitais, possuindo valor político e, sobretudo, econômico, vez que podem ser a matéria prima (JÖNS, 2016, p. 18) para as novas formas de controle e, assim, de poder social, especialmente mediante o uso de algoritmos, de inteligência artificial e de *Big Data*.

Os perfis são composições, ou melhor dizendo, são mosaicos compostos pelas informações fornecidas pelos usuários em uma formatação igualmente constituída e circunstanciada pelo que é consciente e livremente disponibilizado e pelo que advém das pegadas digitais, dos cruzamentos e dos vazamentos de dados. Importa relembrar que o que caracteriza o dado como sensível é a possibilidade de ser utilizado de modo discriminatório e, dessa forma, há de se reconhecer que o manejo/tratamento desses dados pode expressar uma afetação direta à pessoa humana.

Assim, e.g., em virtude do uso frenético de drones, de câmeras digitais, de senhas eletrônicas, torna-se praticamente impensável traçar um modelo fechado para as fronteiras de qualquer identidade digital e, nessa medida, torna-se muito imprecisa e, de certa maneira, anacrônica a forma atual de se pensar a proteção da pessoa humana em um panorama que tende a se alterar em virtude da implantação de novos paradigmas de rastreamento e de identificabilidade advindos com a internet 5.0 e com o acirramento do emprego de *Big Data* e, mais recentemente, do uso dos computadores quânticos[6].

No que toca aos dados sensíveis, reafirma-se a exigência de uma proteção especial[7]

universitários, histórico de compras em cadeias de lojas virtuais e não virtuais, consumo por meio de aplicativos, assinaturas de periódicos, dados bancários, dados fornecidos à receita federal, dados obtidos no departamento de trânsito, da polícia, dos cartões de crédito, histórico de páginas visitadas, participação em enquetes virtuais etc.

[6]Um **computador quântico** é um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como sobreposição e interferência. Teoricamente, **computadores** quânticos podem ser implementados e o mais desenvolvido atualmente, o D-Wave Two, trabalha com 512 qubits de informação (VELASCO, 2019).

[7]Da aplicabilidade dos princípios da precaução e da prevenção em um esquadro de responsabilidade no meio ambiente virtual/digital. Destaque-se que a lógica no meio ambiente virtual/digital migra do indivíduo para o coletivo. Ademais, como o ciberespaço funciona com uma dinâmica diferente que lhe é característica, a cada dia o cotidiano se alarga em autonomia, desenvolvendo-se em diferenciações que se afastam do meio ambiente físico (mundo real). Observa-se que, em rigor, uma espécie de dialética se estabeleceu em dois universos paralelos baseados na exploração e na exposição e, assim, em uma composição que metamorfoseia o universo contemporâneo em algo híbrido, meio real e meio virtual. Não se pode olvidar nesta altura que a ideia de risco e de impacto advindas dessa nova composição implica em responsabilidade, ou seja, na responsabilidade enquanto obrigação de responder pelo dano produzido, tenha este como origem uma causa natural ou antrópica. Responsabilidade que, mesmo em situações como atual em que o contexto se encontra eminentemente permeado da atuação de grandes gigantes tecnológicos, reclama a decidida intervenção dos poderes públicos, não apenas restrita a uma orientação reparadora, mas de prevenção, de precaução, de redução e, no possível, de eliminação dos riscos. Neste viés torna-se cada vez mais imprescindível a qualidade da regulação e as suas possibilidades factíveis de efetividade social. Com efeito, estabelece-se como hipótese, oportunamente, o valor da aplicação dos princípios da precaução e da prevenção nesse domínio da sociedade informacional, disruptiva. Entende-se que esses devam ser a base da atuação e da estruturação de uma espécie de Governança algorítmica que, por sua vez, deve engendrar uma principiologia própria e especificamente voltada para os contornos do mundo virtual

alicerçada no princípio da dignidade da pessoa humana, cuja fundamentalidade ainda radica e sustenta a própria ideia contemporânea de democracia e o atual molde de Estado de Direito (HABERMAS, 2012, p. 37). Este reforço antropológico encontra amparo, e.g., no artigo segundo do Tratado da União Europeia, no qual se consagra, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos humanos (UNIÃO EUROPEIA, 2019). E foi da experiência europeia, mais especificamente, do protagonismo alemão nessa área que remonta aos anos setenta do século passado, que adveio o legado quanto à proteção de dados nos moldes atuais[8] e, nesse sentido, o seu reconhecimento como um direito humano e fundamental.

O emblemático caso Snowden, e.g., culminou na edição da Resolução da ONU de 25 de novembro de 2013 "Direito à privacidade na era digital" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2020). Assim, na 34ª sessão do Conselho de Direitos Humanos das Nações Unidas (CDH), em 21 de novembro de 2016, foi aprovada a resolução sobre o direito à privacidade na era digital, projeto apresentado pelo Brasil, em conjunto com a Alemanha, dentre outros Estados. A resolução reafirma o direito à privacidade conforme previsto na Declaração Universal de Direitos Humanos e no Pacto Internacional de Direitos Civis e Políticos. O documento do CDH conclama os Estados a respeitar e a proteger o direito à privacidade, a pôr fim às violações, a prover medidas efetivas de reparação e a assegurar que qualquer restrição ao direito à privacidade deverá respeitar os princípios da legalidade, da necessidade e da proporcionalidade. Restou ainda salientada naquele documento a paridade do alcance dos direitos humanos consagrados tanto na realidade física quanto na realidade virtual.

sem descuidar do elemento intrínseco à confiabilidade dos sistemas que é a responsabilidade. Relativamente ao princípio da prevenção, este se diferencia do princípio da precaução, vez que "reside no grau estimado de probabilidade de ocorrência do dano (certeza *versus* verossimilhança)". Conveniente é relembrar que o princípio da prevenção, ainda que não esteja expresso em nomenclatura, está previsto implicitamente na Declaração de Estocolmo sobre o Meio Ambiente Humano de 1972.Enquanto no princípio da precaução não se tem conhecimento completo sobre os efeitos que podem resultar de determinada técnica de pesquisa, de sua utilização, armazenamento e transferência de dados, no princípio da prevenção já se pode antever o resultado. No princípio da prevenção tem-se a "verdade sabida" e o potencial lesivo já é conhecido. Pelo princípio da precaução, não se tem como seguro de que haverá impacto, mas se pode vislumbrar a existência de um problema desta ordem o que caracteriza um dos pressupostos para a aplicação do princípio da precaução. É claro que as medidas de precaução devem ser tomadas na presença de temores razoáveis sob pena de provocarem limitações desastrosas e, assim, produzir uma certa paralisia herética e absolutamente irrealizável em relação aos dados pessoais, em particular em relação aos dados sensíveis. Com efeito, as degradações do meio ambiente, incluindo sobremaneira as advindas do meio ambiente digital/virtual, atingem a sustentabilidade existencial, implicando em danos que podem afetar os seres humanos em sua essência psíquica, emocional etc., a dizer, em sua integralidade. E por isto são tão graves, vez que envolvem riscos e impactos legais, éticos, patrimoniais e, de modo geral, riscos sociais incalculáveis e ainda imprevisíveis.

[8] Doneda esclarece as diversas ondas em que se inscreveu a atual ideia de um sistema normativo de proteção de dados (DONEDA, Danilo, 2019, p. 172).

2.1. Da identidade digital

Atualmente os computadores e os sistemas de informação, de codificação e de tratamento de dados passaram a ser entendidos como extensão da pessoa humana, particularmente no sentido de forjar identidades (FUKUYAMA, 2020, p. 131) digitais[9].

Elas consistem em um conjunto de informações transformadas em *bits* ou em *pixels* que representam uma pessoa humana, podendo ser utilizadas na relação com as máquinas ou com os outros usuários, e.g., *passwords,* dados sobre reconhecimento da face, da voz, da íris, das impressões digitais. A identidade digital, diga-se, não deve ser confundida com o Protocolo de Internet (IP) que, de fato, diz respeito à conexão e não à máquina, ou seja, por meio dele é possível rastrear uma conexão que se formou em um momento bem estrito, pois se encontra inserido na *Uniform Resource Locator* (URL).

Nesse sentido, enfatize-se que a adjetivação pessoal, inclusive quando se trata de dados, diz respeito à singularização da pessoa humana face aos demais, sendo, pois, uma forma de diferenciação da pessoa que pode ser extensível aos bens. Os dados, nessa medida, assumem agora uma indiscutível proeminência em relação ao tema da identidade e, em decorrência, da proteção à personalidade.

A propósito, esse mosaico identitário não consiste somente nos dados espontaneamente fornecidos, mas é igualmente extraído das pegadas ou das sombras digitais, a dizer, do histórico de todas transações efetuadas pelo usuário que formam os registros dos sites e dos portais de acesso à internet. Proporcionais ao uso que se faz da internet, as sombras ou pegadas digitais incluem as imagens em câmeras de vigilância, os dados advindos das movimentações bancárias, das ligações telefônicas, das informações, dos diagnósticos e dos prontuários médicos, das cópias de scanners e de exames hospitalares, das informações de crédito, do histórico de compras e de condenações, sobretudo as penais. A identidade digital consiste, em síntese, na plêiade de todas as informações que podem ser acessadas nos *Datacenters*.

O sistema civil de tutela da pessoa humana, por sua vez, passa necessariamente pelo inadiável enfrentamento das transformações do conceito de identidade que, a princípio, era entendido em uma perspectiva individual e não como um bem ou um valor, ou seja, como uma síntese biográfica produzida em uma nova dimensão relacional que produz inclusive um patrimônio de natureza imaterial, seja ele intelectual, ideológico, ético, religioso, sexual e profissional[10].

[9]Der Mensch, nicht seine Daten, steht also im Mittelpunkt.“ Cf. KNOBLOCH, Hans-Heinrich. Der Schutz der Persönlichkeit im Internet (LEIBLE; KUTSCHKE, 2019, p. 13).

[10] O art. 5 da LGPD esclarece que dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável, tendo por dado sensível aqueles que tratem sobre origem racial ou

Desse modo, atualmente requer uma ampla reformulação no feixe de direitos e de garantias de forma que correspondam à proteção da personalidade no âmbito da sociedade informacional, mas que, com redobrada ênfase, atentem para os aspectos referentes ao uso dos dados pessoais, aos bens digitais[11] e aos inauditos aspectos sucessórios. Há, dessa maneira, uma elaboração que vai além dos contornos do direito à privacidade e que, por sua vez, toca em aspectos como o direito à revisão de decisões automatizadas, implicando necessariamente em uma relação, mais fidedigna quanto possível, entre os dados e a pessoa humana, isto é, em uma composição tanto clara quanto transparente em termos de garantia do direito de acesso, de revisão e de retificação.

A tutela da identidade se desdobra, consequentemente, em, no mínimo, dois aspectos, ou seja, em uma proteção da identidade pessoal propriamente dita que visa ao livre desenvolvimento da personalidade, como honra, reputação, imagem, dentre outras e na necessária proteção face às atuais técnicas de identificação do sujeito, ou seja, aos novos delineamentos da identidade advindos do tratamento dos dados pessoais. Não custa mencionar que sendo parte da tessitura de direitos da personalidade, o direito à identidade é, em geral, premissa básica para a atual configuração do Estado Democrático de Direito e, portanto, garantido mundo afora por inúmeras cartas constitucionais e pela Constituição Federal de 1988.

Nessa altura, importante esclarecer que, de acordo com a LGPD, o conceito de dado pessoal é entendido em uma perspectiva alargada na medida da identificabilidade, atrelando-a ao conceito de dados anônimos e, consequentemente, às técnicas de anonimização, vez que há um reforço no teor dessa lei quanto à ideia de que a informação é um fruto do processo de tratamento dos dados.

De fato, o que caracteriza um dado como pessoal é, sem dúvida alguma, entendido a partir da relação entre o contexto, o uso e a qualidade da tecnologia empregada. Não há, dessa forma, uma radical metodologia de anonimização total, vez que toda parametrização pode ser alvo de engenharia reversa.

As principais técnicas são a supressão, a generalização, a randomização e a pseudoanonimização, tendo em vista sempre a noção de quebra da vinculação entre o dado

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.

11 E o que são bens digitais? São todos bens incorpóreos (imateriais), existentes no meio digital. Dentre os principais exemplos, destacam-se: acervos que incluem textos, base de dados, imagens, áudios, gráficos, planilhas, criptomoedas, softwares, páginas de internet, perfis em redes sociais, ideias, entre outros. Muitos desses recursos têm valor e significância, constituindo, assim, uma herança que deve ser protegida e preservada para presentes e futuras gerações. Inclusive, de acordo com a UNESCO, o patrimônio digital é tão importante que sua sucessão pode chegar a desconsiderar laços sanguíneos e/ou afetivos e se tornar um instituto autônomo, denominado de "patrimônio mundial", composto por sites de valor cultural e natural.

e a pessoa. A ideia primordial é tornar o vínculo, na medida do possível, mediato, inexato e impreciso. Assim, o que se têm, na realidade, é uma espécie de gerenciamento contínuo da identificabilidade das bases de dados. Todo processo de anonimização, conveniente reconhecer, é circunstancial e precarizado em face do desenvolvimento de novas técnicas, tratando-se de um mito que se impõe de uma maneira geral para o engendramento da proteção sistemática da pessoa na sociedade informacional e que exige uma atenção redobrada e contínua, em particular quando se tem em vista a criação de algoritmos para a desanonimização de bases de dados pessoais, inclusive sensíveis.

Interessa salientar que, em face dos processos de agregação de bases de dados e, portanto, de reidentificação, qualquer dado anonimizado é, em regra, um dado pessoal e, assim, as formas de discriminação podem igualmente sofrer alterações profundas, inclusive por vezes se tornando sutis e imperceptíveis ao cidadão comum. Oportunamente, deve-se clarificar que o termo identificável é, em regra, superável, tendo sido recepcionado pela LGPD no que diz respeito às formas de expressão da razoabilidade, ou seja, ao nível de investimento de tempo e de dinheiro envolvidos no processo de anonimização. De toda sorte, a pseudoanonimização, não custa mencionar, constitui um meio termo entre o dado pessoal e o dado anomizado.

De fato, entende-se, em concordância com o que a LGPD dispõe, que, em especial em situações como as que tocam ao âmbito da proteção de dados pessoais sensíveis, no processo de anuência as informações devem ser previamente esclarecidas em linguagem clara, precisa, apropriada e suficiente, mormente quanto à pertinência, à finalidade, à adequação, ao tempo da coleta, às modalidades de armazenamento, ao tratamento e à transmissão dos dados obtidos. E, em princípio, devem possibilitar a renúncia, a alteração, o uso, a cessão, e a disponibilidade ou a recusa daquele que consente.

Afirma-se, dessa maneira, o protagonismo do sujeito na condução e na construção de sua própria vida. Importando, nesses termos, garantir ainda a proteção contra os riscos de danos materiais e imateriais, e.g., em casos de criação de perfis falsos, de violação da privacidade de modo geral, de retenção e de manipulação de dados, de estigmatização, de discriminação (ALMEIDA, 2020, p. 53-54), direta ou indireta por meio de cadastros, de manipulação de dados, de emprego de algoritmos que forjam um cruzamento de dados e de *Big Data*.

Inadmite-se, portanto, qualquer limitação injustificada aos direitos da personalidade, mais especificamente quanto aos contornos do direito à identidade, na medida em que se trata de parte irrenunciável na composição do conceito de personalidade que, por sua vez, se encontra aferrado ao de dignidade. Com isso, entende-se pela necessidade de uma regulação apropriada ao meio virtual para a garantia do direito à proteção de dados sensíveis, impedindo que os sistemas de tratamento de dados e, consequentemente, os algoritmos sejam utilizados

para enganar, manipular, condicionar ou agrupar as pessoas humanas em franca violação a sua condição de sujeitos de direito.

Quanto às técnicas de anonimização, deve-se apontar para a estruturação clara de um pacote/programa de governança digital que vise efetivamente reduzir e minimizar os riscos e os impactos de incidentes de segurança, em especial no que concerne ao compartilhamento e ao cruzamento de dados.

Assim, os algoritmos devem servir, em regra, para a emancipação e, assim, para aumentar, complementar e capacitar as habilidades cognitivas, sociais, éticas e culturais dos seres humanos. Nesse ponto, oportunamente, entra em cena o debate sobre os limites da governança digital relacionada à responsabilidade algorítmica, que, em rigor, não será tratado direta e nem profundamente nesse artigo apesar de sua extrema significância.[12]

Entende-se, de toda sorte, que o papel apropriado ao sujeito de direito no âmbito digital/virtual implica por um lado em uma atitude responsável com relação à exposição de si e com a disponibilização de seus dados sensíveis na internet como parte de um exercício de cidadania e, por outro, implica igualmente em uma ação conjunta de caráter interventivo partindo dos setores público e privado (DETERMANN, 2015, p. 12-13) para a garantia da democracia digital.

2.2. Da privacidade à proteção dos dados pessoais sensíveis em face da dignidade da pessoa humana

A princípio, pode-se esboçar a ideia do fim da privacidade, melhor dizendo, o fim da sua tradicional acepção. De todo modo, uma abordagem arqueológica desse direito inexoravelmente remete ao artigo publicado por Samuel D. Warren e Louis D. Brandeis, em dezembro de 1890, na *Harvard Law Review*, intitulado *The Right to Privacy,* no qual os autores defendem que “o direito à vida passou a significar o direito de aproveitar a vida, -- o direito de ser deixado só”.[13]

O estudo é tido como um marco do surgimento desse direito no âmbito teórico-jurídico. Em outras palavras, os autores enfatizaram a necessidade de se proteger da constante ameaça à privacidade e, nesse sentido, afirmaram-na como um agravo à personalidade (WARREN; BRANDEIS, 2015) O grande avanço desse estudo foi o de ensejar a migração do direito à privacidade, que antes se encontrava no âmbito dos direitos reais para o âmbito dos direitos pessoais. A propósito, deve-se salientar que o direito à privacidade, sobretudo na composição com o direito à identidade, está diretamente relacionado à dignidade da pessoa

[12]Preocupada com a questão, a União Europeia instituiu um Comitê Específico para estudo da matéria (EUROPEAN COMISSION. 2020).

[13]“[…] the right to life has come to mean the right to enjoy life, -- the right to be let alone” (WARREN; BRANDEIS, 2015).

humana (SARLET, 2017). O direito à privacidade, é tutelado no artigo 5º, inciso X da Constituição Federal brasileira, estando inserido no rol dos direitos de personalidade. Assim, a "esfera individual" é inerente à honra e diz respeito ao nome, à reputação e à imagem do titular. A esfera privada se refere à individualidade e, pois, a não intromissão externa na intimidade do titular, garantindo um certo isolamento do ser humano frente a seus semelhantes (VIEIRA, 2007, p. 22).

Personalidade, destarte, inclui em sua estruturação, um processo em que o indivíduo supera etapas com a intenção de reconhecer o ser-humano em si e no outro. Em rigor, ser-pessoa é uma experiência integradora e deve, portanto, ser entendida além de uma síntese proteica, projetando-se em uma composição de essência (incluindo estrutura e relação) e de existência (autorrealização intersubjetiva mediada e possibilitada). Trata-se, portanto, de uma categoria que expressa tanto a interioridade (relação para dentro) quanto a exterioridade (relação para fora) da pessoa humana. Em suma, pode-se trabalhar com uma esfera social-individual e em outra dimensão, com uma esfera privada. Os atos inerentes a primeira esfera (*Individualsphäre)*, dizem respeito a comportamentos abertos – aqueles facilmente perceptíveis e valorados – do indivíduo (COSTA JR, 1970, p. 24).

Com efeito, tal esfera confunde-se com o direito à honra propriamente dito, protegendo o titular contra diversos tipos de agravos e, consequentemente, de danos.

Em contraposto, a esfera privada abarca os chamados comportamentos encobertos que o indivíduo pretende manter a par do conhecimento e da interferência alheia, (HENKEL, 1970, p. 24-25) ou seja, diz respeito ao direito à privacidade[14]. E é justamente neste tópico que se inserem os dados pessoais, notadamente os dados sensíveis que, em regra, têm sido considerados como *commodities* no panorama contemporâneo a despeito de sua relevância, vez que são geralmente irrenunciáveis e se encontram atrelados de modo insuperável à identidade pessoal. Assim, a respeito da vedação ao emprego discriminatório que se fizer deles há sempre que se dedicar uma atenção redobrada.

Importa salientar, de toda sorte, que a privacidade ainda que em franca reconfiguração no sistema jurídico e na vida cotidiana, pode ser dividida em diferentes categorias: (a) privacidade física – proteção contra procedimentos invasivos não autorizados como exames genéticos ou testes de drogas; (b) privacidade do domicílio – é aquela prevista no artigo 5º, inciso XI da Constituição Federal que dispõe: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"; (c) privacidade

[14]"O direito à privacidade consistiria em um direito subjetivo de toda pessoa – brasileira ou estrangeira, residente ou transeunte, física ou jurídica – não apenas de constranger os outros a respeitaram sua esfera privada, mas também de controlar suas informações de caráter pessoal – sejam estas sensíveis ou não – resistindo às intromissões indevidas provenientes de terceiros" (VIEIRA, 2007. p. 30).

das comunicações – também encontra respaldo constitucional (art. 5, XII); (d) privacidade decisional ou direito à autodeterminação – consiste no poder de decisão do indivíduo. E, por fim, (e) privacidade informacional ou autodeterminação informativa (VIEIRA, 2007, p.31-33).

Partindo dessa noção, é que se pode abordar esse tema, acrescendo outras perspectivas e, portanto, atribuindo aos espaços de privacidade a esfera da autonomia, a esfera das informações pessoais, a esfera da propriedade pessoal e a esfera do espaço físico, isto é, em uma abordagem mais complexa. Isto posto, evidencia-se que a esfera da autonomia privada atrela a privacidade às questões de identidade e de liberdade pessoal, inclusive no que use refere aos aspectos da liberdade de expressão e religiosa, dentre outras.

A esfera das informações pessoais toca diretamente no direito à autodeterminação informativa e, portanto, na privacidade informacional. No que diz respeito à ideia de soberania dos dados pessoais, não se deve olvidar que o âmbito da propriedade pessoal está vinculado às questões como propriedade (privada), posse, disposição do bem e outros aspectos dos direitos das coisas. Por fim, no tocante ao espaço físico visa o respeito ao espaço pessoal, prescindindo da noção de propriedade para que seja respeitado, nos EUA, tal esfera é tutelada pela *Tort Law (*MILLS, 2019).

No que respeita à proteção de dados pessoais, mormente os dados sensíveis, esse feixe de direitos veem consubstanciados na Constituição Federal em diversos dispositivos, mas, mais especificamente, em seu artigo 5º, inciso XII, e está, embora em termos gerais, reforçado pela consagração do *habeas data.*[15] A delimitação de um direito fundamental autônomo e implícito no sistema normativo brasileiro implica em uma compreensão que envolva o direito de acesso e de conhecimento dos dados pessoais existentes em registros (banco de dados) públicos e privados; o direito ao não conhecimento, ao tratamento e à utilização e à difusão de dados pessoais, particularmente no que concerne aos dados sensíveis pelo Estado ou por terceiros. Inclui-se, de toda maneira, um direito de sigilo quanto aos dados pessoais.

Mas, se reconhece um caráter extensivo ao englobar o direito ao conhecimento da identidade dos responsáveis pela coleta, pelo armazenamento, pelo tratamento e pela utilização dos dados. Deve-se igualmente relembrar o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados para arrolar o direito à retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados.

Desta forma, pode-se afirmar que, embora não se trate de uma Carta propriamente

[15]O *habeas data* é um dos mais importantes remédios constitucionais previstos na Constituição de 1988 por destinar-se a proteger a esfera íntima dos indivíduos. Por isto mesmo tem status nas garantias fundamentais dispostas no art. 5º. Dentre as suas finalidades, destacam-se as de proteger a intimidade das pessoas contra usos abusivos de registros de dados pessoais coletados por meios ilícitos e evitar a introdução dos já referidos dados sensíveis nestes arquivos. Visa também a desfazer a conservação de dados falsos ou com fins diversos dos previstos em lei.

digital, a Constituição brasileira se presta para basear e para disciplinar essa temática. Se se tomar, e.g., os direitos à liberdade científica (pesquisa), à intimidade e à privacidade entende-se que são direitos fundamentais e, por sua vez, não sofrem limitações mediante legislações ordinárias[16], vez que o constituinte os imantou com uma proteção adicional, inclusive no que diz respeito à vedação ao retrocesso.

Nessa altura, cumpre enfatizar a posição central da dignidade da pessoa humana que, de fato, é um princípio fundamental da Constituição Brasileira (CF/88, art. 1º, III), sendo inerente ao próprio Estado Democrático de Direito, integrando sua estrutura de modo essencial. E, assim, torna-se possível, a partir dele, inferir diversas constelações protetivas voltadas para a pessoa humana aplicáveis à contemporaneidade e, nesse sentido, apropriadas às atualizações e inclusive à regulação do emprego das tecnologias disruptivas, pautando-se em uma ideia de governança digital que, embora naturalmente flexível, possa garantir uma atuação adequada e, daí, segura à pessoa humana no âmbito informacional.

Não se torna despiciendo reafirmar que, ao dispor sobre os princípios fundamentais na parte inaugural da Constituição, o legislador constituinte deixou registrada de forma clara e inequívoca sua intenção de outorgar aos mesmos o caráter basilar e informativo de toda a ordem constitucional[17], integrando o que pode se chamar de núcleo essencial da Constituição material (SARLET, 2017, p. 113) que, portanto, deve ser tomado como suporte normativo último para a construção de sistemas e de padrões de segurança e de governança digital que sejam anteparos aos direitos humanos e fundamentais engendrados sob a égide dos princípios da prevenção e da precaução e, destarte, eficazes contra as diversas formas de discriminação algorítmica.

Fato inconteste é que, no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, mais especificamente na LGPD, o direito à privacidade é considerado um direito fundamental e um dos direitos da personalidade, sendo um instrumental jurídico que supera a dicotomia entre direito público e privado[18]. Essencial à formação da pessoa humana

[16]A respeito do tema vide Ingo Sarlet em sua obra Eficácia dos Direitos Fundamentais no item 4.2.3 "Os limites dos direitos fundamentais" (SARLET, 2017).

[17]"Consideram-se princípios jurídicos fundamentais *os princípios historicamente objetivados e progressivamente introduzidos na consciência jurídica e que encontram recepção expressa ou implícita no texto constitucional".* Pertencem à ordem jurídica positiva e constituem um importante fundamento para a interpretação, integração, conhecimento e aplicação do direito positivo (CANOTILHO, 2000, p. 1165).

[18]Torna-se perceptível que a proteção à dignidade da pessoa humana envolve um aspecto negativo, no sentido de impedir violações, mas também um aspecto positivo, isto é, de assegurar o pleno desenvolvimento da personalidade de cada um dos indivíduos. Em função disso, a Constituição Federal de 1988 não se restringiu a uma elaboração em que a dignidade da pessoa humana ficasse restrita a um mero enunciado, de fato, a considerou como fundamento que se reflete em todo o texto constitucional. Ainda digno de nota é enfatizar que a dignidade da pessoa humana é fonte primária que apresenta as diretrizes do ordenamento jurídico do Estado de Direito, representando vetor interpretativo e indicativo. E, em se tratando do direito brasileiro, apresenta-se como um dos fundamentos do próprio

e indispensável na construção da identidade pessoal. Logo, é inegável a correspondência entre o princípio da dignidade[19] da pessoa humana com, de modo geral, os direitos fundamentais, observando-se com um destaque superior, em razão do tema dessa investigação, a garantia da liberdade, da intimidade, da privacidade e da proteção de dados pessoais sensíveis na sociedade informacional (SARLET, 2017, p. 110).

Nessa perspectiva é que se torna cada vez mais clara a proeminência da LGPD no ordenamento pátrio na medida em que ela se volta para a regulação do direito à proteção de dados pessoais, garantido a privacidade e, de certa forma, a integralidade e a intimidade dos sujeitos em geral, particularmente quando se tem em mente a superprodução de dados sensíveis na realidade atual e as inomináveis possibilidades de danos advindos a partir de sua manipulação.

Com efeito, a LGPD dispõe, em seu artigo 1º, sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Do teor do artigo 3º enfatiza-se ainda que se trata de uma proteção destinada aos dados que, independentemente do meio, se referem ao fornecimento de bens ou serviços, notadamente, mas não exclusivamente, dos dados de indivíduos localizados em território nacional. De todo modo, deve-se alertar que na medida em que essa legislação entrar em vigor em 2020 e passar a ser manuseada pela academia e aplicada nas esferas pública e privada, mas, principalmente quando for assenhorada pela população e se tiver instituído os verdadeiros limites de ação da ANPD (Agência Nacional de Proteção de Dados), criada por meio da Medida Provisória 869, de 27 de dezembro de 2018, é que realmente vai ficar mais nítido o panorama e as balizas da proteção de dados no Brasil.

3. O CONSENTIMENTO LIVRE, INFORMADO E ESCLARECIDO E AS HIPÓTESES DE TRATAMENTO EM FACE DO DIREITO DE PROTEÇÃO DOS DADOS PESSOAIS SENSÍVEIS

Exsurge inegavelmente da atual ideia de vigilância e de tecnocontrole a tarefa de reforçar a importância do consentimento (RADLANSKI, 2015, p. 10-11), em especial em uma forma escrita, resgatando-o como um dos pontos nucleares do legado do século XX no sentido de valorização da autonomia privada, dos direitos humanos e fundamentais. Em especial, particulariza-se a sua natureza processual na medida em que devem ser garantidas todas as

Estado Democrático de Direito.

[19]Sarlet destaca a complexidade inerente à conceituação jurídica da dignidade da pessoa humana (SARLET, 2017. p. 70).

condições, inclusive temporais, circunstanciais e informacionais, para a tomada de decisão livre, esclarecida, e autônoma em um cenário de liberdade, de solidariedade e de responsabilidade (BRÜGGEMEIER, 2010).

Em outras palavras, o consentimento deve ser efetuado nos moldes de um ato jurídico pleno, respeitando-se a ampliação de uma perspectiva de validade e de perfectibilidade em um panorama em que novos atores, advindos da era informacional (CUKIER, 2014, p. 176), passam a ser cada vez mais corresponsáveis para a criação de um ambiente livre, seguro, minimamente estável nas fronteiras estabelecidas por sistemas auditáveis, compreensíveis e acessíveis. Segundo o art. 5º, XII, da LGPD, trata-se de uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Trata-se, com isto, de uma construção em que as fronteiras do processo de anonimização em face da reconfiguração do direito à privacidade e, consequentemente, do direito à proteção dos dados sensíveis devem se encontrar em um movimento de consonância e de adequação com um padrão protetivo para o resguardo da identidade digital tendo como base a dignidade e a autodeterminação informativa em face da hiperaceleração da tecnologia. Nesse aspecto, urge apontar para a dicção do artigo 5º , X, da LGPD sobre o tratamento de dados pessoais na medida em que esta institui que consiste em toda operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, à modificação, à comunicação, à transferência, à difusão ou à extração.

Um ponto determinante a ser levado em consideração sobre o tratamento dos dados pessoais é que, para que possam ser coletados, é, em regra, necessário o consentimento expresso do titular e, preferencialmente, sob a forma escrita. O consentimento, não custa reforçar, se aplica sempre em razão de uma finalidade explicitada e específica, impossibilitando-se o uso de uma aprovação genérica. Portanto, caso seja necessário usar os dados do titular para outros fins é necessário que haja uma nova aprovação, um novo processo de anuência. Assim, apesar de uma grande maioria das bases já possuírem inúmeros dados extremamente diversificados, os dados previamente existentes também deverão passar por uma revisão e devem receber a autorização dos titulares para serem mantidos, tratados e processados.

Quando se tratar de menores de idade, é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis. Outro aspecto primordial é quanto ao uso estrito dos dados, ou seja, deve ser empregado apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão, vedado o repasse a terceiros. Na ausência do consentimento, só podem serem coletados dados em situações de urgência,

devendo-se imediatamente entrar em contato com pais ou com os responsáveis para garantir a maior e mais adequada proteção à criança e ao adolescente. Nesse ponto observa-se uma relação clara entre a LGPD, o ECA (Estatuto da Criança e do Adolescente) e a principiologia constitucional.

Daí, a imprescindibilidade da garantia do *design* de sistemas centrado no ser humano (*human centered design*) e, assim, pautado na ideia de responsabilidade algorítmica que, em outro giro, aponta para a produção de sistemas rastreáveis, auditáveis, os quais possibilitem um monitoramento contínuo não somente na medida de uma valorização da autodeterminação informativa, mas, sobretudo, como por meio da oportunização diversificada, plena no caráter informativo, e acessível acerca das formas de manifestação e de revisão das modalidades de anuência.

Em razão disso, pertinente é relembrar que a despeito da extrema relevância do consentimento (MELE, 2017, p. 54-55) como instrumental para a reafirmação da autonomia, atualmente há outros aspectos que emolduram o cotidiano e, consequentemente, o enfraquecem, tais como: o volume e o fluxo de informações que elevam a velocidade das transações a níveis exponenciais, comprometendo o processo de formação da vontade consciente; o excesso de pegadas/sombras digitais que são geradas por todas as pessoas, independentemente de sua anuência; e, por fim, a incapacidade do Estado em sua configuração atual para enfrentar a crise de soberania que o fenômeno da sociedade informacional revelou e, dessa forma, a incontestável precarização da garantia da dignidade da pessoa humana que se tem testemunhado.

Aliado a esses aspectos, interessante apontar os déficits educacionais da população brasileira que gera uma realidade desalentadora na qual esse novo instrumento legal se insere a partir de 2020 (BRUINI, 2020).

O que se projeta quando se trata do ato de consentir, destarte, é uma espécie de ideal que deve ser sempre posto na condição de *standard* mínimo, vez que em sua totalidade se torna cada vez mais impossível de ser experienciado em sua plenitude, tanto no que se refere ao mundo real quanto ao mundo digital. Com efeito, a ideia acerca de uma racionalidade absoluta a despeito dos vieses cognitivos que eivam qualquer decisão humana ainda ampara significativamente o conceito de sujeito de direito a despeito das contribuições científicas, destacando as advindas das pesquisas em neurociências.

Em rigor, o que se pode inferir da relação do ser humano nessa clivagem da História é que na medida em que se tornou seu único predador, tornou-se igualmente ansioso e amedrontado em relação a sua capacidade e engenhosidade (CROUCH, 2017, p. 107-108). Assim, carece de mais tempo para a interlocução com o momento atual e, dessa forma, carece do encetamento de uma processualística apta à realidade fendida em diversos mundos que interagem entre si.

Outros aspectos problemáticos podem ser ainda apontados, e.g., a questão da reversibilidade dos processos de anonimização e, em consequência, da impermanência do consentimento que, nesse ponto, passa a ser necessariamente, sempre precário e, portanto, circunstanciado a um momento determinado. Portanto, não há eternidade quando se refere ao consentimento, vez que ele demanda sempre uma certa atualização do sujeito em relação ao uso dos seus dados pessoais, particularmente quando se trata de dados sensíveis.

De qualquer sorte, o processo de consentir permanece como um dos ícones nessa era digital, essência (NIDA-RÜMELIN, 2018, p. 235) da dignidade da pessoa humana, devendo ser valorizado e, na medida do possível, adequado às novas circunstâncias oriundas da velocidade, da fluidez e da flexibilização de fronteiras, ou seja, em relação ao potencial da *privacy by design*. Destaca-se, nessa altura, a fundamentalidade do ato de consentir, sobretudo no âmbito da internet, como fruto de uma relação gnosiológica, ou seja, como um processo de conhecimento.

Não custa relembrar que a LGPD evidenciou a transparência como elemento central e, desta forma, tornou cristalina a ideia de que todos os procedimentos envolvendo dados pessoais, sobretudo os dados sensíveis, devam ser compatíveis com a finalidade da coleta e minimizados em uma política de uso racional, sobretudo em razão da sua perenidade. Outro aspecto notável foi o fortalecimento da proteção e a decorrente vedação de uso de dados sensíveis para fins discriminatórios independentemente do consentimento do usuário, especialmente face aos riscos de destruição, de divulgação e de acesso indevido em razão da estrutura aberta da internet.

Há em razão dos diversos riscos advindos com a sociedade informacional, sobretudo no que toca à submissão da pessoa humana às decisões irreflexivas, automatizadas, discriminatórias e irrenunciáveis, uma superior necessidade de um esforço global quanto ao reforço da relevância das expressões da autonomia privada no âmbito digital. Notória passou a ser a ideia de granulação quando se trata do processo decisório e, por outro lado, enfatiza-se o incremento de um debate acerca dos limites de regulação do emprego de algoritmos e da inteligência artificial, vez que podem impactar de maneira radical a vida dos indivíduos com especial atenção, e.g., para a criação de perfis comportamentais de navegação que, por sua vez, podem ter fins discriminatórios.

De fato, o legislador assegurando a ideia de exceção e, desse modo, enaltecendo a anuência do titular dos dados, esclareceu no artigo 11 da LGPD as hipóteses de tratamento de dados sensíveis. Conferiu ainda as hipóteses de tratamento sem o fornecimento do consentimento quando se tratar de: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados

pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral nos termos da Lei de Arbitragem; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia de prevenção à fraude e à segurança do titular, nos processos de identificação e de autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º da LGPD e exceto em caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ainda convém apontar o teor do artigo 17 da LGPD na medida em que arrola os direitos dos titulares dos dados e, nessa dimensão, oportunamente deve ser sublinhada a ação da ANPD que, ao contrário do que prescrevia a LGPD foi subtraída na sua atuação mais livre e desvinculada dos órgãos públicos, mas, que deve, em última instância contribuir de modo decisivo para a criação de um cenário de governança e de democracia digital no Brasil.

4. SÍNTESE CONCLUSIVA

Na sociedade informatizada, são trocados dados pessoais com elevada frequência. Estes dados representam um valioso instrumento, além de gerarem informações essenciais, para as empresas privadas e para as autoridades públicas, já que permitem o desenvolvimento de políticas públicas mais eficientes e podem gerar lucro para o setor privado. No entanto, muitas vezes são tratados sem qualquer preocupação com a sua segurança, tornando o seu armazenamento, tratamento, transferência e manipulação como elementos ameaçadores dos direitos humanos e fundamentais, destacando-se o direito à proteção de dados que, como se depreende dessa investigação, pode ser entendido como um direito autônomo no sistema normativo brasileiro, sobretudo no que afeta aos dados sensíveis.

Acerca desta temática, foi preliminarmente editado o Marco civil da internet que, em termos gerais, implantou um novo patamar no que toca à internet, mas consistiu apenas em um estágio germinal quanto ao cuidado em relação aos riscos de discriminação algorítmica e, em especial, aos possíveis impactos de acidentes de vazamentos de dados na sociedade informacional.

De fato, foi com a Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, ora em estado de *vacatio legis*, que o sistema normativo brasileiro passou a integrar um conjunto de países que adotaram medidas legais de segurança digital e, dessa maneira, garantiram sua presença no ambiente de transações internacionais que tem utilizado, direta ou indiretamente, os dados como mercadoria principal.

A LGPD instituiu um feixe de direitos referentes à proteção dos dados pessoais,

enfatizando a necessidade de se proteger os dados sensíveis em razão das possibilidades de uso discriminatório e em razão de sua ampla possibilidade de afetação à pessoa humana. Dado sensível, por sua vez, diz respeito aos aspectos mais nucleares da personalidade.

Dessa maneira, pautando-se nos princípios da precaução e da prevenção, reconheceu a vinculação dos dados à pessoa humana e, de modo particular, destacou a relevância do consentimento livre, específico, atrelado a uma finalidade e fruto de um processo gnosiológico de emancipação e de informação nas operações envolvendo trafego de dados pessoais, sobretudo quando se trata de dados sensíveis. Por sua vez, reforçou-se a ideia de que a anuência deve ser diretamente atrelada a uma finalidade, tratando-se de óbice às formas de consentimento abstratas e genéricas. A questão permanece praticamente em aberto, todavia, quando se trata do uso de *Big Data*.

Outro aspecto central nesse debate diz respeito ao fato de que, embora os dados possam ser relacionados aos seus titulares, não se pode desconhecer que, em razão do uso de *Big Data* e de inteligência artificial há sempre a relação com os dados de outrem, portanto, a proteção de dados pessoais sensíveis deve ir além da ideia de soberania de dados. Há, portanto, uma dimensão relacional no que toca à proteção de dados além dos inumeráveis aspectos referentes à esfera dos direitos da personalidade, particularmente em relação ao direito à identidade digital e aos desdobramentos que compõem o livre desenvolvimento da personalidade no âmbito digital/virtual.

No que concerne ao ambiente digital caracterizado pela volatilidade, ambiguidade, incerteza e complexidade, deve-se sublinhar a impermanência e a transitoriedade que devem ser relacionadas às técnicas de anonimização de dados que, com certeza, afetam a ideia de parametrização que, em curto espaço de tempo, acabarão por colocar em xeque as fronteiras entre os modos *off-line* e *on-line* de atuação do sujeito de direito. Dados referentes aos hábitos alimentares, à saúde, à identidade genética, dentre outros, podem vir a ser utilizados para a composição de perfis para fins discriminatórios, portanto, utilizados para fins de caráter inaceitável e injustificável em regimes democráticos e, dessa forma, a noção acerca dos dados sensíveis pode vir a ser radicalmente alterada, carecendo de maior proteção que deve se manter sempre atualizada e em constante atualização.

A proteção dos dados pessoais sensíveis está, dentro desse quadro, diretamente relacionada com a autodeterminação informativa, em especial quando se tem em mente que o controle e o compartilhamento dos mesmos se tornou essencial nos dias de hoje para o livre desenvolvimento da personalidade em uma sociedade assentada na economia de dados e em um contexto marcadamente voltado para a vigilância e para o tecnocontrole. O protagonismo passou, então, a ser da pessoa humana que, em razão do seu empoderamento, pode e deve vir a participar mais ativamente na arena de poder contemporânea quanto à delimitação dos espaços de atuação e de exposição por meio do uso de seus dados. A

privacidade, nesse sentido, continua sendo um direito fundamental elementar que, embora constitucionalmente consagrado desde 1998 passa agora a ter uma nova configuração em uma constelação que confere primazia ao direito à proteção dos dados pessoais.

Nesse ponto, deve ser redimensionada e realinhada a ideia de consentimento livre, esclarecido e informado em seu caráter instrumental, em um panorama de empoderamento da pessoa humana, particularmente no que tange à frenagem da opacidade do tratamento de dados pessoais, que se abre com a entrada em vigor da LGPD, mas que se encontra profundamente relacionado com o papel atribuído à ANPD que, em razão da formatação dada pela Medida Provisória que a instituiu e, desse modo, acabou por estar vinculada à presidência da república. De fato, a ANPD acabou alcançando inclusive outros contornos a despeito do que originalmente previa a LGPD.

A proteção de dados, em suma, vem se tornando um grande desafio, vez que deve servir como um anteparo, uma garantia contra a assimetria relacional que caracteriza o atual cenário globalizado, hiperconectado em que os gigantes tecnológicos se tornaram hegemônicos e suplantaram a atuação dos Estados.

Fundamentalmente, deve-se relembrar que a Internet é um fenômeno global que alterou a gramática cultural, implicando em novos modos de comportamentos mais atentos à possibilidade de engendramento de novas formas ditatoriais e de aniquilamento da pessoa humana.

Esse é, de todo modo, um grande desafio, sobretudo para a sociedade brasileira nos tempos atuais na medida em que urge retirar a LGPD de seu estado de letargia e vivificá-la em um sentido cada vez mais pragmático e adequado ao padrão normativo nacional que, em síntese, parece ser ainda de total alienação. Deve-se encetar um conjunto de ações que fortaleçam a pessoa humana em consonância com um nascente movimento global de antagonismo ao processo de algoritmização da vida.

REFERÊNCIAS

ALMEIDA, Silvio Luiz de. ***O que é racismo estrutural?*** Belo Horizonte: Letramento, 2018.

BRÜGGEMEIER, Gert. Protection of personality rights in the Law of delict/torts in Europe: mapping out paradigms. *In*: BRÜGGEMEIER, Gert; CIACCHI, Aurelia Colombia; O'CALLAGHAN, Patrick (Ed.). ***Personality rights in European tort law***. Cambridge: Cambridge University Press, 2010.

BRUINI, Eliane da Costa. **Educação no Brasil**. *Brasil Escola*, [*s.l.*], [201-]. Disponível em: https://brasilescola.uol.com.br/educacao/educacao-no-brasil.htm.

Acesso em: 10 jan. 2020.

CANOTILHO, J. J. Gomes. **Direto constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2000.

CASTELLS, Manuel. ***A era da informação*: economia, sociedade e cultura**. São Paulo: Paz e Terra, 1999, v. 3.

COSTA JR., Paulo José da. ***O direito de estar só*: tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 1970.

CROUCH, Colin. Postdemokratie. **Gius, Laterza & Figli (Übersz)**. 13. Auf. Frankfurt am Main: Suhrkamp, 2017.

CRYDLEWSKI, Carlos. **Computação sem fronteiras**. Caldeirão de Ideias, [s.l.], [201-]. Disponível em: https://caldeiraodeideias.wordpress.com/2010/07/02/computacao-sem-fronteiras/. Acesso em: 10 dez. 2019.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. **Big data: a revolution that will transform how we live, work and think**. Boston, New York: Mariner Books, 2014.

DETERMANN, Lothar. **Determann's field guide to data privacy law – international corporate compliance**. 2. ed. Massachusetts: Edward Elgar, 2015.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ECHTTERHOFF, Gisele. **Direito à privacidade dos dados genéticos**. Curitiba: Juruá, 2010.

ECO, Umberto. **Der ewige Faschismus. Burkhart Kroeber (Übersz.)**. München: Carl Hanser, 2020.

EUROPEAN COMISSION. European Group on Ethics in Science and New Technologies. Statement of artificial intelligence, robotics and 'autonomous' systems. Brussels, 2018. Disponível em: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. Acesso em 20 jan. 2020.

FREITAS, Eduardo de. **A qualidade da educação brasileira**. Brasil Escola, [s.l.], [201-]. https://educador.brasilescola.uol.com.br/trabalho-docente/a-qualidade-

educacao-brasileira.htm. Acesso em: 10 jan. 2020.

FUKUYAMA, Francis. **Identität: wie der Verlust der Würde unsere Demokratie gefährdet**. Hamburg: Hoffmann und Campe, 2020.

GRABOSCH. Jens. **Analoges Recht in der digitalen Welt**. Braucht das BGB ein update? Eine Untersuchung am Beispiel digitaler Inhalte. Europäische Hochschulschriften Recht, Berlin, Band 6065, s. 27-29, 2019.

HABERMAS, Jürgen. **Um ensaio sobre a Constituição da Europa**. Tradução de Mirian Toldy; Teresa Toldy. Lisboa: Edições 70, 2012.

HENKEL. **Der Strafschutz des Privatlebens gegen Indiskretion, in Verhandlungen des 42**. Deutschen Juristentages (Düsseldorf, 1957), Band II, Teil D, Erste Abteilung, Tübingen, 1958, p. 81 apud COSTA JR., Paulo José da. O direito de estar só: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

HENNING, Klaus**. Smart und digital: wie künstliche Intelligenz unser Leben verändert**. Aachen: Springer, 2019.

HOFFMANN-RIEN, Wolfgang. Inteligência artificial como oportunidade para a Regulação Jurídica. Direito Público, Porto Alegre; Brasília, n. 90, nov./dez. 2019.

JÖNS, Johanna. **Daten als Handelsware. Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)**, 2016.

KNOBLOCH, Hans-Heinrich. **Der Schutz der Persönlichkeit im Internet.** In: LEIBLE, Stefan; KUTSCHKE, Torsten (Hrsg.). Der Schutz der Persönlichkeit im Internet. Tübingen: Boorberg, 2013.

KROHM, Niclas. **Der Schutz personenbezogener Daten in Zuge von Unternehmenstransaktionen**. In: SIMITIS, Spiros Simitis (Hrsg..). Veröffentlichungen der Forshungsstelle für Datenschutz an der Johann-Wolfang-Goethe-Universität. Band 39. Frankfurt am Main: Nomos, 2012.

LE BRETON, David. **Desaparecer de si: uma tentação contemporânea**. Tradução de Francisco Morás. Petrópolis, RJ: Vozes, 2018.

LEIBLE, Stefan; KUTSCHKE, Torsten (Hrsg.). **Der Schutz der Persönlichkeit im Internet**. Tübingen: Boorberg, 2013.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2008.

MELE, Alfred R. **Willensfreiheit und Wissenschaft: ein Dialog**. Guido Löhter (Übersz.). Berlin: Suhrkamp, 2017.

MENDES, Laura Schertel; MATTIUZZO. **Discriminação algorítmica: conceito, fundamento legal e tipologia**. Direito Público, Porto Alegre; Brasília, n. 90, nov./dez. 2019.

MILLS, John L. Privacy the lost right apud RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize (Colaboradora). **O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito – UFPR, Curitiba, n. 53, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768. Acesso em: 22 out. 2019.

MURAT, Pierre. **L'identité imposée par le droit et le droit à connaître son identifié**. In: MALLET-BRICOUT, Blandine; FRAVARIO, Thierry Fravario (Dir.). L'identité, un singulier au pluriel. Paris: Dalloz, 2015.

NIDA-RÜMELIN, Julian. **Philosophie und Lebensform**. 2 Auf. Frankfurt am Main: Suhrkamp, 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral da ONU aprova resolução de Brasil e Alemanha sobre direito à privacidade. [S.l.], 19 dez. 2013. Disponível em: https://nacoesunidas.org/assembleia-geral-da-onu-aprova-resolucao-de-brasil-e-alemanha-sobre-direito-a-privacidade/. Acesso em: 02 jan. 2020.

OTTO Y PARDO, Ignacio de. **La regulación del ejercicio de los derechos y libertades**. Madrid: Cuadernos Civitas, 1988.

RADLANSKI, Philip. **Das Konzept der Einwilligung in der datenschutzrechtlichen Realität.** Tübingen: Mohr Siebeck, 2015.

RYDLEWSKI, Carlos. **Computação sem fronteiras**. Caldeirão de Ideias, [s.l.], [201-]. Disponível em: https://caldeiraodeideias.wordpress.com/2010/07/02/computacao-sem-fronteiras/. Acesso em: 10 dez. 2019.

SALES, G. B.; MOLINARO, C. A. **Questões tecnológicas éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data**. Direitos Fundamentais & Justiça, Porto Alegre, v. 13, p. 183-213, 2019.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 12 ed. Porto Alegre: Livraria do Advogado, 2017.

SCHMIDT, Eric; COHEN, Jared. **The new digital age: reshaping the future of people, nations and business**. London: John Murray, 2014.

SILVA, Virgílio Afonso da. **Direitos fundamentais: conteúdo essencial, restrições e eficácia**. 2. ed. 3. tir. São Paulo: Malheiros, 2014.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. [S.l.], 2000. Disponível em: http://www.direitoshumanos.usp.br/index.php/Documentos-não-Inseridos-nas-Deliberações-da-ONU/carta-dos-direitos-fundamentais.html. Acesso em: 12 dez. 2019.

VELASCO, Ariane. **Saiba o que são computadores quânticos e por que eles são melhores**. CanalTech, [S.l.], [201-]. Disponível em: https://canaltech.com.br/inovacao/computadores-quanticos-o-que-sao/. Acesso em: 01 dez. 2019.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Fabris, 2007.

WARREN, Simon D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, Boston, v. IV, n. 5, 15 Dec. 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.Acesso em: 13 mar. 2015.

ZENNER, Florian. **Algorithmenbasierte Straftatprognosen in der Eingriffsverwaltung – Zu den verfassungsrechtlichen Grenzen und einfachgesetzlichen Möglichkeiten von "Predictive Policing"**. In: WIECZOREK, Mirko Andreas (Hrsg.). Digitalisierung: Rechtsfragen rund um die digitale Transformation der Gesellschaft. Göttingen: Cuvillier, 2018.

Recebido em 02/03/2021
Aprovado em 30/08/2021
Received in 03/02/2021
Approved in 08/30/2021