UNIVERSIDADE PRESBITERIANA MACKENZIE

GERALDO RODRIGO SOARES DE SOUZA

DIREITOS DOS TITULARES DE DADOS PESSOAIS E PROCEDIMENTOS PARA SUA OPERACIONALIZAÇÃO

São Paulo

2020

GERALDO RODRIGO SOARES DE SOUZA

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADOR: EDUARDO ALTOMARE ARIENTE

São Paulo

2020

GERALDO RODRIGO SOARES DE SOUZA

DIREITOS DOS TITULARES DE DADOS PESSOAIS E PROCEDIMENTOS PARA SUA OPERACIONALIZAÇÃO

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovado em:

BANCA EXAMINADORA

_____

Examinador(a): Prof: Dra. Geisa de Assis Rodrigues

_____

Examinador(a): Prof. Dr. Pedro Buck Avelino

“Dê-me uma alavanca e um ponto de apoio e eu erguerei o mundo”

Arquimedes

RESUMO

A presente monografia objetiva analisar o contexto em que sobressai o direito à privacidade, à proteção de dados e à autodeterminação informativa. Tal contexto, comumente denominado de "sociedade da informação" é marcado pelo avanço da tecnologia de processamento de dados sobre todas as facetas da vida privada e social dos indivíduos. O âmbito de apreensão e controle da tecnologia sobre a vida pessoal ultrapassa de forma esmagadora as capacidades individuais de gerenciamento do fluxo dos dados pessoais dos titulares. A fim de buscar a aplicação prática e a operacionalização dos direitos dos titulares de dados pessoais, analisa-se os aspectos materiais e procedimentais presentes na Lei Geral de Proteção de Dados, Lei 13.709/2018, em abordagem sistemática, tendo também como parâmetro outras disposições e princípios do ordenamento jurídico pertinentes. Por fim, são feitas breves visualizações de como a tecnologia pode ser utilizada para potencializar a operacionalização dos direitos dos titulares.

PALAVRAS CHAVES: PROTEÇÃO DE DADOS, PRIVACIDADE, TITULARIDADE DE DADOS PESSOAIS, PROCEDIMENTOS, TECNOLOGIA DE APRIMORAMENTO DA PRIVACIDADE.

ABSTRACT

This monograph aims to analyze the context in which the right to privacy, data protection and informational self-determination stand out. Such context, commonly called “information society”, is marked by the advancement of data processing technology on all facets of an individual´s private and social life. The scope of apprehension and control of the technology over personal life overwhelmingly goes beyond the individual capacities of managing the flow of personal data of the holders. To seek the practical application and operationalization of the protection of personal data, the material and procedural aspects present in the Lei Geral de Proteção de Dados, Lei 13.709/2018 are analyzed in a systematic approach, taking as a parameter, other provisions and relevant legal order principles. Finally, brief views will display on how technology can enhance the operationalization of the rights of holders.

KEY WORD: DATA PROTECTION, PRIVACY, PERSONAL DATA HOLDER, PROCEDURES, PRIVACY ENHANCEMENT TECHNOLOGY.

SUMÁRIO

INTRODUÇÃO

A trajetória da regulamentação do tratamento de dados no mundo poderia ser abordada como uma história única com capítulos separados conforme o país ou região do Globo. Cada uma com suas forças, percalços e duração. No Brasil, esta trajetória apresenta, como uma das suas características, o longo tempo de maturação. A Lei Geral de Proteção de Dados nacional, a Lei 13.709 de 14 de agosto de 2018, entrou em vigor no dia 18 de setembro de 2020, com exceção dos dispositivos que preveem sanções administrativas. A vigência da lei nacional de proteção de dados é um tópico sui generis no "capítulo brasileiro" da regulamentação do setor: em sua redação original, o art. 65 da lei previa seu início para 18 meses após a sua publicação, o que se daria em fevereiro de 2020. O dispositivo sofreu alteração posterior pela Medida Provisória nº 869 de 2018, cujo conteúdo foi praticamente repetido pela Lei 13.853 de 2019, dispondo que as Seções I e II do Capítulo IX, que tratam respectivamente da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade entrariam em vigor no dia 28 de dezembro de 2018, enquanto todo o restante da lei entraria em vigor não mais 18 meses após sua publicação, mas 24 meses após, o que se daria em Agosto de 2020.

O ano de 2020, marcado pela ocorrência da pandemia do Novo Corona Vírus, agravou a dificuldade de contar a história da vigência da LGPD. Se alguns setores já ansiavam pelo adiamento da vigência da Lei, a pandemia fez parecer necessário este adiamento para muitos. Projetos de Lei e Medida Provisória surgiram em um curto período visando alterar a vigência da LGPD para 2021, algumas para o início, outras para a metade do ano. Tamanha foi a confusão na sucessão aprovações, de vetos e derrubadas de vetos, que mesmo quem acompanhava de perto o trâmite destes atos normativos tinha dúvida acerca do que iria realmente acontecer. Desta forma, este trabalho se desviará da ingrata tarefa de descrever a série de voltas e reviravoltas por que passou a vigência da LGPD, para dizer apenas, como já afirmado, que a Lei 13.709 de 2018 entrou em vigor no dia 18 de setembro de 2020, com exceção dos dispositivos que tratam das sanções administrativas, que entrarão em vigor no dia 01 de agosto de 2021.

À parte da contextualização histórica acerca da dinâmica de elaboração formal do direito à proteção de dados, outro aspecto relacionado ao tema diz respeito a todo um "movimento" gerado em torno da LGPD no país, que se relaciona diretamente à motivação do presente trabalho. Trata-se da inequívoca ênfase que tem sido dada por profissionais do direito,

escritórios jurídicos, e muitos estudiosos do tema à dimensão da conformidade das empresas aos ditames da referida lei. O presente trabalho parte de uma motivação diversa: busca extrair da LGPD, e do ordenamento jurídico como um todo, os procedimentos definidos ou subentendidos para que se possa fazer valer os direitos dos titulares dos dados pessoais frente a alguns dos possíveis controladores ou agentes de tratamento.

A metodologia utilizada foi a consulta bibliográfica, o exame sistemático da legislação pertinente, e o uso de aplicações disponíveis na internet como subsídio exemplificativo de algumas indicações.

A fim de se delimitar o escopo deste trabalho, serão deixados de lado os procedimentos de exercício dos direitos do titular que envolvam o peticionamento perante órgãos de defesa de direitos como a Autoridade Nacional de Proteção de Dados, os órgãos de defesa do consumidor, o Ministério Público ou a via da ação judicial. Delimitando ainda mais, o presente estudo busca, principalmente, o exercício dos direitos do titular frente a agentes de tratamento que sejam pessoas jurídicas de direito privado, embora pareça possível vislumbrar que várias etapas do procedimento possam ser iguais ou semelhantes quando do exercício perante pessoas jurídicas de direito público.

Parece possível deduzir da organização lógica da LGPD que a mesma tem por objetivo trazer empoderamento ao titula dos dados e, para isto, uma série de direitos exercitáveis por ele mesmo em face dos controladores e operadores foram previstos.

Buscar-se-á, portanto, a descrição de aspectos importantes para uma abordagem procedimental centrada nos usuários de serviços e aplicações, no denominado titular dos dados pessoais. Ao mesmo tempo, considerando o cenário da multiplicidade, volume e velocidade da coleta de dados e da produção de informações sobre os titulares, é de se intuir que a tarefa de exercer a sindicabilidade sobre o tratamento dos seus dados, conforme as prerrogativas conferidas ao titular pela LGPD, não será fácil e poderá mesmo se tornar frustrante. De nada adiantará conferir ao titular direitos materiais que ele não consiga exercer. Por este motivo, será feita uma tentativa de explorar como alguns recursos tecnológicos poderiam contribuir nesta tarefa para superar obstáculos que são típicos deste universo das tecnologias de tratamento de dados. Resumidamente, quer este trabalho investigar possíveis caminhos para se conferir ao titular certa "paridade de armas" no exercício dos seus direitos.

Os direitos à privacidade e à proteção de dados pessoais (direitos da personalidade) têm por fim, dentre outros, garantir os direitos à autodeterminação e ao livre desenvolvimento da personalidade. Tais conceitos foram dotados de um feixe de significados relacionados a esta

esfera da liberdade a partir de decisões da Corte Constitucional alemã de 1983. A autodeterminação informacional "se consolidou como o direito de os indivíduos decidirem em princípio por si próprios quando e dentro de que limites seus dados pessoais são revelados e podem ser utilizados." (ALIMONTE, 2020, p. 177). Contudo, a relação entre o livre desenvolvimento da personalidade e a proteção de dados não é facilmente apreensível sem uma categoria conceitual intermediária que estabeleça esta relação de forma clara. Muitas vezes, a proteção de dados tem pouca relevância como tema de preocupação da grande massa de usuários de aplicativos e serviços on-line (ou mesmo daqueles que fornecem o número do seu Cadastro Nacional de Pessoa Física em supermercados ou farmácias), podendo parecer, diante de outros temas urgentes, tratar-se de mero problema "cosmético". Para buscar evidenciar a importância do tema, serão evocados os conceitos complementares de privacidade contextual (NISSENBAUM, 2004, apud BIONI, 2020) e colapso contextual (BOYD, 2020). A clareza acerca do que está em jogo é fundamental para não se contentar com soluções "cosméticas" para problemas reais.

Adentramos na era do *Big Data*. Do ponto de vista da evolução da sociedade e seus modelos de produção de riqueza, há forte consenso de que a atual pode ser denominada de *sociedade da informação*. "A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial." (BIONI, 2020, p. 5). O modelo de organização em rede das empresas é um dos elementos centrais na configuração desta dinâmica: uma empresa que fornece determinado produto ou serviço terceiriza ao máximo sua cadeia produtiva. Precisam, para atuarem de forma coordenada e para gerar conhecimento útil para seu posicionamento competitivo no mercado, compartilhar dados entre si. Tanto dados próprios, quanto dados dos seus consumidores. Cientes da importância destas informações, as empresas, secundadas pelas gigantes do setor informacional, entenderam a necessidade de obtê-las não apenas quando seus consumidores visitam seus estabelecimentos, ou estabelecem relações diretas com seus sites e serviços de atendimento, mas sobretudo através do "rastro" informacional deixado por consumidores e potenciais consumidores em sites e aplicações diversas. Passam a ser objeto de grande interesse das empresas até mesmo as interações do seu consumidor com serviços utilizados em contextos outros da sua vida, ainda que completamente estranhos ao seu ramo de atuação. Por exemplo, uma rede de supermercados pode estar interessada em ter acesso a informações de saúde de seus consumidores, informações estas que antes só faziam sentido em serem revelados a um

profissional ou serviço da área da saúde. Tal prática anuncia o problema denominado por danah boyd[1] (2020) de "colapso contextual": o apagamento das fronteiras contextuais em que a comunicação de cada pessoa é veiculada na camada de aplicação da internet.

Cada pessoa interage com sites, aplicativos e com temas em diversos graus de pessoalidade. Nestas interações, registros vão sendo criados, armazenados e compartilhados através de diversas técnicas, a fim de se detectar desde interesses até aspectos comportamentais mais finos, como o tempo de reação a um anúncio e o grau de engajamento do usuário com determinado conteúdo e em quais dias ou em que hora do dia e em que local no mapa, assim como as emoções expressas nas interações com outros usuários das aplicações. A previsibilidade extraída destas informações é a "menina dos olhos" desta economia baseada em coleta de dados. Ela serve de base para o aprimoramento de produtos existentes, para a compreensão do mercado, para a oferta de produtos no lugar, no momento e para a pessoa certa. "Há uma ´economia de vigilância´ que tende a posicionar o cidadão como um mero expectador das suas informações". (BIONI, 2020, p. 12)

As relações se tornaram, à revelia do consumidor, mais complexas. No fluxo informacional, na maior parte das vezes, não há mais uma relação bilateral entre consumidor e fornecedor de serviço, mas relações plurilaterais, pois sempre estarão presentes as práticas de compartilhamento de dados com "parceiros". Por traz deste comércio de dados surgiram novos ramos de negócio explorados comercialmente como redes de publicidade e *data brokers* que replicam os dados dos usuários entre vários atores deste mercado, associam os dados de forma nova e extraem deles novos dados. Completam a estrutura deste ramo os serviços de *Big Data* e o uso da *Inteligência Artificial*. Os primeiros compreendendo um conjunto de tecnologias capazes de processar volumes agregados de dados em quantidades antes inimagináveis, em enorme variedade e em velocidade altíssima – os três "Vs". A Inteligência Artificial, utilizada neste processo, permite que a máquina descubra padrões no emaranhado de dados em velocidade quase instantânea e seja capaz de organizar os dados de forma a dar respostas a questões específicas. Assim, quanto mais dados disponíveis, mais padrões perceptíveis para a máquina, e previsões mais acuradas.

Embora óbvio, é preciso lembrar que todo este movimento é estruturado em tecnologia de ponta, desenvolvida por grandes empresas com orçamentos bilionários destinados a pesquisa e desenvolvimento que, pela dinâmica de mercado, almejam retorno sobre o investimento. Salta

[1] Se escreve mesmo em minúsculo.

aos olhos a assimetria de forças entre as partes nesta relação jurídica. Esta monografia considera toda esta estrutura tecnológica e econômica em torno do modelo de negócios da coleta e tratamento de dados, pois dela resulta uma tensão entre os interesses dos controladores dos dados e os dos titulares dos dados. E nesta relação é evidente a hiper vulnerabilidade dos últimos, uma vez que pesa sobre a pessoa natural uma racionalidade sempre muito limitada frente à capacidade de processamento de informações que a estrutura tecnológica fornece às pessoas jurídicas controladoras dos dados.

As *Tecnologias para Aprimoramento da Privacidade (PETs)* surgiram como instrumentos tecnológicos de tentativa de empoderamento dos titulares dos dados pessoais. De forma resumida, Bioni (2020, p. 168) as divide entre as *focadas no plano da coleta de dados* e as *focados no plano do gerenciamento do uso e compartilhamento dos dados pessoais*. Entre as primeiras, estariam ferramentas como o *Do Not Track (DNT)*: objeções na forma de barreiras à coleta de dados pessoais implícitas, por exemplo, no navegador de internet usado pelo titular dos dados. Por concepção *(by Design)*, este navegador não permitiria a atuação de ferramentas de coleta e rastreamento da navegação. Contudo, as ferramentas focadas no plano da coleta parecem sofrer severa limitação em sua eficácia diante da ausência de regulação que as torne cogentes para os provedores de aplicação.

Já as *PETs* focadas no gerenciamento do uso e compartilhamento dos dados parecem proporcionar margem maior de controle ao titular, sobretudo se usadas como suporte para os procedimentos derivados da legislação pertinente à proteção de dados, como se tentará demonstrar através da descrição de serviços baseados em tecnologias de proteção à privacidade já colocados no mercado em países europeus, graças à vigência da General Data Protection Regulation - GDPR.

Este trabalho busca de delinear possível procedimento para o exercício e defesa dos direitos do titular de dados pessoais reconhecendo, porém, que uma abordagem que se baseie nos direitos do titular dos dados pessoais derivados da legislação nacional pertinente e no suporte de tecnologias que facilitem o exercício da privacidade, parece essencial pelos motivos que se exporá no curso do trabalho.

Aposta-se aqui na hipótese de que, na efetivação da proteção do titular dos dados pessoais, os direitos dos titulares previstos na LGPD podem fornecer às PETs uma espécie de eficácia *erga omnes*, pois elas terão a possibilidade de, representando o titular, direcionar a todos os controladores sujeitos àquela Lei as solicitações por ela facultadas ao titular – as

solicitações LGPD. E por sua vez, as PETs podem fornecer ao direito a escalabilidade e a prontidão de resposta que ele não teria com seus métodos habituais.

CAPÍTULO 1

Direitos do titular de dados pessoais

A regulamentação de um setor implica o controle de atividade que antes parecia completamente livre ou que, por ser nova, gozava de certa intangibilidade aos instrumentos tradicionais de controle. As Tecnologias de Informação e Comunicação realmente criaram um novo ambiente de relacionamento humano. Da singela troca de e-mails aos dispositivos de vestir conectados; da ARPANET, uma das primeiras redes de comutação de pacotes de dados destinada a ser uma "espinha dorsal capaz de conectar redes menores preexistentes" (LADEIRA, 2018),[2] à já inaugurada Internet das Coisas (IoT). O pioneirismo dos seus criadores e desenvolvedores presentificou entre nós o que antes era ficção. Como não poderia ser diferente, a inovação, ao ser incorporada ao modo de reprodução das sociedades, traz a reboque o direito. *Ubi societas, ibi jus*. Já concretizadas, as relações digitais precisam agora de segurança, garantias e proteções, como ocorre nas relações humanas onde quer que se deem.

A tensão entre regulação e inovação foi pautada nas discussões que precederam a criação da Lei Geral de Proteção de Dados, bem como na sua positivação, que sofreu a influência deste vetor e, portanto, tem em mira a importância da inovação e busca permitir condições para seu prosseguimento. Já se vislumbra que no dia a dia da sua implementação essa tensão estará sempre presente.

Sem questionar sua importância, a inovação por si só não será o foco deste trabalho. Aqui se buscará estar ao lado do titular dos dados pessoais, entender sua posição hipossuficiente/hiper vulnerável, seus direitos e os meios para sua concretização. O titular dos dados, este que há muito tem servido, a sua revelia, de insumo para a criação de valor para setores diversos na economia de dados, tem agora a sua posição e a sua contribuição valorizada e reconhecida. Buscar-se-á, desta forma, extrair do direito, mais especificamente da LGPD, seu conteúdo protetivo e procedimental a fim de que os fundamentos previstos em seu artigo 2º, incisos I a VII ganhem concretude e operacionalidade ao alcance da mão do titular destes direitos.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;

[2] O artigo de Ladeira (2018) faz uma interessante síntese do contexto da criação do que conhecemos como Internet e da conjunção de interesses de burocratas, militares, industriais e acadêmicos nos esforços que nela resultaram. Conjunção resultante do direcionamento por uma agenda Estatal Norte-Americana de competição internacional pela vanguarda nas fronteiras tecnológicas e pela posição de predomínio político-militar e econômico mundial.

> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ao prever direitos a legislação prevê também obrigações. No caso em tela, estas se expressam em obrigações relativas a construtos técnicos definidos no artigo 5º da LGPD, tais como "dado pessoal", "dado pessoal sensível", "dado anonimizado", "banco de dados", "tratamento", "eliminação", dentre outros.

Neste processo, os atores que coletam e tratam dados pessoais devem adequar suas práticas, seus protocolos e sua infraestrutura tecnológica aos parâmetros principiológicos do direito, traduzidos pela LGPD para a seara do tratamento de dados. No artigo 6º da referida lei, a boa-fé objetiva vem insculpida no caput como verdadeiro polo magnético a orientar a leitura dos princípios que elenca em seus incisos. Assim, as empresas não poderão em sua prática e em sua estrutura tecnológica, coletar, tratar ou compartilhar dados pessoais sem que nelas haja correspondência à finalidade legítima, adequação, necessidade, garantia de livre acesso, qualidade dos dados, transparência, segurança e prevenção, não discriminação e possibilidade de responsabilização. Tal adequação implicará desde a reformulação de contratos até a exclusão de dados que extrapolem a finalidade, a adequação e a necessidade do modelo de negócio da empresa, bem como a legítima expectativa dos clientes. Comentando acerca do aspecto regulatório da LGPD, Bioni (2019) afirma:

> Todo o sistema gira em torno da lógica em se criar uma trilha auditável do dado, pela qual o cidadão e os demais agentes econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades econômicas e relações sociais que fazem parte.

Da necessidade da conformidade dos controladores a princípios do artigo 6º como o do livre acesso, o da transparência e o da responsabilização e prestação de contas, a LGPD torna exigíveis prestações de fazer e deixar fazer, tais como a possibilidade de ser auditado e fiscalizado em relação ao tratamento que é feito dos dados de seus usuários. Sujeitam-se os controladores à possibilidade de escrutínio individual ou coletivo. Aponta a lei uma série de atores legitimamente interessados na fiscalização e na exigência destas obrigações. São eles o

titular dos dados pessoais coletados e o Estado regulador através da Autoridade Nacional de Proteção de Dados e dos organismos de defesa do consumidor.

Tal fiscalização e responsabilização poderá ocorrer a partir das vias de atendimento e suporte ao cliente, por procedimentos auto compositivos, administrativos e, em decorrência da inafastabilidade da jurisdição, também judiciais.

1.1) Núcleo axiológico dos direitos do titular

A razão da legislação nacional de proteção de dados é a proteção da pessoa natural. O objetivo expresso da LGPD vem traçado no art. 1º: " proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Liberdade, privacidade e livre desenvolvimento da personalidade são valores que por si mesmos e isoladamente, fazem jus à proteção pelo direito. Contudo, apenas a pálida evocação ou remissão a ideais iluministas não é mais suficiente para se compreender a carga valorativa e vivencial que tais conceitos devem representar para o cidadão, a sociedade e o direito atual. Conforme alerta Doneda (2020, p. 29), "eventualmente, ocorre que nos encontremos em um dos momentos em que se verifica uma certa defasagem entre a carga semântica de um conceito e o que ele efetivamente representa". O autor faz este alerta no início da sua obra quando faz menção à noção de que "a privacidade está fortemente ligada à personalidade e ao seu desenvolvimento, para o qual é elemento essencial". Contudo, o conteúdo individualista e patrimonialista de outrora do conceito de privacidade é de fato pouco relevante para a noção de desenvolvimento da personalidade.

A ideia de privacidade e a sua busca como valor passou por diferentes momentos históricos. Nos seus primórdios, a privacidade era traduzida no direito a ser deixado só (*zero relationship*). Era uma "prerrogativa reservada a extratos sociais bem determinados", pontua Doneda (2020, p. 32). Esta fase é superada em um segundo momento em que se passa a um Estado de bem estar social. Há uma mudança na relação do Estado com o cidadão. A demanda mais generalizada de direitos faz surgir uma tendência de se buscar informações sobre os indivíduos motivada por aspirações de eficiência e controle dos Entes Públicos responsáveis por políticas públicas ou serviços de larga escala – censos e pesquisas demográficas são a forma de levantamento destas informações. Quando a capacidade de processamento de informação ganha o impulso da tecnologia tornando o custo da coleta e do tratamento acessível a organizações

privadas, elas se veem capazes de lidar com um fluxo astronômico de dados, e assim, a coleta de dados dos cidadãos por empresas diversas visando ao lucro e o momento atual da privacidade se iniciam.

Este momento é marcado pela ubiquidade da coleta de dados sobre a pessoa natural. Em um primeiro momento, entusiasmados com as facilidades oferecidas em troca dos dados pessoais, os usuários consentem rápida e descuidadamente na sua coleta. Posteriormente, o fazem por estarem impotentes frente à superestrutura da coleta de dados, e à enorme fadiga que seria consentir ou não de forma realmente esclarecida em centenas de contratos e termos de uso de serviços.

Este é o contexto em que a privacidade, a proteção de dados e o livre desenvolvimento da personalidade devem ser compreendidos. Como a privacidade e a proteção de dados, condicionam o livre desenvolvimento da personalidade?

Dois conceitos oriundos da ciência da informação e da sociologia parecem promissores na tentativa de fazer uma ligação forte e evidente entre privacidade e proteção de dados e o livre desenvolvimento da personalidade. São os conceitos de *privacidade contextual* e *colapso contextual* concebidos respectivamente pelas pesquisadoras Helen Nissenbaum (NISSENBAUM, 2004, apud BIONI, 2020) e danah boyd (BOYD, 2020).

Explicando a riqueza do conceito proposto pela pesquisadora Helen Nissenbaum para a compreensão do que seria um fluxo apropriado de dados, Bioni (2020, p. 196) diz que

> a professora da Cornell University propõe que o trânsito das informações pessoais tem um valor social, guiado por considerações políticas e morais, que é o que determina ser ele (in)apropriado. A intelecção do que venha a ser (in)apropriado decorre do contexto de cada relação subjacente na qual as informações pessoais fluem.

Conforme o autor explica, em nossas relações sociais, cada contexto pressupõe o que é apropriado e válido quanto ao fluxo de informações pessoais. Desta forma, em um consultório médico revelamos informações pessoais que não revelaríamos na escola, ou na concessionária de automóvel, ou para a Receita Federal, e vice-versa. Da mesma forma, parece razoável que, no interesse do tratamento, o médico compartilhe nossas informações pessoais com a equipe de saúde com que trabalha, mas não com a nossa escola ou com o nosso empregador. Assim, a privacidade contextual diz respeito a este senso de adequação e pertinência entre a informação e o contexto em que ela flui.

Segundo Bioni (2020, p. 196), a abordagem de Helen Nissenbaum parte da percepção de que as novas tecnologias de informação provocam um "desnorteamento" do fluxo informacional.

Este “desnorteamento” parece ter sido captado com muita precisão por danah boyd em seu conceito de *colapso contextual*. Assim, tais proposições parecem captar o mesmo fenômeno, mas esclarecer nuances distintas e complementares.

O artigo de onde se extraíram as considerações acerca da contribuição da pesquisadora danah boyd é a tradução para o português de um capítulo de sua tese defendida na Universidade de Califórnia em 2008 (Taken Out of Context – *American teen sociality in networked publics*). Ali, boyd (2020, p. 27) que estudava a forma como adolescentes construíam perfis em redes sociais, esclarece a noção de colapso contextual:

> Em situações sociais não mediadas, as pessoas tendem a saber quem está presente para testemunhar um ato social. Esse não costuma ser o caso em públicos em rede, onde audiências são invisíveis e o acesso é assíncrono. As limitações físicas ajudam a controlar os limites de ambientes não mediados–as paredes definem o espaço e as expressões podem ser testemunhadas apenas de forma auditiva ou visual. Online, os limites são porosos–a pesquisa colapsa os contextos, a replicabilidade permite que traços de atos sociais sejam copiados para outros espaços e a permanência dos dados significa que os atos executados não são delimitados pela efemeridade. Em outras palavras, tentar restringir os atos sociais a um único espaço online é inútil, mesmo que essa seja a norma em ambientes não mediados.

Portanto, o *colapso contextual* seria a expressão do “desnorteamento” do fluxo informacional percebido por Helen Nissenbaum, e seria o “apagamento do conjunto de circunstâncias que tendem a acompanhar uma comunicação propagada, neste caso, por meio digital” (BOYD, 2020, p. 6).

Tal colapso ou desnorteamento apresentam reais obstáculos ao livre desenvolvimento da personalidade, uma vez que priva a pessoa da possibilidade de ocultar-se, de escolher quais aspectos de si quer deixar à mostra. Como foi precisamente apontado por Bioni (2020, p. 91), a possibilidade de efetuar este “gerenciamento” do próprio *ser com os outros e no mundo* foi evidenciada por Hannah Arendt:

> Como observa Hannah Arendt, lançando luz sobre o prefixo idion de indivíduo, a vida em absoluta privatividade ou em total escrutínio público seria idiota. Os fatos que contornam a individualidade de cada ser humano devem ser compartilhados de acordo com as suas respectivas opções para que ele revele e desenvolva a sua personalidade (p. 91).

Assim, a privacidade e a proteção de dados, ao proteger a pessoa do crescente colapso contextual dos fluxos de suas informações pessoais e da perda do direito de se ocultar ou revelar, são condições para o livre desenvolvimento da personalidade, valor fundamental à pessoa humana que, ao fim, resguarda também o valor fundamental da democracia e da convivência na diversidade e na pluralidade.

1.2) Aspectos materiais dos direitos do titular

O Capítulo III da LGPD se intitula "Dos Direitos do Titular". Conforme definição do art. 5º, inciso V da referida Lei, titular é a pessoa natural a quem se referem os dados pessoais objeto de tratamento. Contudo, a possibilidade de pessoas jurídicas figurarem também como titulares destes direitos à proteção de dados pessoais é assunto que poderá vir a ser objeto de discussões, dado o disposto no polêmico Art. 52 do Código Civil de 2002 que prevê que *"aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade"*. Fazendo menção a um dos seus artigos, o Relator do Projeto de Lei 4.060/2012, que se tornou a Lei 13.709/2018 (LGPD), afirmou que o direito do titular sobre seus dados é o elemento essencial de todo o arcabouço da referida lei.

É interessante notar que no Capítulo II, "Do Tratamento de Dados Pessoais", o legislador se preocupou em inserir no art. 9º da Seção I intitulada "Dos Requisitos para o Tratamento de Dados Pessoais", a lembrança de que *"o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca"* da finalidade específica do tratamento, da forma e duração, da identificação do controlador e suas informações de contato, bem como da ocorrência de compartilhamento com terceiros. Desta forma, o princípio do livre acesso (art. 6º, IV) é traduzido em requisito de tratamento e direciona para os direitos materiais do titular elencados a seguir.

O art. 17 da LGPD reafirma que toda pessoa natural tem direito à titularidade sobre seus dados pessoais e têm garantidos os direitos fundamentais à liberdade, à intimidade e à privacidade. O art. 18, talvez o principal dispositivo do capítulo, traz em seus onze incisos e oito parágrafos, os direitos que os titulares de dados pessoais podem exercer perante os controladores, algumas condições para o exercício destes direitos, e finalmente parâmetros que os controladores devem obedecer na prestação de dar informações. O art. 19 define alguns

procedimentos. O artigo 20 estabelece direitos do titular acerca de decisões a seu respeito tomadas através do tratamento automatizado de seus dados pessoais. O art. 21 estabelece regra de proteção à confiança do titular e o art. 22 indica, ainda que desnecessariamente, ser os direitos do titular sindicáveis judicialmente.

O que a LGPD busca estabelecer são condições de equalização de forças entre os titulares dos dados e os controladores. Se antes os direitos fundamentais da liberdade, da intimidade e da privacidade acabavam ficando à mercê da boa vontade dos controladores ou de uma custosa ação judicial, agora, as relações jurídicas em que há tratamento de dados pessoais contam com a proteção de obrigações acessórias estabelecidas por lei que devem ser adimplidas no curso da relação entre titular e controlador.

O entendimento do exato escopo de cada um dos direitos previstos nos incisos do Art. 18 precisará ser buscado na compreensão dos direitos que pretendem proteger, bem como nos casos concretos.

Os direitos previstos no Capítulo III da LGPD (Dos Direitos do Titular) são estruturados de forma a permitir ao titular o conhecimento da situação jurídica dos seus dados em tratamento pelo controlador para, em seguida, disponibilizar as medidas corretivas que se fizerem necessárias. A fim de garantir a paridade de armas no curso da relação jurídica onde há fluxo informacional, o dispositivo instrumentalizou o titular com um procedimento cuja dinâmica é análoga à do procedimento judicial e à do direito de ação: "primeiramente, declara-se a verdadeira situação jurídica, para depois realizá-la, ou tutelá-la", leciona Humberto Theodoro Júnior (2019, p. 142) ao explicar acerca das espécies de processo.

Esta classificação entre direitos de conhecimento e direitos de tutela pode ser aplicada aos dispositivos elencados no art. 18, bem como aos do art. 20 (que inicia por prever o direito à tutela, para depois tratar do direito ao conhecimento).

Assim é que os incisos do art. 18 podem ser divididos entre aqueles destinados a conferir ao titular condições para conhecer a verdadeira situação jurídica do tratamento dos seus dados na relação informacional e entre aqueles destinados a tutelar o seu direito ao tratamento adequado e corrigir eventuais tratamentos indevidos. Entre os primeiros estão os incisos I, II, VII e VIII, enquanto os demais são os destinados às medidas corretivas.

Os incisos I e VII se referem à obtenção da confirmação da existência de tratamento e da informação sobre os agentes com os quais ocorreu uso compartilhado dos dados. Poderá o titular obter de determinada pessoa física ou jurídica, de direito privado ou público, a

confirmação se seus dados pessoais estão sendo por ela tratados, bem como com quem estes dados foram compartilhados. É decorrência dos princípios da transparência e do livre acesso. O titular pode assim conhecer quem lhe conhece.

O inciso II possibilita o acesso aos dados. Havendo o tratamento, pode o titular saber o que a seu respeito é conhecido pelo controlador, ou em que medida é conhecido pelo controlador.

O inciso VIII obriga o agente de tratamento a fornecer informação sobre a possibilidade de o titular não fornecer consentimento e sobre as consequências da negativa. Pode assim o titular saber exatamente sobre quais bases legais, entre as previstas no art. 7º, o tratamento de seus dados por aquele controlador se fundamenta.

Contudo, as informações obtidas necessitarão ainda de parâmetro que permita estimar sua situação jurídica. Tal parâmetro se encontra no direito do titular erigido como um dos requisitos de tratamento pelo art. 9º: o titular tem direito a informação clara, ostensiva e adequada acerca da finalidade do tratamento. A finalidade do tratamento, por sua vez, deverá ser proporcional à *legítima expectativa* do titular. Assim, por exemplo, um provedor de aplicação de rede social que coleta dados da interação do titular com os conteúdos e com outros usuários da rede pode ter por finalidade o oferecimento de anúncio comercial relevante. Contudo, o armazenamento e a coleta dos dados relativos ao comportamento do titular na aplicação por anos a fio sem que sejam apagados tende a gerar um arcabouço tão minucioso de informações sobre o indivíduo que provavelmente excederá e violará a legítima expectativa do titular, pois a quantidade e a qualidade das informações em poder do controlador poderão ser suficientes para que este conheça nuances da personalidade do titular que este só aceitaria revelar em um contexto mais íntimo ou em que existisse, por exemplo, uma finalidade terapêutica e estivesse garantido o sigilo da relação médico-paciente. Daí a importância das noções de *privacidade contextual* e *colapso contextual*: elas fornecem um parâmetro quase intuitivo acerca da adequação entre finalidade do tratamento de dados e legítima expectativa. Sempre que uma operação de tratamento de dados tender a colapsar o contexto da relação em que ocorreu a coleta/fornecimento dos dados ela provavelmente estará eivada de antijuridicidade (esta proposição é cabível inclusive às pessoas jurídicas enquanto titulares).

Do confronto entre a medida, a quantidade e a qualidade dos dados tratados, e a finalidade do tratamento e a legítima expectativa do titular, se poderá estimar a necessidade (quantidade mínima necessária, proporcional e não excessiva) dos dados tratados para aquela finalidade; a adequação (compatibilidade) daquele tratamento em relação àquela finalidade; e

finalmente, a suficiência da base legal utilizada para suportar o tratamento dos dados (uma ou mais das previstas no art. 7°).

Os incisos I e II do art. 18 permitirão ainda que o titular avalie a qualidade dos dados (art. 6º, V) em poder do controlador em relação à *"exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"*.

A partir da ciência pelo titular da situação jurídica dos seus dados perante o controlador, ele poderá lançar mão das providências discriminadas nos incisos III, IV, V, VI e IX, destinadas a tutelar seu direito ao tratamento adequado dos seus dados. São os direitos à correção de dados incompletos, inexatos ou desatualizados (inciso III); à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (inciso IV); à portabilidade dos dados a outro fornecedor de serviço ou produto (inciso V); à eliminação dos dados pessoais tratados com o consentimento do titular (inciso VI); e à revogação do consentimento (inciso IX) e a consequente interrupção do tratamento dos seus dados. Ao que parece, com certa redundância, o § 2° do mesmo art. 18 estabeleceu a possibilidade de o titular se opor ao tratamento, ainda que feito em uma das hipóteses em que o consentimento é dispensado, se o controlador descumprir o disposto na Lei, proteção que parece já estar contemplada pelo disposto no inciso IV acima mencionado.

A mesma dinâmica "processual" está no art. 20, apesar de o dispositivo ter iniciado por prever a medida de tutela em seu caput e, nos seus parágrafos, por imperativo lógico, disposto sobre o direito de conhecimento. Assim é que, conforme o art. 20, § 1º, o titular tem o direito de solicitar ao controlador "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial". Já o caput do art. 20 prevê a consequente tutela posta à disposição do titular: a solicitação da "revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

1.3) Direitos dos titulares como deveres acessórios dos controladores

Do ponto de vista dos controladores e agentes de tratamento, o Art. 18 parece poder ser visto como um rol de deveres acessórios que eles devem cumprir a fim de permitir ao titular o

exercício da sindicabilidade dos seus dados pessoais. Parece bastante importante frisar a razão de ser destes deveres acessórios como sendo a possibilidade de exercício da sindicabilidade e controle dos dados pessoais pelos titulares a fim de garantir seu direito à autodeterminação informativa. Desta razão de ser específica advém uma distinção importante acerca da sistemática lógico-jurídica que se deve ter como referência para a compreensão dos seus desdobramentos. Tratar-se-ia da sistemática dos deveres ou obrigações acessórias afetas ao direito obrigacional civil ou aqui se estaria mais diante de um direito **análogo** àquele da sistemática dos deveres acessórios afetos às prerrogativas do direito de exercer o poder de polícia (sindicabilidade), típico, por exemplo, da Administração Pública em relação à obrigação tributária?

A importância da distinção advém do fato de que, na sistemática das obrigações acessórios do direito obrigacional civil, tais deveres acessórios existem, em regra, com a finalidade de cooperar para a consecução das obrigações principais. Já na sistemática das obrigações acessórias do direito tributário, os deveres acessórios existem para permitir ao Estado o exercício do seu direito de fiscalizar o contribuinte acerca da correta conduta na relação obrigacional tributária. As disposições acerca da obrigação acessória nos respectivos diplomas legais são esclarecedoras e apontam as diferentes consequências.

O Código Civil de 2002 prevê em seu Art. 184:

> [...] a invalidade da obrigação principal implica a das obrigações acessórias, mas a destas não induz a da obrigação principal.

Assim, na perspectiva do direito obrigacional civil, aplica-se a regra geral de que o acessório segue o principal. Não faria sentido, na dinâmica protetiva da LGPD, se pensar que caso a obrigação principal fosse considerada inválida, as obrigações acessórias do Art. 18 também o seriam. Ou, de outra forma, se a finalidade principal da coleta dos dados for considerada inválida, o controlador estaria dispensado das obrigações ou deveres acessórios quanto aos dados pessoais por ele coletados, previstos no Art. 18.

No direito tributário, por sua vez, dentre outras disposições sobre as obrigações acessórias, vale pinçar o Art. 175, parágrafo único da Lei 5.172/1966 (Código Tributário Nacional):

> A exclusão do crédito tributário não dispensa o cumprimento das obrigações acessórias dependentes da obrigação principal cujo crédito seja excluído, ou dela conseqüente.

O dispositivo deixa claro que, mesmo que o sujeito passivo, o contribuinte, esteja dispensado da obrigação principal (crédito tributário excluído), ele não estará dispensado das

obrigações acessórias dele dependentes. Sabe-se que na seara tributária, as obrigações acessórias dizem respeito a prestações positivas ou negativas impostas ao sujeito passivo no interesse da arrecadação e da fiscalização.

A **analogia** das obrigações acessórias previstas no Art. 18 da LGPD com a sistemática lógico-jurídica das obrigações acessórias da seara tributária, e não da seara das obrigações civis, faz sentido por uma razão prática e por uma razão jurídica. A razão prática é devida à falta de sentido em se pensar que um controlador ou agente de tratamento cuja obrigação principal fosse invalidada seria dispensado dos comandos do Art. 18 da LGPD, considerando-se que os mesmos possam ser chamados de "obrigações acessórias" da relação de tratamento de dados. Já a razão jurídica advém do fato de que os direitos dos titulares previstos no Art. 18 são garantias do direito à autodeterminação informativa, que deve ser reconhecido como direito de ordem pública, o que condiz com o seu reconhecimento como direito fundamental e não meramente um direito de ordem contratual privada. Assim, embora na "cartografia" dos ramos do direito o direito à proteção de dados e o direito tributário estejam distantes entre si, a evocação do segundo para se fazer esta **analogia** entre ambos, pois parecem ter em comum a indisponibilidade do bem jurídico que protegem: se o direito tributário tem por fim a o interesse público, o direito à proteção de dados tem por fim o direito fundamental à autodeterminação informativa.

Portanto, se na relação jurídica entre o titular e o controlador prestador de um serviço privado o dever do primeiro perante o segundo é um dever tipicamente de direito privado, pois deriva, em sua maior parte, dos Termos de Uso ou dos Termos do Serviço; os deveres do controlador perante o titular, por seu turno, no que diz respeito às balizas de tratamento dos dados pessoais, são tipicamente deveres de ordem pública. Os direitos dos titulares previstos no Art. 18 da LGP D, na perspectiva dos agentes de tratamento (enquanto sujeitos passivos da obrigação), poderiam ser reconhecidos como deveres ou obrigações acessórias da relação jurídica, mas no sentido de um direito de ordem pública e não no sentido do direito contratual[3].

1.4) Aspectos procedimentais dos direitos dos titulares

[3] Ousa-se aqui discordar da concepção de que os deveres amplos de transparência dos controladores para com os dados pessoais dos titulares seriam explicados como sendo obrigações acessórias de ordem contratual pautada em uma visão solidarista do direito das obrigações, como parece ser defendido por Bioni (2020). Este entendimento, embora perfeitamente razoável quando se pensava o direito à privacidade como direito de natureza privada, não parece o mais adequado quando se entende que a autodeterminação informativa é um direito fundamental, inclusive porque se aplica também nas relações do titular com entes Estatais. É como parece pender o entendimento da Suprema Corte brasileira. Vide a ADI 6.387-DF/2020.

Importante tentar brevemente dar um contexto para o que se busca descrever aqui como "procedimental". Na doutrina jurídica é típico dos processualistas a preocupação em definir e distinguir processo de procedimento. Busca-se, portanto, os ensinamentos de Humberto Theodoro Júnior (2019). O eminente processualista mineiro ensina que o *processo* "é o *método*, isto é, o *sistema* de compor a lide em juízo(...) enquanto *procedimento* é a forma material com que o processo se realiza em cada caso concreto" (p. 137). Buscando a etimologia e/ou o significado de *processo, método e procedimento*, tem-se que: *processo* vem do latim *processus*, e significa avanço, marcha, progressão. *Método* vem do grego *methodos*, e significa através (*meta*) de um caminho (*hodos*). Por fim, *procedimento* significa modo de atuar, tem a mesma raiz latina de *processo* e também encerra a ideia de ir adiante, marchar, avançar. *Procedimento* seria então um modo de avançar.

No direito processual há certo consenso de que o processo seria a relação que segue uma determinada marcha ou procedimento a fim de se buscar a solução de uma demanda, porém dentro de um sistema contraditório. O exercício dos direitos dos titulares que se busca aqui descrever não será aquele sempre possível no âmbito do contraditório judicial, quando já há litígio ou pretensões resistidas, onde, enfim, falamos em *processo* (*procedimento* em contraditório). Mas será sim aqueles *métodos* ou aquelas *metodologias* a serem adotadas previamente, e que são facultadas pela Lei. Por isto a escolha e uso do termo *procedimento* para nomeá-las. Duas características fenomênicas de um *procedimento* apontadas por Humberto Theodoro Júnior (2019, p. 141) vêm a calhar: do ponto de vista objetivo, o *procedimento* seria a multiplicidade de atos coordenados, dependentes um do outro e que, em sequência, se legitimam e têm por fim o alcance um propósito. Do ponto de vista subjetivo, o *procedimento* "se apresenta como obra de cooperação necessária entre seus protagonistas".

Assim, para cada um dos direitos materiais previstos, haverá uma maneira de proceder a fim de exercê-lo, um procedimento. Por exemplo, o direito material do titular de obter a confirmação da existência de tratamento perante um controlador será exercido de uma dada maneira, por um determinado caminho, através de um certo procedimento. É o que se buscará esboçar a seguir.

1.4.1) Sujeito Ativo das solicitações e os requerimentos

O art. 18, caput, prevê que os direitos do titular perante o controlador serão exercidos *a qualquer momento mediante requisição.* Portanto, os direitos do titular são exercitáveis desde o início do tratamento dos dados e enquanto ele durar. Conforme alerta Cots e Oliveira (2018, p. 159) "o exercício de tais direitos é realizado mediante requisição, ou seja, não se trata de pedido ou solicitação, não podendo o controlador se opor, salvo nos casos previstos na LGPD".

De acordo com o art. 18, § 3°, o requerimento poderá ser feito expressamente pelo "titular ou por representante legalmente constituído, a agente de tratamento". A possibilidade de se exercer os direitos do titular requerendo-os pessoalmente perante o agente de tratamento é modalidade sem necessidade de maiores esclarecimentos. Já a modalidade do requerimento por meio de "representante legalmente constituído" parece necessitar de certa elucidação, uma vez que pode suscitar dúvida sobre o tipo de representação: estaria o dispositivo se referindo à representação legal (necessária) ou à representação voluntária (privada)?

O art. 115 do Código Civil de 2002 prevê que "os poderes de representação conferem-se por lei ou pelo interessado". Segundo Farias e Rosenvald (2017) a representação legal "corresponde ao poder, conferido por lei, de agir em nome de outrem, de um incapaz. É o caso dos pais, tutores e curadores" (p. 623). Já a representação voluntária, seguem os autores, é "quando o poder de atuação em nome de outra pessoa é concedido por ato do próprio interessado, da própria pessoa cujos interesses estarão em pauta" (p. 624). Enquanto a representação legal se funda na incapacidade do titular do direito de exercer os atos da vida civil, a representação voluntária se funda na possibilidade de que, por seu interesse e conveniência, o titular, embora capaz, se valha da colaboração de outrem para lhe fazer as vezes, ou lhe representar, como se ele fosse, perante terceiros, seja para celebrar negócio jurídico, seja para manejar direitos.

Ainda segundo Farias e Rosenvald (2017, p. 625), "qualquer negócio jurídico, como regra, admite a representação privada". Assim, o instituto da representação é meio hábil de exercer os atos da vida civil, sendo certa, como regra geral, a sua ampla validade para o exercício de direitos. Vale recordar que o ordenamento jurídico permite até mesmo que pessoas se casem por meio de representante ou procurador, conforme art. 1.542 do Código Civil de 2002.

Assim, nada permite concluir que o exercício dos direitos do titular de dados pessoais perante os agentes de tratamento seriam uma exceção à regra geral da possibilidade e validade ampla da representação voluntária. Portanto, o "representante legalmente constituído" mencionado pelo § 3º do art. 18 seria aquele constituído por uma das formas previstas no art.

115 do Código Civil de 2002, ou seja, aquele cujos "poderes de representação conferem-se por lei ou pelo interessado", pela representação legal ou voluntária.

Superada esta questão, será necessário, no exercício dos direitos do titular, encontrar mecanismos que tenham validade jurídica e sejam seguros para certificar ou autenticar a identidade do titular e do representante quando do recebimento dos requerimentos pelos agentes de tratamento. Certamente aqui será de grande utilidade a utilização e aprimoramento dos mecanismos de assinatura digital, dentre outras tecnologias de autenticação e identificação.

1.4.2) Sujeito Passivo das solicitações

O art. 18, em seu caput, dispõe que o titular tem direito de obter do controlador os direitos ali previstos. Contudo, o mesmo art. 18 em seu § 3º dispõe que os direitos previstos no artigo serão exercidos mediante requerimento a agente de tratamento.

O art. 5º traz as seguintes definições:

> 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;
> IX - agentes de tratamento: o controlador e o operador;

Percebe-se que o § 3º é mais abrangente do que o caput do artigo, pois indica tanto o controlador quanto o operador como sujeitos passivos da obrigação de resposta ao titular. A abrangência destes dois agentes de tratamento na sujeição passiva mencionada é também mais condizente com os princípios da autodeterminação informativa, do livre acesso e da transparência, dando, portanto, maior garantia e proteção ao titular dos dados.

1.4.3) Formas de disponibilização de acesso

As formas de disponibilização de acesso aos dados pelos agentes de tratamento devem ser informadas pelos princípios do livre acesso e da transparência, ambos previstos na LGPD. O primeiro garante a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos dados pessoais (art. 6º, IV), e o segundo garante informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI). No esclarecimento da abrangência da noção de livre acesso aos dados, é sempre importante ter em vista o conteúdo

elencado no art. 9º: as informações disponibilizadas devem ser claras, adequadas e ostensivas sobre

> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

O art. 19, traduzindo o princípio de que os dados pessoais são da titularidade da pessoa a que se referem, prevê dois objetivos de acesso a eles: um destinado a informar o titular sobre a situação jurídica dos seus dados, e outro destinado a permitir que o titular porte os seus dados para a finalidade que lhe aprouver.

Assim é que, para a confirmação da existência do tratamento ou do acesso aos dados, estão previstos dois formatos de declaração: a simplificada e a completa. Os dispositivos da Lei pouco esclarecem sobre quando cada uma será usada e sobre qual a diferença entre elas. Sobre o quando da utilização delas, pode-se imaginar que será conforme a amplitude da solicitação do titular. Quando o titular solicitar apenas que o agente de tratamento confirme se trata algum dado pessoal seu (confirmação da existência), a declaração poderá ser simplificada. Já se a solicitação for de acesso aos dados, a declaração terá que ser completa. Quanto à diferença entre a declaração simplificada e a completa, o art. 19, II dá algumas indicações: a declaração completa deve indicar a "origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento". Para melhor entendimento, parece importante cotejar o dispositivo com o art. 9º, que trata da amplitude do livre acesso. Assim, a origem dos dados, os critérios utilizados e a finalidade do tratamento, parecem corresponder aos incisos I e II do art. 9º: finalidade específica do tratamento e forma e duração do tratamento, respectivamente. A informação acerca do uso compartilhado de dados pelo controlador e sua finalidade, disposto no inciso V do art. 9º poderia ser incluída no escopo da declaração completa, pois também terá que abordar a finalidade. Portanto, se a solicitação do titular abranger todos os incisos do art. 9º, a declaração fornecida pelo controlador deverá ser a completa. Já se a solicitação for apenas sobre a confirmação da existência do tratamento ela poderá ser simplificada e abordar o disposto nos incisos III, IV, VI e VII do art. 9º, ou seja: identificação do controlador, suas informações

de contato, responsabilidades dos agentes de tratamento e direitos do titular (estas duas últimas, talvez apenas tratem de citação informativa de dispositivos da LGPD).

Sobre a forma de acesso, poderá o titular escolher por receber a declaração por meio eletrônico ou impresso, sob o requisito da segurança e da idoneidade. Mais uma vez se coloca o problema da identificação adequada do titular, pois os agentes de tratamento deverão se certificar de que o requerente é o próprio titular ou representante legalmente constituído, bem como de que o meio eletrônico seja seguro e idôneo para garantir que apenas o titular e/ou seu representante terão acesso à declaração.

Por outro lado, visando ao objetivo de permitir que o titular porte seus dados, o § 3º do art. 19 prevê que, quando o tratamento tiver origem no consentimento do titular, ele poderá solicitar cópia eletrônica integral dos seus dados em formato que permita sua utilização subsequente em operações de tratamento. O dispositivo prevê uma obrigação específica aos agentes de tratamento que corresponde ao direito à portabilidade dos dados do titular. Trata-se da obrigação de resguardar a interoperabilidade dos dados entre diferentes agentes de tratamento, inclusive concorrentes no mercado.

1.4.4) Direito à revisão de decisões automatizadas

O titular tem o direito de pedir a revisão de decisões automatizadas com base nos seus dados pessoais que afetem seus interesses (conceito aberto), incluindo aqueles relacionados à definição de seu perfil pessoal, profissional, de consumo e de crédito (rol exemplificativo), bem como a aspectos de sua personalidade (outro conceito aberto). A composição de um perfil a partir de decisões automatizadas, com base em dados pessoais de alguém, pressupõe que estes dados serão objeto de operações de tratamento que envolverão extração de padrões, comparação com dados de terceiros, subsídio a elaborações de novos padrões mais amplos para obtenção de novos dados, dentre outros. Nesse processo, os dados novos, que não foram coletados do titular direta ou indiretamente, mas que se referem a ele, também serão dados pessoais sob a sua titularidade.

O controlador, ao atender a esta providência, deve informar os critérios dos procedimentos utilizados na decisão automatizada. Neste âmbito, mais do que em qualquer outro, a ressalva quanto aos segredos comerciais e industriais tem maior força. Pode, inclusive o controlador se recusar a fornecer tais informações baseado na proteção aos segredos comercial

e industrial. Mas neste caso, se submete a auditoria da ANPD acerca dos critérios utilizados nas decisões automatizadas.

1.4.5) Simetria de providências entre os Sujeitos Passivos no caso de uso compartilhado de dados

O § 6º do art. 18 estabelece a obrigação de que o agente de tratamento instado pelo titular às providências de correção, eliminação, anonimização ou bloqueio dos dados informe imediatamente aos demais agentes com quem realiza uso compartilhado para que efetuem as mesmas providências para que haja simetria entre a situação dos dados do titular que tenham sido coletados no âmbito da mesma relação jurídica.

Porém, o dispositivo cria uma exceção a tal obrigação para os casos em que a comunicação aos demais agentes de tratamento seja impossível ou implique esforço desproporcional. Tal previsão parece criar um verdadeiro "ponto cego" na proteção dos direitos do titular, pois acaba por isentar o agente de tratamento da responsabilidade por fazer uso compartilhado dos dados do titular com terceiros duvidosos.

Seria, por exemplo, o caso de um agente de tratamento, pessoa jurídica, que, após receber uma ampla quantidade de dados pessoais, venha a se extinguir. No caso, embora os dados tenham deixado de ser pertinentes à finalidade específica almejada, parece necessário uma salvaguarda distinta para o caso da extinção da pessoa do agente de tratamento. Na seção destinada ao término do tratamento de dados, a LGPD não abordou expressamente esta situação, mas somente os casos em que, embora haja o término do tratamento, a pessoa do agente de tratamento ainda exista.

Assim, se um operador se extinguir e a possibilidade de comunicação com ele for tecnicamente impossível ou desproporcional, ficaria o controlador isento de responsabilidade em relação aos dados do titular cujo controle se perdeu? Parece ser esta uma questão que necessitará receber tratamento, seja por acréscimo na Lei, seja por regulação da ANPD.

1.4.6) Prazo de resposta ao requerimento do titular

Dispõe o § 4º do art. 18 que "**em caso de impossibilidade de adoção imediata** da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá(...)". Percebe-se que o legislador, embora na maneira da redação tenha se valido de

referência indireta ou *a contrario sensu*, estabeleceu expressamente que a regra é o atendimento imediato da requisição do titular pelos agentes de tratamento.

O prazo de resposta às requisições do titular pelos agentes de tratamento foi abordado de forma confusa pelo legislador, sendo necessário uma leitura sistemática para uma correta compreensão. Em alguns dispositivos regulou diretamente os prazos enquanto em outros delegou o tema à competência regulamentar da Autoridade Nacional de Proteção de Dados (ANPD). Sem a referida leitura sistemática, tal delegação pode parecer redundante e inclusive dar margem a interpretações equivocadas de que a ANPD teria competência para regular completamente o tema. Assim, é que no § 5°, logo após mencionar no parágrafo anterior a regra geral da "adoção imediata da providência de que trata o § 3º" o legislador dispôs sobre a não incidência de custos no requerimento para o titular e que o atendimento se dará "nos prazos e termos previstos em regulamento". Assim, é certo que alguns aspectos do prazo de resposta ao requerimento do titular serão regulamentados pela ANPD, porém nem todos. Neste sentido, a leitura do art. 19 fornece parâmetros:

> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
>
> I - em formato simplificado, imediatamente; ou
>
> II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

A confirmação da existência do tratamento e o acesso aos dados podem ser fornecidos em dois formatos: simplificado e por declaração completa. Enquanto o inciso I do referido artigo prevê que a resposta em formato simplificado será fornecida imediatamente, o inciso II prevê que a resposta completa será fornecida no prazo de 15 dias da data do requerimento do titular. Logo, por exclusão, o que o legislador chamou de "imediatamente" quando se referiu ao prazo de resposta, certamente não pode ser igual ou maior do que 15 dias (pois tornaria desnecessária a distinção dos formatos de resposta). Caberá então à ANPD regular o prazo que se considerará adequado para a resposta imediata no formato simplificado, sendo certo que será menor do que 15 dias, guardadas as exceções previstas no § 4º do art. 19.

A Lei não forneceu indicação sobre o que definirá se a resposta ao requerimento do titular será simplificada ou completa, o que faz parecer que isto será definido conforme a

amplitude da solicitação do titular. Parece sugerir a Lei (art. 18, § 4º, II) que, nos casos de resposta imediata, o não atendimento deste prazo deve ser sindicável, pois a justificativa dada pelo controlador deverá corresponder à realidade.

Por fim, pela leitura sistemática do disposto no art. 18, §§ 3º e 4º e no art. 19 se conclui que:

a) O § 3º do art. 18 menciona todos os direitos previstos no art. 18, logo, os previstos do inciso I ao IX:

"§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento."

b) O § 4º fala sobre atendimento da providência de que trata o § 3º, logo, de todos os direitos previstos no art. 18 e estabelece que, em regra, o prazo para atendimento dos requerimentos dos titulares (acerca de todos os direitos previstos no art. 18) é imediato. Ponto passível de regulamentação, mas certamente menor do que 15 dias (leitura sistemática - parâmetro do art. 19, I e II):

"§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência."

c) No formato de resposta simplificada referente à confirmação da existência de tratamento e acesso aos dados, o prazo é imediato (menor do que 15 dias) ou, conforme o inciso II do § 4º do art. 18, mediante indicação das "razões de fato e de direito que impedem a adoção imediata da providência", em até 15 dias (leitura sistemática - parâmetro do art. 19, I e II).

d) No formato de resposta completa, o prazo é de até 15 dias.

e) Por fim, a ANPD poderá definir prazos diferenciados para setores específicos.

Se uma leitura rápida da Lei faz parecer que o prazo de atendimento às requisições dos titulares referentes aos direitos previstos nos incisos III a IX do art. 18 ficaria completamente sujeito a regulamentação posterior da ANPD, na leitura sistemática que aqui se sugere isto não parece possível, uma vez que, na falta de disposição expressa da Lei quanto à diferenciação destes prazos, parece mais razoável a leitura dos dispositivos com as remissões devidas aos

anteriores e posteriores que tratam sobre o prazo de resposta em questão. Nesta perspectiva, conclui-se que a competência regulamentar da ANPD, no que diz respeito aos prazos de resposta dos agentes de tratamento às requisições dos titulares, será circunscrita a:

a) Definição do que será entendido por "imediatamente", lacuna deixada pela LGPD, mas sendo certo, pela leitura sistemática dos dispositivos indicados anteriormente, que será menor do que 15 dias. Ainda, a razoabilidade sugere que este prazo deverá ser significativamente menor do que 15 dias, do contrário, não faria sentido a distinção feita pelo legislador entre um prazo "imediato" para resposta simplificada e um de 15 dias para resposta completa.
b) Possibilidade de diferenciação do prazo de resposta para setores específicos.

Desta leitura também se pode concluir que a melhor redação para o § 5º do art. 18 seria: *O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos* ***nesta Lei e*** *em regulamento.*

1.4.7) Questões probatórias

A Lei Geral de Proteção de Dados adota para a relação entre titular e controladores um princípio geral de proteção dos primeiros face à sua posição de pessoa natural que tem um bem jurídico personalíssimo sendo utilizado ou explorado por outrem com finalidade comercial, administrativa, de pesquisa, dentre outras. É a chamada posição de vulnerabilidade do titular que, muitas vezes, como se analisará no capítulo seguinte, é uma hiper vulnerabilidade. De igual maneira, não há dúvida de que em várias destas relações entre titulares e controladores há uma relação propriamente consumerista. A LGPD deixou claro este fato em vários dos seus dispositivos que se preocuparam em informar a aplicabilidade subsidiária ou suplementar do Código de Defesa do Consumidor, Lei 8.078 de 1990. O art. 2º, VI da LGPD estabelece como um dos fundamentos da disciplina da proteção de dados, a defesa do consumidor, ao lado da livre iniciativa e da livre concorrência. O § 8º do art. 18 da Lei de Proteção de Dados prevê a legitimidade dos órgãos de defesa do consumidor para receber, alternativamente à Autoridade Nacional de Proteção de Dados, as petições do titular contra os controladores na defesa dos seus dados pessoais. O § 2º do art. 52 do mesmo diploma definiu que as sanções administrativas previstas naquele artigo não substituem as sanções administrativas, civis e penais previstas no CDC. Fica, pois, evidente, que a relação de tratamento de dados pessoais, muitas vezes ocorre no curso de uma relação de consumo.

Consequência lógica desta relativa simetria ou complementaridade da LGPD e do CDC é a aplicabilidade do instituto consumerista da inversão do ônus da prova em várias situações relacionadas aos direitos dos titulares na LGPD. O art. 6º, inciso VIII do CDC prevê como direito básico do consumidor:

> A facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

Segundo Nunes (2019, p. 871), a hipossuficiência que fundamenta a inversão do ônus da prova é a hipossuficiência técnica:

> Mas hipossuficiência, para fins da possibilidade de inversão do ônus da prova, tem sentido de desconhecimento técnico e informativo do produto e do serviço, de suas propriedades, de seu funcionamento vital e/ou intrínseco, de sua distribuição, dos modos especiais de controle [...].

Portanto, para a relação de tratamento de dados no âmbito de relações consumeristas, o requisito da hipossuficiência técnica está plenamente preenchido, como se verá no Capítulo 02.

A viabilidade da inversão do ônus da prova em matéria de proteção à privacidade e tratamento de dados é justificada então por dois caminhos. O primeiro caminho, já mencionado acima, se extrai da própria aplicabilidade do direito consumerista à relação de tratamento de dados. O segundo caminho, decorre da condição geral de vulnerabilidade do titular dos dados pessoais, ainda que não se trate de relação de consumo, que tornará aplicável o § 1º do art. 373 do Código de Processo Civil (Lei 13.105/2015). Assim, embora na regra geral prevista no art. 373, inciso I , o ônus da prova incumba ao autor quanto ao fato constitutivo do seu direito, o § 1° do dispositivo ressalva que:

> "Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído".

Portanto, nas relações de tratamento de dados entre titular e controladores, ainda que ela não se dê no contexto de uma relação de consumo, a simples condição de vulnerabilidade técnica do titular, que lhe traria "excessiva dificuldade" de provar o seu direito, faculta-lhe o benefício da inversão do ônus da prova. Embora este se trate de um instituto de direito processual, sua evocação neste momento em que se examina formas procedimentais não

judiciais de exercício dos direitos do titular é importante para que o sistema protetivo daquele que está em posição de desvantagem seja observado desde sempre. Este é o objetivo da LGPD.

As observações anteriores foram evocadas para que forneçam também um parâmetro hermenêutico para a compreensão e leitura de um modelo de regramento utilizado em vários dos dispositivos da Lei de Proteção de Dados: muitas vezes associada à recomendação da anonimização dos dados pessoais aparece a locução "sempre que possível". Na verdade, das cinco vezes em que esta locução ocorre no texto da LGPD, apenas em uma não está associada à palavra anonimização. Todos estes quatro dispositivos se referem à possibilidade de tratamento de dados pessoais por órgãos de pesquisa. A LGPD previu como uma das bases legais de tratamento de dados pessoais a realização de estudos por órgãos de pesquisa. conforme o art. 7º, IV, esta hipótese dispensa o consentimento do titular dos dados. E não só. Até mesmo o tratamento de dados pessoais sensíveis, que recebeu maior proteção pelo diploma legal, dispensa o consentimento do titular quando *indispensável* para a realização de estudos por órgãos de pesquisa, conforme disposto no art. 11, II, "c". Colaciona-se a seguir os quatro dispositivos mencionados, pois são passíveis de interpretação pela mesma chave de leitura.

> **1)** Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
>
> **2)** Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> **3)** Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
>
> **4)** Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Percebe-se que houve um cuidado do legislador em aplicar a locução "sempre que possível" ao apontar a garantia da anonimização dos dados pessoais em todas as hipóteses em que o seu tratamento dispensa o consentimento do titular. A Lei considera anonimização a "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" (art. 5º, XI). Portanto, quer a Lei dizer que, a menos que seja estritamente necessário, para os objetivos da pesquisa, trabalhar com dados associáveis a um indivíduo, o órgão de pesquisa deverá anonimizar os dados pessoais antes de tratá-los. Ou seja, nesta base legal de tratamento de dados pessoais, "sempre que possível, a anonimização".

Consequência disto é que, se por um lado a LGPD concedeu prerrogativas especiais aos órgãos de pesquisa para tratar dados pessoais sem o consentimento do titular, impôs, por outro lado, a sujeição de que, quando os dados não forem anonimizados, deverá provar a necessidade da manutenção da identificabilidade do titular para a pesquisa e a adequação desta condição, ou seja, que ela não coloca em risco o titular do dado pessoal tratado. Portanto, há aqui uma inversão do ônus da prova do direito à anonimização dos dados pessoais do titular para o tratamento pelos órgãos de pesquisa. Não será o titular que terá o ônus de provar que seus dados foram tratados sem o seu consentimento de forma desnecessária. Será o órgão de pesquisa quem deverá provar que não era possível o uso de dados anonimizados para se alcançar os objetivos da pesquisa, ou que não era possível, metodologicamente, efetuar a anonimização antes da coleta. Ou melhor, deverá o órgão de pesquisa provar que era estritamente necessário e adequado usar dados pessoais cujos titulares estejam identificados ou identificáveis. Do contrário atuará em desacordo com a norma geral de proteção de dados.

Outra questão importante que se pode vislumbrar e que certamente trará dificuldades práticas é a seguinte: como o titular poderá ter certeza de que o controlador atendeu sua solicitação de correção ou, principalmente, de eliminação ou de anonimização dos seus dados pessoais? Seja na gestão direta dos dados pessoais perante o controlador, seja em uma situação de autocomposição ou em uma disputa judicial, como esta prova pode ser feita? Sem uma solução para esta questão o direito à autodeterminação informativa acabará sofrendo erosões consideráveis, sobretudo diante de pontos fracos da própria Lei. Um destes pontos parece ter sido as disposições da Seção IV sobre o Término do Tratamento de Dados, pois parecem ter

admitido uma contradição entre proteção e desproteção dos dados do titular que poderia seria mitigada com a solução das indagações anteriores.

O art. 15, inciso I prevê que, alcançada a finalidade da coleta ou a desnecessidade dos dados pessoais para a finalidade específica almejada, dar-se-ia o término do tratamento. Já o art. 16, caput, determina que após o término do tratamento os dados pessoais serão eliminados. Até aí há perfeita coerência. Porém, nos seus incisos III e IV, o art. 16 abriu exceções que podem acabar permitindo a substituição das finalidades específicas de tratamento iniciais por outras não previstas quando da coleta. Assim, de acordo com estes dispositivos, a critério exclusivo do controlador, e sem o consentimento do titular, após o término da finalidade inicial declarada ou implícita do tratamento, este poderá ser continuado para que ocorra a transferência dos dados pessoais a terceiros, respeitados os requisitos de tratamento da Lei (art. 16, III), ou poderão ser mantidos para uso exclusivo do controlador, desde que anonimizados (art. 16, IV). Fica a dúvida acerca de quais situações e requisitos legais facultariam uma transferência dos dados a terceiros de forma desvinculada das finalidades iniciais do tratamento. O risco destes dispositivos é que a duração do tratamento dos dados pessoais acabe ocorrendo por tempo indefinido, à revelia da vontade do titular e para finalidades distintas daquelas perante as quais ele consentiu na coleta. Para mitigar este risco serão necessários procedimentos transparentes de prova que atestem a correta anonimização ou eliminação dos dados pelos controladores, do contrário, tais dispositivos permitirão a erosão do direito à autodeterminação informativa e da força normativa da Lei Geral de Proteção de Dados.

Capítulo 02

Assimetria de poder no fluxo das informações pessoais

Para seguir adiante na busca de um esboço de procedimento para o exercício dos direitos dos titulares frente aos agentes de tratamento, parece necessário dar um passo atrás para se compreender melhor as posições destes sujeitos na relação jurídica que os vincula. Como e por que a relação de fornecimento e tratamento de dados pessoais se inicia? Que instrumentos cada uma das partes dispõe para gerenciar e controlar seus respectivos interesses no curso desta relação? Qual a capacidade de processamento que cada uma das partes dispõe para tanto?

2.1) Agentes de tratamento: capital, tecnologia e conhecimento especializado na conformação do ecossistema de tratamento de dados

Para uma melhor visualização das dimensões do setor da análise de dados e da economia baseada em dados e da organização dos seus fatores de produção, propõe-se aqui uma categorização da mesma em duas dimensões: vertical e horizontal. A dimensão vertical seria relativa à capacidade e robustez da tecnologia que suporta a atividade: capacidade de armazenamento e processamento envolvidos no processo de tratamento de dados. A dimensão horizontal seria relativa à complexa organização dos diversos atores envolvidos em um sistema de tratamento de dados, composto por distribuição de tarefas e especialização de funções. Nesta dimensão, o uso compartilhado de dados do titular é um recurso chave para a geração de riqueza.

Assim, buscando esboçar um singelo panorama da dimensão vertical, percebe-se pelas descrições da história dos modelos lógicos de organização de bancos de dados e dos suportes tecnológicos da ciência da computação que, quanto menor era a capacidade de processamento e armazenamento das máquinas, mais compartimentados e estruturados precisavam ser os bancos de dados. Logo, estes funcionavam com menor quantidade de informações, informações mais selecionadas e amostrais. A integração das informações entre bancos de dados diferentes e boa parte da extração de conhecimento dos dados era feita por pessoas, com seus recursos intelectuais que, embora especializados, tinham e têm a marca da cognição humana e suas limitações.

À medida em que a capacidade de processamento e armazenamento das máquinas aumenta, os bancos de dados vão passando a ser semiestruturados e finalmente não estruturados. Assim, passam a poder conter quantidades astronômicas de dados, quase dispensando a seleção dos mesmos e também o tratamento amostral, pois os sistemas de armazenamento e processamento suportam lidar com dados quase integrais acerca de alguns fenômenos que pretendem analisar[4]. Aqui a integração dos dados e a extração de conhecimento ocorre na própria máquina, cuja capacidade mnemônica e de processamento incansável supera a do ser humano em proporções que todos conhecem. O intelecto humano entra agora nesta relação com a máquina fazendo a ela perguntas e direcionando sua robusta capacidade de processamento para o universo dos dados que quer conhecer.

É o que se pode vislumbrar ao se comparar a linha de evolução dos modelos de bancos de dados de suporte à decisão na Figura 01 com o gráfico de evolução dos microprocessadores, conforme a Lei de Moore[5] na Figura 02.

Assim, dos bancos de dados dos sistemas de apoio à decisão dos anos 70, suportados em máquinas com microprocessadores com cerca de 10.000 transístores, aos bancos de dados no modelo Big Data e à Análise de Redes Sociais (dados completamente desestruturados) dos anos 2010 e seguintes, suportados por máquinas com microprocessadores com mais de 1 bilhão de transístores cada, chega-se, finalmente, aos processos atuais em que grandes bancos de dados (Datawarehouses) passam por processos de tratamento e processamento através de Deep Learning[6], suportados por máquinas com microprocessadores do porte dos TPUs (Tensorflow Processing Unit), microprocessadores

[4] A prescindibilidade de tratamento amostral de dados representa, por si mesma, mais uma ameaça à privacidade do titular, pois quanto mais amplo o repositório de dados sobre ele, mais identificáveis serão. Por outro lado, quanto mais amostrais, menos identificáveis serão com relação ao titular.

[5] "Em 14 de abril de 1965 o fundador da Intel, Gordon Moore, publicou na revista Electronics Magazine um artigo sobre o aumento da capacidade de processamento dos computadores. Moore afirma no artigo que essa capacidade dobraria a cada 18 meses e que o crescimento seria constante. Essa teoria ficou conhecida como a 'Lei de Moore'[...]". ALMEIDA, Bruno Rafael. Evolução dos Processadores. Comparação das Famílias de Processadores Intel e AMD. (p. 02). Disponível em https://www.ic.unicamp.br/~ducatte/mo401/1s2009/T2/089065-t2.pdf. Acesso em 03 nov 2020.

[6] "De forma simplificada, podemos dizer que deep learning são esses algoritmos complexos construídos a partir de um empilhamento de diversas camadas de 'neurônios', alimentados por quantidades imensas de dados, que são capazes de reconhecer imagens e fala, processar a linguagem natural e aprender a realizar tarefas extremamente avançadas sem interferência humana. A principal aplicação dos algoritmos de Deep Learning são as tarefas de classificação, em especial, reconhecimento de imagens". Fonte: Machine learning e Deep learnin: aprenda as diferenças. In: Salesforce blog. Disponível em: https://www.salesforce.com/br/blog/2018/4/Machine-Learning-e-Deep-Learning-aprenda-as-diferencas.html . Acesso em 28 out 2020.

que, estima-se, tenham entre 1 e 2,5 bilhões de transístores[7]. Ainda, encontra-se pela internet notícias[8] de desenvolvimento de chips pela IBM com cerca de 30 bilhões de transístores.

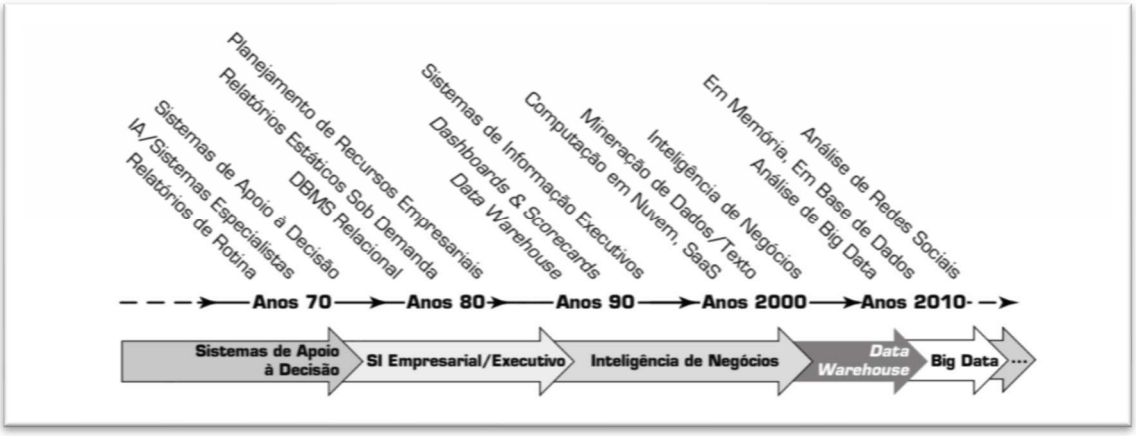

Figura 01: Evolução do apoio à decisão, inteligência de negócios e análise de dados. Fonte: Business Intelligence e Análise de Dados para Gestão do Negócio. p. 12

[7] Ver: Augusto, José Soares. What is the transistor count of Google's TPU ASIC? In: Quora. Disponível em: https://www.quora.com/What-is-the-transistor-count-of-Google%E2%80%99s-TPU-ASIC Acesso em 08 out 2020

[8] Ver: Novo chip de 5 nanômetros da IBM apresenta 30 bilhões de transistores. In: Techmundo. Disponível em: https://www.tecmundo.com.br/hardware/117395-novo-chip-5-nanometros-ibm-apresenta-30-bilhoes-transistores.htm Acesso em 08 out 2020

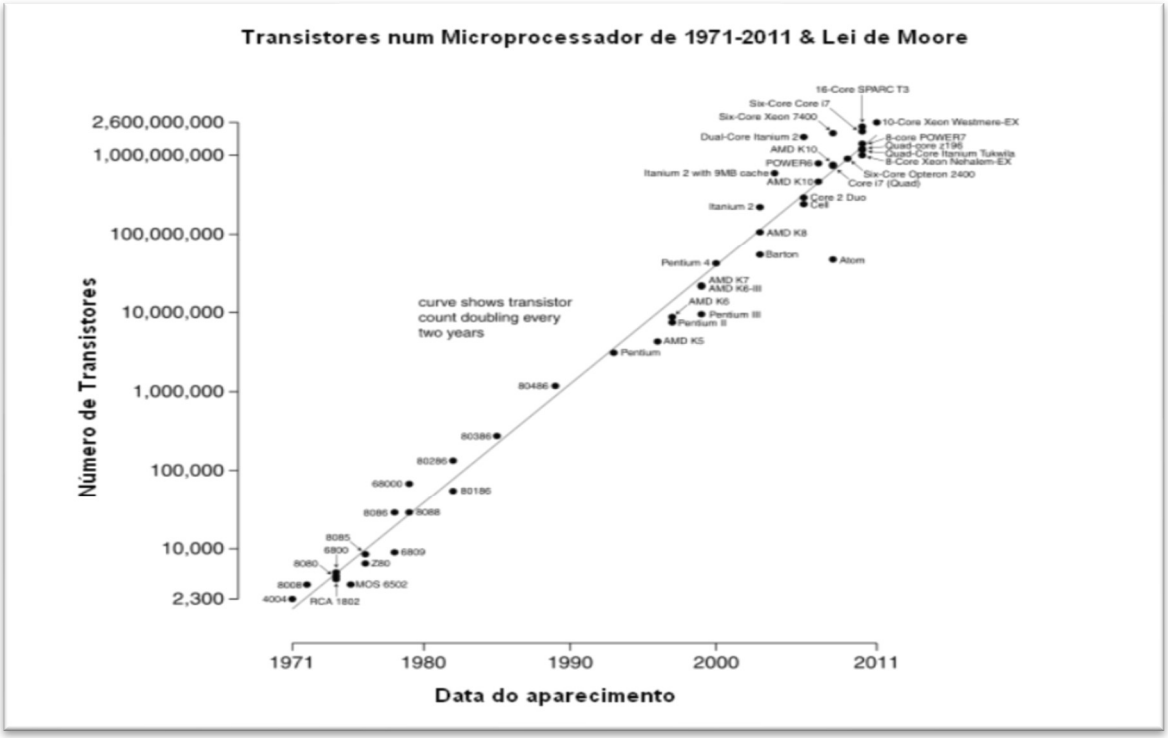

Figura 02: Lei de Moore até 2011. Fonte: https://www.newtoncbraga.com.br/index.php/eletronica/52-artigos-diversos/8084-a-lei-de-moore-art1177

Já na dimensão horizontal, para se vislumbrar a amplitude deste universo do tratamento de dados e da economia baseada em dados, a multiplicidade de atores envolvidos deve ser considerada. Sharda (2019) descreve esta multiplicidade de atores como um ecossistema de análise de dados. Para este autor, este ecossistema seria organizado na forma da Figura 03:

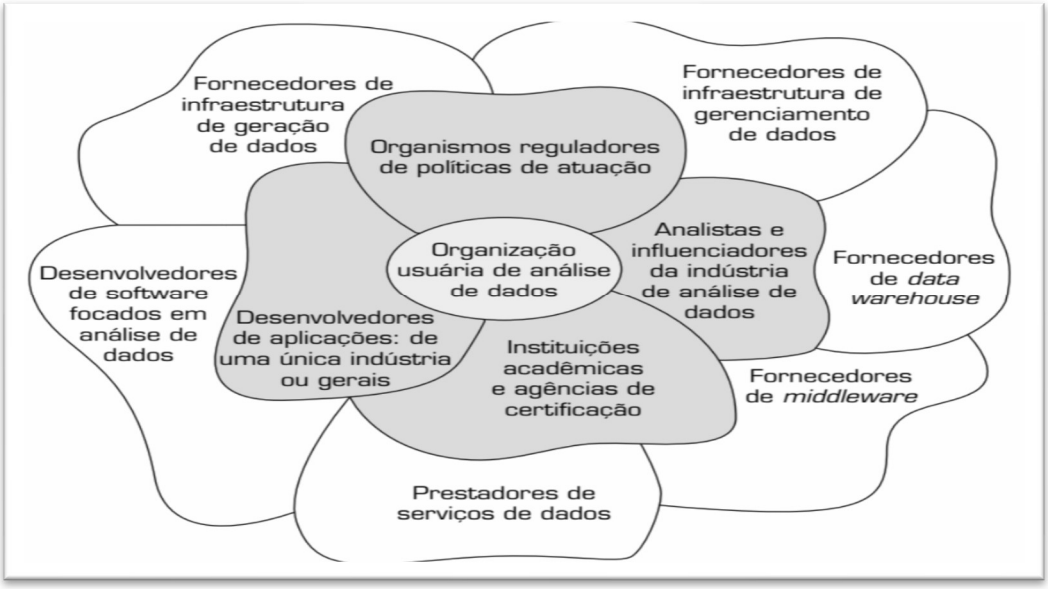

Figura 03: Ecossistema de análise de dados. Fonte: Sharda (2019, p. 43).

Cada uma das "pétalas" representa um agrupamento de organizações e atores que desempenham aquela função. Neste ecossistema, percebe-se que uma organização usuária, tal como a que está no centro da "flor" é secundada por inúmeras outras organizações e atores com papeis diferentes e em camadas diferentes deste sistema. Tanto dados operacionais das organizações usuárias quanto dados pessoais dos seus consumidores ou potenciais consumidores circulam por diversas organizações a fim de que cada elo ou "pétala" deste ecossistema extraia dele algum valor.

Consequência da amplitude deste ecossistema, e, em alguns dos seus elos, da sua habitual operação à margem de qualquer respeito por mínimos direitos dos titulares dos dados pessoais, é a existência, sobretudo nas estruturas de geração de dados, de um verdadeiro mercado de varejo ilícito de dados pessoais. Testemunho disso é a recente Ação Civil Pública 0730600-90.2020.8.07.0001 impetrada, já na vigência da LGPD, pelo Ministério Público do Distrito Federal e Territórios contra a empresa Infortexto e contra o Núcleo de Informação e Coordenação do Ponto Br – NIC.BR. Na inicial, o Parquet aduz que:

> "A Unidade Especial de Proteção de Dados e Inteligência Artificial, identificou a comercialização maciça de dados pessoais de brasileiros através do site intitulado "lembrete digital", com o domínio lojainfortexto.com.br registrado perante o Núcleo de Informação e Coordenação do Ponto BR. A título de exemplo, o mencionado site comercializa dados pessoais de 500.000 (quinhentas mil) pessoas naturais da cidade de São Paulo, consistentes em nomes; e-mails, endereços postais ou contatos para SMS, bairro, Cidade, Estado e CEPs".

Ilustrativo ver como a empresa ré dispunha o banco de dados pessoais à venda em seu site, conforme a Figura 04, extraída da inicial da referida ACP:

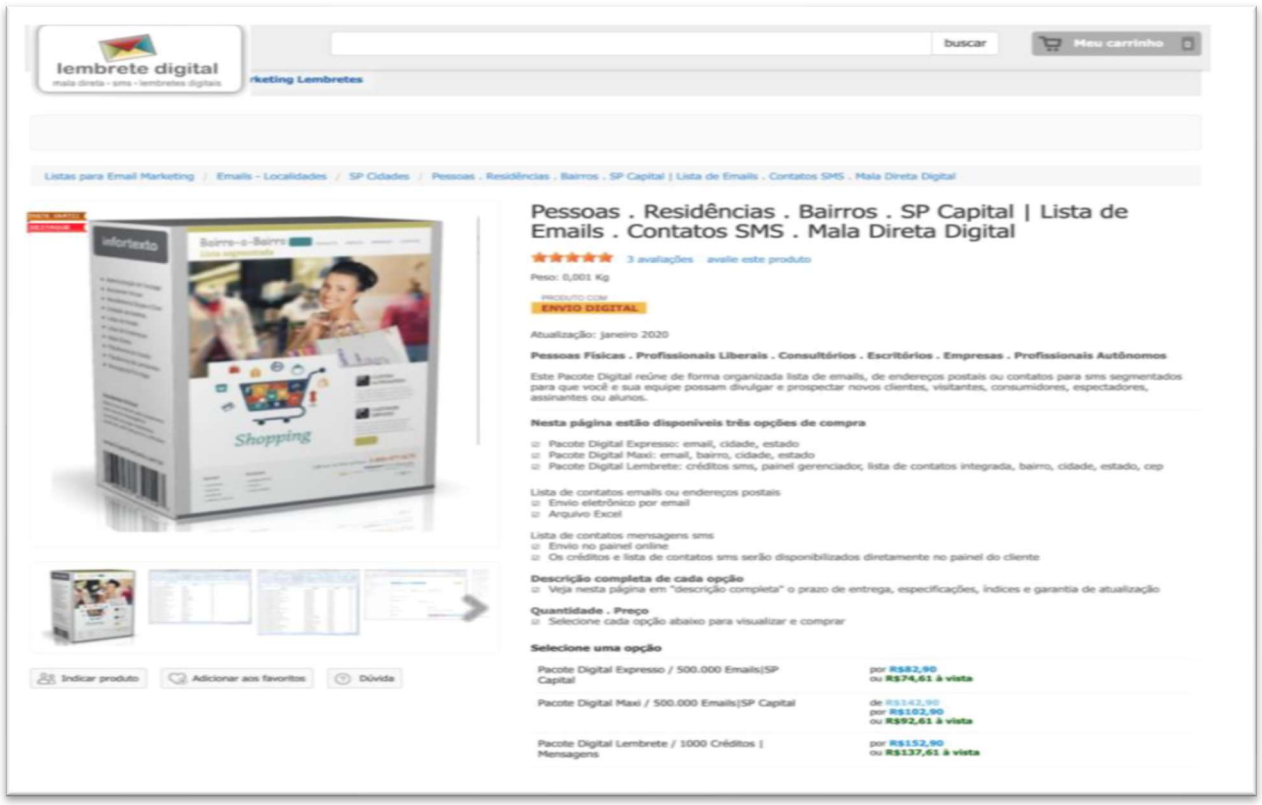

Figura 04. Fonte: Ação Civil Pública 0730600-90.2020.8.07.0001.

Por tudo isto, percebe-se que além da profundidade de captação, armazenamento e processamento de dados pessoais que o ecossistema mencionado fornece, há também o problema da amplitude do compartilhamento e circulação destes dados entre diversos atores do ecossistema, tornando a ideia de controle sobre os próprios dados pessoais, para o titular dos dados, uma verdadeira disputa de "David contra Golias", ou mesmo pior.

2.2) Titulares e os meios individuais de controle: consentimento e capacidade cognitiva; fadiga e impotência.

Tema recorrente quando se trata do avanço da tecnologia é o relativo a se e quando os computadores ou os robôs, enfim a inteligência artificial, se tornarão uma ameaça aos seres humanos. Pelo menos no que diz respeito à possibilidade de um mesmo robô, munido de uma inteligência artificial tal que o torne não só capaz de andar por aí, mas de realizar atividades humanas diversificadas e genéricas (dirigir um carro, fazer compras, sacar dinheiro em um caixa eletrônico, redigir um texto, fazer planos, entender notícias da política,

etc.), parece haver consenso de que a tecnologia ainda precisa muito que evoluir. Esta seria o que se chama de Inteligência Artificial Genérica[9]. Se e quando esta Inteligência Artificial Genérica poderia ser alcançada é questão bem controversa entre os especialistas[10]. Alguns acreditam que pode ocorrer em uma década, outros acreditam que possa ocorrer em 50 anos, e outros acreditam que pode ser quase impossível. Isto porque a Inteligência Artificial, por mais avançada que seja, é um sistema super especialista, de forma que aquela que é treinada para reconhecer imagens e/ou movimentos não é capaz de jogar xadrez ou GO, e vice versa.

Já a inteligência humana é uma inteligência genérica, racional e também intuitiva. É capaz de se adaptar e se auto aprimorar para responder a situações muito diversas, embora, algumas vezes, com um alto custo. O ser humano, ao contrário da máquina, se cansa, se entedia, se dispersa, se esquece e, por fim, tem pouco tempo! Esta relação foi belamente captada pelo compositor Gilberto Gil em sua canção "Cérebro Eletrônico":

O cérebro eletrônico faz tudo
Faz quase tudo
Faz quase tudo
Mas ele é mudo
O cérebro eletrônico comanda
Manda e desmanda
Ele é quem manda
Mas ele não anda[11]
Só eu posso pensar
Se Deus existe
Só eu
Só eu posso chorar
Quando estou triste
Só eu
Eu cá com meus botões
De carne e osso
Eu falo e ouço. Hum
Eu penso e posso
Eu posso decidir
Se vivo ou morro por que
Porque sou vivo
Vivo pra cachorro e sei
Que cérebro eletrônico nenhum me dá socorro
No meu caminho inevitável para a morte

[9] "É fato que o anseio pela criação de uma Inteligência Artificial Genérica (ou Geral), capaz de realizar as mais diversas atividades por meio de um 'algoritmo universal para aprender e atuar em qualquer ambiente', remonta à própria origem da Inteligência Artificial. Não obstante, trata-se de objetivo altamente complexo e inexequível com o nível de desenvolvimento tecnológico hodierno". (MEDINA e MARTINS, 2020, p. 2)

[10]Ver: Zuin, Lidia. Quão próximos estamos de criar uma inteligência artificial genérica? In: Medium. Disponível em https://medium.com/up-future-sight/qu%C3%A3o-pr%C3%B3ximos-estamos-de-criar-uma-intelig%C3%AAncia-artificial-geral-2e07e9cd0b7d. Acessado em 28 out 2020.

[11] A incapacidade do "Cérebro Eletrônico" de andar era uma verdade absoluta em 1969, ano de lançamento da canção. Hoje, é fato superado magistralmente pela tecnologia: vide o modelo Atlas da empresa Boston Dynamics. Disponível em https://www.bostondynamics.com/atlas. Acessado em 28 out 2020.

Porque sou vivo
Sou muito vivo e sei
Que a morte é nosso impulso primitivo e sei[...].

Não obstante as limitações acima apontadas, as pessoas são chamadas a lidar com o fenômeno da datificação do seu mundo da vida. Segundo Bioni(2020, p. 85) o termo datificação foi introduzido no contexto do Big Data por Viktor Mayer-Schonemerger, e quer dizer o registro em formato digital, passível de armazenamento e qualquer tipo de tratamento, pelos meios de computação disponíveis. Exemplo claro são as redes sociais. Elas têm se tornado gigantescos repositórios dos mais diversos tipos de dados possíveis (dados não estruturados) sobre o usuário: textos, fotos, vídeos, áudios; opiniões sobre todos os âmbitos da vida, relacionamentos, padrões de comportamento, dentre outros. Segundo Van Dijck (2013, apud WIELSCH, 2020, p. 97) o advento de a rede de computadores se tornar social significa tornar "[...] a socialidade técnica. A socialidade codificada pela tecnologia torna as atividades das pessoas formais, gerenciáveis e manipuláveis". A datificação da vida não só tem criado novas condições de socialização, não só virtualizado a socialidade, mas também as tem tornado manipuláveis de acordo com critérios comerciais e com os interesses lucrativos de corporações.

Assim, via de regra, temos uma organização com fins lucrativos como fornecedora de uma infraestrutura de sociabilidade através de aplicações e serviços que promovem a coleta dos dados. Sendo a relação dos titulares dos dados com estas organizações relações privadas, são elas mediadas por contratos denominados Termos de Uso ou Termos de Serviço. Na perspectiva individualista do direito contratual, a aceitação dos termos pressuporia um assentimento mútuo, consciente e esclarecido entre as partes. Porém, os Termos de Serviço são, na maioria, contratos de adesão em que o fornecedor da aplicação ou serviço dita todas as regras e condições de participação dos titulares neste ambiente de sociabilidade privatizada, como no caso das redes sociais; ou como condição para acesso ao conhecimento facilitado pelos motores de busca na internet; ou como condição para o acesso a descontos que podem chegar a 50% do preço em estabelecimentos comerciais como drogarias. Segundo Wielsch (2020, p. 103)

> Da perspectiva econômica, a não negociação de termos e condições de uso é a expressão de uma falha parcial do mercado, devida a assimetrias de informação entre utilizador e cliente[...]. Isso se aplica com maior razão no caso de oferta de uma prestação de serviços complexa [...].

Tal situação é evocada para apontar as limitações e dificuldades dos titulares para consentir de forma consciente e esclarecida. Se esta dificuldade já é desproporcional com relação a um único Termo de Serviço, o que dizer sobre as dezenas ou centenas de Termos de Serviço com que uma pessoa tem que lidar rotineiramente para o uso das diversas facilidades que lhe são oferecidas, sem falar nas diversas atualizações por que passam estes contratos. Além da impossibilidade cognitiva de uma pessoa examinar de forma exaustiva todos os Termos de Uso a que anui, há ainda a dificuldade imposta pelo modelo de persuasão utilizado pelas políticas de fornecimento de uso gratuito de facilidades em troca dos dados pessoais. Em termos de tempo de espera ou de latência, os benefícios do fornecimento dos dados são imediatos e contíguos ao comportamento de consentir, o que gera um fortalecimento deste comportamento. Por outro lado, os prejuízos relacionados a este comportamento ocorrem de forma dispersa, distantes no tempo, e sua vinculação ao comportamento só é possível através da mediação de uma série de raciocínios abstratos e percepções pouco disponíveis. Assim, é bastante difícil se associar os prejuízos decorrentes do uso abusivo dos dados pessoais por terceiros ao comportamento de consentir na sua coleta. Tal dinâmica há muito foi identificada pela psicologia comportamental. Dentre outros, Keller & Shoenfeld (1970, apud DEL PRETTE 2012).

Diferentemente da vulnerabilidade presente em relações como as trabalhistas e consumeristas tradicionais, em que os prejuízos para a parte vulnerável são mais facilmente mensuráveis: horas a mais trabalhadas, valores pecuniários não pagos, condições de trabalho desrespeitadas, cobrança de preço desproporcional por um produto, produto com qualidade aquém do esperado, dentre outros. O prejuízo da vulnerabilidade na relação de fornecimento de dados pessoais é difuso no tempo. Seja atingindo uma coletividade ou o indivíduo, não é mensurável de forma direta. Sabe-se que, quanto mais dados coletados, quanto mais sensíveis forem, quanto maior o tempo de coleta e tratamento e quanto maior a extensão do compartilhamento com terceiros, maior o prejuízo à autodeterminação informativa, menos as decisões do titular sobre seus dados poderão ser respeitadas, mais ele estará exposto e sujeito a ingerências indesejáveis sobre sua vida pessoal e sobre suas decisões, e mais a coletividade terá seus mecanismos de escolha democrática viciados ou *hackeados*. Diferentemente de uma relação consumerista tradicional, em que, regra geral, o consumidor e o fornecedor se relacionam de forma pontual ou, quando em uma relação continuada, têm objetos de troca bastante claros e limitados, na relação de compartilhamento de dados pessoais, muitas vezes se trata de relações continuadas (e muito intensivas), há troca de

serviços por bens jurídicos irrenunciáveis e infungíveis, posto que os dados fornecidos são referentes a uma personalidade humana. O dano decorrente da perda de controle do titular sobre este bem jurídico, o dado pessoal, pode ser irreparável e duradouro: informações sensíveis cuja possibilidade de mapeamento do uso por agentes de tratamento se perdeu são informações que poderão ser usadas contra os interesses do titular permanentemente.

Solução normalmente apontada é a da regulamentação destas relações, seja por meio de leis em sentido amplo, seja por meio de uma autoridade reguladora e fiscalizadora. Ambas são muito necessárias, porém, parecem insuficientes. Explanando acerca dos Termos de Serviço no contexto das redes sociais à luz de dispositivos do Código Civil alemão, Wielsch (2020, p. 103), aduz que

> A vinculatoriedade jurídica na relação horizontal não pode resultar de um consenso transacional alcançado entre as partes sobre todos os conteúdos relevantes (df. art. 154 e ss. do Código Civil alemão), mas deriva, sim, de uma concordância global com a validade[...].

Esta validade é relativa às normas que regulamentam a atividade e servem de parâmetro de controle dos Termos de Serviço. Assim, quando o titular dos dados consente na relação com os agentes de tratamento mediante o Termo de Serviço, o fundamento da validade do seu consentimento é menos a autonomia privada e mais a confiança na conformidade desta relação com o parâmetro regulatório, bem como na boa fé objetiva a que devem obediência os agentes de tratamento.

Importante sugestão de Bioni (2020, p. 166) seria "investigar como a tecnologia poderia massificar as escolhas dos consumidores sobre o trânsito de seus dados pessoais para toda a miríade de atores do mercado informacional". Assim, os dispositivos eletrônicos de acesso aos serviços e aplicações do titular já conteriam as disposições de compartilhamento de dados pessoais em que ele consente ou não, e então caberia aos fornecedores dos serviços e aplicações aceitar ou recusar a relação conforme houvesse acordo entre ambos. Seria a massificação das escolhas do titular, ou um tipo de contrato de adesão ao inverso, graças a um suporte tecnológico configurado para armazenar as preferências de compartilhamento de dados do titular.

Certamente seria uma medida útil, mas, de certa forma, ainda estaria no âmbito da regulamentação contratual e neste sentido, a extensão da sua utilidade pode ser limitada. Nesse modelo de relação duradoura e de intensivo fluxo de dados, a garantia do fiel

cumprimento dos termos do contrato e da norma geral regulatória é o maior desafio. Uma peculiaridade dos dados pessoais é que uma vez rompido o elo de controle do titular sobre eles, seus danos estão consumados ou potencialmente consumados. Por isto a regulamentação e fiscalização estatal é necessária, mas não suficiente. Os titulares precisam de mecanismos de sindicabilidade individual do cumprimento da norma geral ou do contrato durante a execução do serviço e do tratamento dos seus dados ou o mais próximo disto, pois do contrário, o controle acabará sendo apenas *ex post*.

Bioni (2020, p. 165) alerta para a necessidade de um controle *ex ante* da conformidade do tratamento dos dados do titular e parece crer que a regulação teria o condão de fornecer tal controle:

> "(...)a proteção contratual do consumidor no âmbito das políticas de privacidade não deve ser vista como o mecanismo ideal para a proteção dos dados pessoais. Deve ser encarada como uma ação paliativa se a causa regulatória primária falhar, qual seja, o empoderamento ex ante do cidadão para exercer um controle genuíno sobre seus dados pessoais".

Com a devida vênia, a expectativa de que a regulação seja suficiente para empoderar o titular para o exercício do controle dos seus dados parece inadequada. Vale dizer, aposta-se aqui que a regulamentação e o poder de polícia estatal não serão suficientes para gerar o *enforcement* adequado nos controladores para a garantia da privacidade e da autodeterminação informativa do titular. Haja vista que após 30 anos de vigência do Código de Defesa do Consumidor e da existência do Sistema Nacional de Defesa do Consumidor composto por Procons, Ministério Público, Defensoria Pública, Delegacias de Defesa do Consumidor, Juizados Especiais Cíveis e Organizações Civis de defesa do consumidor, ainda hoje a violação dos direitos do consumidor é flagrante. Segundo dados do "Consumidor em Números", sistema de integração de informações dos Procons e do Consumidor.gov.br, em 2018 ocorreram 2.883.835 reclamações nestes dois sistemas. O índice de solução foi de 76,5% dos Procons e de 81% do Consumidor.gov.br[12]. São, porém, soluções *ex post*. Embora possam ser adequadas na proteção do consumidor por solucionar situações com objeto específico e delimitado, como prestação de serviço de telefonia ou serviços bancários, parecem insuficientes para a solução de violações a direitos em matéria

[12]Consumidor em Números Reclamações de consumo em 2018. In: Ministério da Justiça e Segurança Pública. Governo Federal. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1552676889.94/arquivos/consumidor-em-numeros-2018_portal.pdf. Acessado em 28 out. 2020.

de proteção de dados, pois aqui, as soluções *ex post*, embora possam responsabilizar os controladores e ressarcir em parte os danos provocados, não serão capazes de impedir a erosão do bem jurídico protegido: a garantia do direito fundamental à autodeterminação informacional e da privacidade na forma da proteção de dados pessoais, dada a natureza mais fluida deste bem jurídico.

Pelo exposto, confrontados os recursos e meios de fazer valer os próprios interesses dos titulares dos dados pessoais de um lado, e os dos agentes de tratamento, detentores dos meios de produção de serviços baseados em dados de outro lado, fica evidente a hiper vulnerabilidade dos primeiros. A regulamentação do setor e o poder de polícia estatal, bem como Termos de Serviço consentâneos à legislação e que considerem o consentimento do titular, são de suma relevância, mas são insuficientes, pela própria natureza fluida dos dados. Se os necessários meios de solução de conflitos ou irregularidades administrativos, auto compositivos e judiciais também são insuficientes por terem pequena eficácia protetiva *ex ante*, cabe buscar meio que seja passível de instrumentalizar a regulamentação e a sindicabilidade dos direitos do titular de forma concomitante ao tratamento dos seus dados.

Aqui parece haver uma lacuna protetiva, que, também pela característica própria do objeto protegido e dos meios de sua exploração, precisará ser colmatada por instrumentos que se valham de toda tecnologia disponível, voltada agora para a sindicância do tratamento ou de aspectos sensíveis do mesmo, ou seja, uma tecnologia que permita ao titular seguir os seus dados durante o seu fluxo de tratamento, ou que se aproxime disto.

Capítulo 03

Tecnologias de Facilitação de Privacidade (Privacy Enhancing Technologies - PETs)

Neste ponto tenta-se demonstrar que a lacuna protetiva deixada pela regulamentação e poder de polícia estatal, bem como pelos Termos de Serviço, poderá ser coberta de forma eficaz através da conjugação dos direitos dos titulares previstos na Lei com tecnologias que instrumentalizem o titular com a possibilidade de obter conhecimento simples e facilitado acerca do tratamento que seus dados pessoais recebem, em tempo hábil a permitir que ele tome decisões a respeito da continuidade da relação, da solicitação de providências de correção, ou acione mecanismos de autocomposição ou heterocomposição. Aqui estaríamos no campo da sindicância ou auditoria privada e personalizada.

Importante mencionar que um meio termo entre a regulamentação e fiscalização estatal e a sindicância privada seriam os procedimentos de credenciamento por entidades certificadoras e de padronização técnica. No caso da privacidade e proteção de dados, há a norma ABNT NBR ISO/IEC 27701: norma técnica de segurança que prevê requisitos e diretrizes para a gestão da privacidade da informação[13]. O processo de credenciamento de uma empresa nesta norma prevê uma série de adequações e auditorias periódicas pelo ente que fornece a acreditação. Esta acreditação e conformidade com normas técnicas de certificação fornece certa segurança para os clientes da empresa certificada, pois significa que ela está se submetendo à auditoria de uma entidade externa independente, que detém legitimidade entre seus pares e que zela pela legitimidade dos seus certificados. Porém, dois aspectos restam descobertos por este procedimento: este credenciamento é voluntário, portanto, não pode ser exigido dos controladores de dados. A conformidade perante a Lei é exigível de todos os agentes de tratamento, mas a conformidade perante um determinado ente certificador não o é. O ato de se credenciar perante esses entes certificadores apenas depõe a favor do agente de tratamento, pois além da sindicância estatal a que todos estão sujeitos por força da Lei, significa que ele tem a intenção de atuar em conformidade com a Lei e com as melhores práticas do seu ramo de atuação, bem como aceita ser auditado por um ente externo independente e não estatal. Outro ponto que fica a descoberto é que o titular do dado, individualmente, ainda terá o trabalho de saber se, no seu caso particular, o tratamento feito por um controlador específico, embora esteja em conformidade com as

[13] Vem aí a ABNT NBR ISO/IEC 27701. In ABNT. Disponível em http://www.abnt.org.br/images/Docspdf/Artigos/Artigo_27701.pdf. Acessado em 28 out. 2020.

melhores práticas, seria ainda passível de lhe causar algum dano ou de erodir a sua autodeterminação informativa. Por exemplo, no caso de coleta de dados biométricos em que a finalidade do tratamento dada pelo controlador, embora legítima e conforme às boas práticas, pode estar extrapolando a legítima expectativa[14] do titular, sendo, pois, seu direito conhecer este fato e poder escolher outro fornecedor de serviços cujo escopo de tratamento destes dados seja mais consentâneo com a sua expectativa pessoal.

Esta sindicabilidade ou auditabilidade privada, como se quer denotar aqui, tomará como ponto de partida e como condição de possibilidade os direitos dos titulares previstos na Lei, mas poderá e precisará ser embarcada em alguma tecnologia que facilite o gerenciamento pessoal pelo titular dos dados fornecidos a um ou a vários agentes de tratamento. A falta desta "tecnologia protetiva de direitos" seria mesmo um vácuo a ser preenchido por novos formatos de serviços de garantia de direitos, uma vez que o setor de coleta e tratamento de dados é caracterizado hoje pelos três "Vs" típicos do "Big Data": Volume, Variedade e Velocidade. Assim, como poderia a atuação tradicional e "analógica" do direito fazer face a estes três "Vs"? Como poderia o direito fornecer ao titular um suporte que dê conta da variedade, do volume e da velocidade da coleta e tratamento de dados quando, nesta seara, a perda do controle dos dados por um lapso de tempo curto, em apenas um dos múltiplos campos da coleta, pode ser suficiente para uma grande erosão no direito do titular? Isto sem falar na Internet das Coisas (IoT), que está apenas começando, com a coleta e compartilhamento de dados muito mais presente, automática e massiva[15]. Parece haver uma desproporção de armas também entre o setor tecnológico e a atuação tradicional do direito

[14] Parece possível vislumbrar que o conceito jurídico aberto de "Legítima Expectativa" (previsto no art. 10, II da LGPD) comportará uma dimensão coletiva, que servirá de parâmetro, por exemplo, para se delimitar até onde pode ir o tratamento feito com base no "Legítimo Interesse do Controlador" (previsto no art. 7º, IX da LGPD), mas também pode ser importante considerar a "Legítima Expectativa" de um grupo de pessoas ou de uma pessoa em particular. Desta feição particularizada da "Legítima Expectativa", embora não resulte uma normatividade geral, pode resultar uma normatividade para o caso concreto, a ser reconhecida por uma decisão judicial, ou, no mínimo, a fundamentar a decisão do titular de romper a relação jurídica com determinado controlador e solicitar a eliminação dos seus dados.

[15] Não à toa, já se tem falado no meio tecnológico em *"Deep Privacy"*. De modo simplificado, seriam modelos lógicos, envolvendo inteligência artificial, presentes nos dispositivos de IoT que fariam uma espécie de filtragem dos dados coletados e transmitidos por ele para que somente sejam transmitidos dados necessários à finalidade do serviço, excluindo ao máximo dados pessoais desnecessários. Exemplo seria um veículo autônomo que, ao transmitir dados de imagem dos pedestres ao servidor ou a outros dispositivos de IoT, realize, automaticamente e antes da transmissão, uma filtragem nos dados das imagens de modo a tornar os rostos não identificáveis. A anonimização dos dados pessoais tenderia a ocorrer no próprio dispositivo em que são coletados, antes de serem transmitidos pela rede a que está conectado. Para mais informações: OSIA, Seyed Ali et al. A Hybrid Deep Learning Architecture for Privacy-Preserving Mobile Analytics. IEEE Internet of Things Journal, May 2020. Disponível em https://arxiv.org/abs/1703.02952.

que requer uma adequação de instrumentos. Há assim um campo importante a se explorar quanto ao uso de suporte tecnológico para a efetivação da sindicabilidade privada sobre os dados do titular permitida pela Lei Geral de Proteção de Dados. Esta tecnologia poderia ser enquadrada entre as Tecnologias de Facilitação da Privacidade ou *Privacy Enhancing Technologies* (PETs). Este, segundo Bioni (2020, p. 167), seria um "termo que, como um guarda-chuva, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade".

3.1) PETs no nível da coleta

Estas tecnologias têm sido desenvolvidas para atuar em um ou mais de um aspecto do ciclo de tratamento de dados pessoais. Quando atuam no próprio desenho lógico de funcionamento do serviço ofertado representariam a concretização do princípio de *Privacy by Design and Default*. Como explica Arbix (2020, p. 57):

> A proposta de by Design and Default é que o planejamento atento à privacidade preceda o processamento de dados pessoais, ou seja, que potenciais problemas com a privacidade dos titulares sejam identificados e solucionados no início do ciclo de desenvolvimento de um produto ou serviço ou de sua nova versão, antes de seu lançamento no mercado.

Dentre estas tecnologias, as Do Not Track (DNT) e as Platform for Privacy Preferences (P3P) são lembradas por Bioni (2020), e, segundo este autor, ambas seriam formas de fazer valer as escolhas dos titulares no plano da coleta dos dados pessoais. O DNT é configurado no navegador de acesso aos sites da internet e impediria a atuação de mecanismos de rastreamento diversos, conforme a escolha do usuário. Outras ferramentas voltadas para o controle da coleta são as Platforms for Privacy Preferences (P3P). Segundo o W3C – World Wide Web Consortium[16], o P3P seria uma forma de padronização das políticas de privacidade de forma a permitir que o usuário manifestasse seu consentimento ou não consentimento apenas uma vez através da P3P, que se tornaria o padrão das suas escolhas frente a qualquer outra aplicação. Uma das dificuldades em relação a este método está na ausência de obrigatoriedade da adoção deste modelo padrão de política de privacidade.

3.2) PETs de gerenciamento

[16]Platform for Privacy Preferences (P3P) Project Enabling smarter Privacy Tools for the Web. In W3C. Disponível em https://www.w3.org/P3P/. Acessado em 28 out. 2020

Outras duas PETs bastante interessantes citadas por Bioni (2020) são o Lightbeam e o Polisis. Cada uma destas aplicações, ao seu modo, pode ajudar o titular a gerenciar o uso dos seus dados. O Lightbeam é uma ferramenta desenvolvida para ser uma extensão do navegador web que possibilita a visualização, através de animações gráficas, da relação entre o site visitado pelo usuário e sites ou aplicações de terceiros. A Figura 05 abaixo é uma visualização da animação gráfica do Lightbeam extraída após o acesso a 12 sites no dia 26 de outubro de 2020. Conforme descrito acima da animação gráfica, para estes 12 sites outros 56 sites ou aplicações de terceiros receberiam de alguma forma dados relacionados ao acesso.

O Polisis, por sua vez, é uma aplicação disponível no site *https://pribot.org/*. A ferramenta se propõe a ser uma estrutura automatizada para análise de políticas de privacidade[17] através do uso de *processamento de linguagem natural*[18]. Dentre várias informações que esta aplicação extrai de uma Política de Privacidade, sobressaem, no que diz respeito ao potencial de suporte e empoderamento do titular, as visualizações gráficas que permitem perceber, por exemplo, os tipos de dados coletados e suas razões ou finalidades e os tipos de dados compartilhados com terceiros e as razões do compartilhamento.

No dia 26 de outubro de 2020, realizou-se consulta ao Polisis, no site acima indicado, acerca da Política de Privacidade do site *amazon.com.br*. A Figura 06 é uma ilustração demonstrando quais dados são coletados pela *amazon.com.br* para uso próprio. Do lado esquerdo aparecem os tipos de dados coletados e do lado direito aparecem as razões ou finalidades da coleta. Cada tipo de dado coletado é ligado a uma ou mais de uma finalidade de coleta através de faixas. Na aplicação, ao se posicionar o cursor sobre os tipos indicados, aparece pequeno quadro descritivo acerca de cada um deles. Já a Figura 07 é uma ilustração sobre como os dados coletados pela *amazon.com.br* são compartilhados com terceiros. Do lado esquerdo são elencados os tipos de dados que são compartilhados e do lado direito as razões ou

[17] Harkous, Hamza. Et All. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. Disponível em: https://pribot.org/files/Polisis_USENIX_Security_Paper.pdf. Acessado em 28 out. 2020.

[18] Processamento de língua natural (PLN) é uma subárea da ciência da computação, inteligência artificial e da linguística que estuda os problemas da geração e compreensão automática de línguas humanas naturais. Sistemas de geração de língua natural convertem informação de bancos de dados de computadores em linguagem compreensível ao ser humano e sistemas de compreensão de língua natural convertem ocorrências de linguagem humana em representações mais formais, mais facilmente manipuláveis por programas de computador. Alguns desafios do PLN são compreensão de língua natural, fazer com que computadores extraiam sentido de linguagem humana ou natural e geração de língua natural. Fonte: Processamento de linguagem natural. In: Wikipédia. A enciclopédia livre. Disponível em https://pt.wikipedia.org/wiki/Processamento_de_linguagem_natural. Acessado em 28 out. 2020.

finalidades do compartilhamento. Cada tipo de dado compartilhado é ligado por uma faixa a uma ou mais razões de compartilhamento.

Embora os Termos de Uso e as Políticas de Privacidade não sejam mais a fonte principal de regulação da relação entre o controlador e os titulares, uma vez que esta função agora é desempenhada pela Lei, estes Termos são importantes para verificar a finalidade da coleta, os tipos de dados coletados, quem são os terceiros com quem se fará uso compartilhado dos dados, dentre outros aspectos típicos daquela relação jurídica ou do âmbito e escopo do tratamento feito por aquele controlador.

Ferramentas como as descritas são modos engenhosos de se propiciar ao titular maneiras de se conscientizar acerca do uso dos seus dados e das possíveis implicações do seu consentimento e uso de determinados serviços. Contudo, ainda demandam um esforço acentuado e um grande dispêndio de tempo do titular, uma vez que ele precisaria verificar uma a uma, com tais ferramentas, as demais aplicações que utiliza. E além do mais, estas duas ferramentas descritas estão adstritas aos sites acessados via navegador web, deixando de fora deste escrutínio, muitos dos aplicativos para dispositivos móveis.

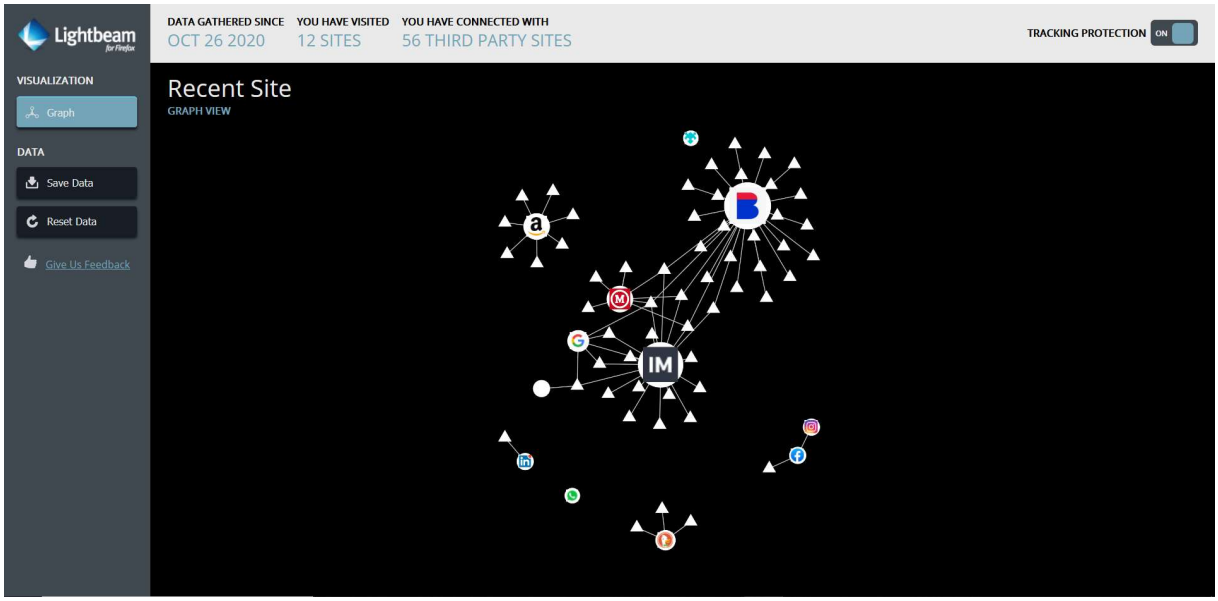

Figura 05. Ilustração do Lightbeam. Fonte: moz-extension://3f17c22e-14b5-4c38-a186-7dfa90cfc9a8/index.html

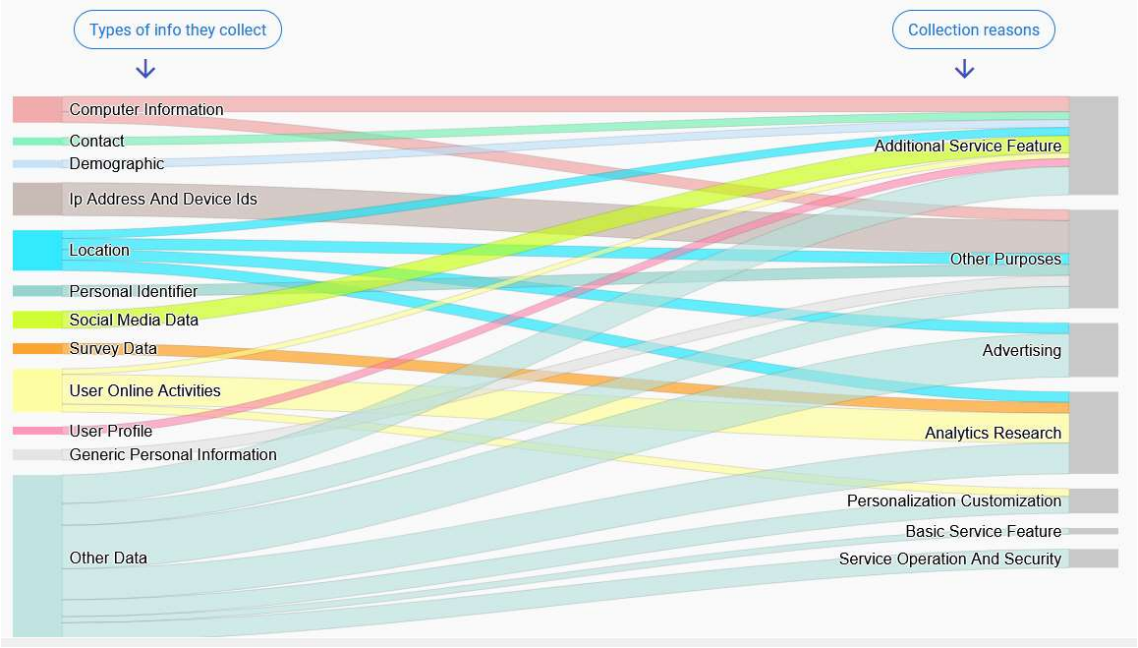

Figura 06. Ilustração do Polisis – Dados coletados para uso próprio. Fonte: https://pribot.org/polisis/?_id=5ae5b1a77331f740be5c1d16&company_url=amazon.com.br&category=first-party-collection-use

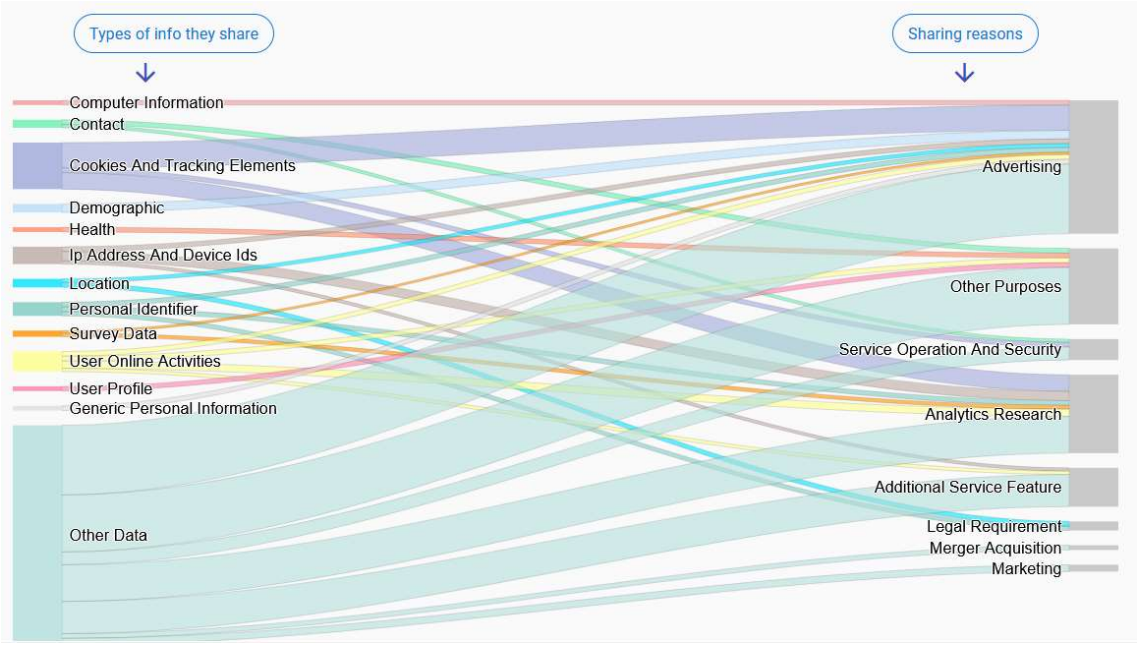

Figura 07. Ilustração do Polisis – Dados compartilhados com terceiros. Fonte: https://pribot.org/polisis/?_id=5ae5b1a77331f740be5c1d16&company_url=amazon.com.br&category=first-party-collection-use

3.3) PETs de gerenciamento centradas no usuário

Sob a vigência da General Data Protection Regulation (GDPR), vários serviços que podem ser considerados PETs têm surgido, ou se tracionado, em território europeu, com modelos de negócio voltados para o gerenciamento dos dados pessoais dos titulares. Uma ótima seleção destes serviços é encontrada na página do MyData Global. Esta é uma organização sem fins

lucrativos que tem o objetivo de capacitar os indivíduos melhorando seu direito à autodeterminação em relação aos seus dados pessoais[19]. O MyData Global adota o *paradigma centrado no ser humano*, confome o descreve: *"The human-centric paradigm is aimed at a fair, sustainable, and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationship between individuals and organisations"*[20]. Com base neste paradigma, é realizado anualmente o MyData Operator Award em que a organização confere reconhecimento e premia operadores de infraestrutura que colocam o indivíduo no centro do gerenciamento dos seus dados pessoais e buscam garantir que eles sejam os principais beneficiários dos seus dados. Dentre os 23 operadores premiados em 2020, destaca-se a seguir três deles. As descrições de cada um (em tradução aproximada) foram extraídas das autodescrições apresentadas pelos próprios operadores quando da inscrição no MyData Operator Award 2020[21].

- **BitsAboutMe**

> "BitsaboutMe é uma plataforma online inovadora onde os usuários podem gerenciar com segurança sua vida digital e fazer negócios justos de dados com empresas e organizações. No coração do BitsaboutMe está a privacidade de cada usuário individual. Eles podem mesclar suas contas online em um só lugar, obter uma visão geral transparente de 360 graus de suas vidas digitais e, assim, recuperar o controle total sobre seus dados pessoais. A função de mercado permite que os usuários compartilhem partes de seus dados pessoais com segurança com empresas e organizações em troca de uma recompensa ou anonimamente para fins de pesquisa". (Tradução nossa).

Esta é uma empresa suíça cujos serviços são oferecidos ao consumidor (B2C). Exemplos de casos de uso da aplicação são apresentados na descrição, de onde se extrai os trechos seguintes:

> "Depois de se inscrever no BitsaboutMe, os usuários importam seus dados online para o Personal Data Store (PDS) criptografado individualmente na nuvem privada BitsaboutMe. Uma vez que os conjuntos de dados de perfis de mídia social, contas online / e-mail, sites de comércio eletrônico, plataformas de streaming ou programas de fidelização de clientes são mesclados, é possível navegar pelos dados com a pesquisa de texto completo e usando os filtros. Todos os dados são apresentados em um painel e intuitivamente compreensíveis com a ajuda de ferramentas de análise pré-configuradas. A análise detalhada configurável por fonte de dados permite insights mais profundos sobre os próprios dados.

[19] Fonte: https://mydata.org/about/
[20] Em tradução livre: *"o paradigma centrado no ser humano visa uma sociedade digital justa, sustentável e próspera, onde o compartilhamento de dados pessoais é baseado na confiança, bem como no relacionamento equilibrado e justo entre indivíduos e organizações".* Fonte: https://mydata.org/about/
[21] Fonte: https://mydata.org/mydata-operators/

Usando widgets interativos, os usuários podem mapear seu próprio comportamento em períodos de tempo ou geografias definidas". (Tradução nossa).

O serviço ainda se propõe ser um intermediário confiável para o compartilhamento dos dados do usuário com terceiros que deles pretendam extrair ganhos comerciais, porém com o consentimento do titular, garantindo a conformidade do uso compartilhado com a GDPR e permitindo que o titular dos dados seja remunerado pelo uso dos seus dados por terceiros. A plataforma estabelece limites de segurança para o compartilhamento e as propostas de terceiros para o uso de dados dos titulares só são admitidas após uma análise de conformidade com regras do serviço.

- **Digi.me**

"O Digi.me facilita que os indivíduos compartilhem mais e melhores dados para permitir que as empresas forneçam mais e melhor valor, com privacidade, segurança e consentimento.

Os indivíduos podem recuperar automaticamente uma cópia completa de seus dados de saúde, finanças, sociais, vestíveis e de mídia hoje, usando o aplicativo digi.me em qualquer dispositivo. Esses dados são todos normalizados automaticamente no recebimento e armazenados em nuvem pessoal do indivíduo criptografada com a chave exclusiva do indivíduo mantida apenas em seu dispositivo. O indivíduo pode ver e pesquisar seus próprios dados usando o aplicativo digi.me.

Os usuários de dados podem então usar o Certificado de Consentimento do digi.me e API / SDKs de consentimento para solicitar aos indivíduos seus dados para uma troca de valor e, se o indivíduo der consentimento, seu aplicativo digi.me extrai os dados relevantes e os passa para o aplicativo / serviço . O indivíduo tem um painel de consentimento total para revisar e controlar os consentimentos dados.

Em todos os momentos, o digi.me nunca vê, toca ou segura os dados de um indivíduo. Digi.me é uma plataforma em serviço". (Tradução nossa).

Esta empresa é registrada no Reino Unido, nos Estados Unidos, na Holanda e na Bósnia. Sua proposta é bastante semelhante à da empresa descrita anteriormente: centralizar os dados do usuário e permitir que ele os gerencie em um só lugar, inclusive fornecendo e administrando o consentimento para o uso por terceiros.

- **Myfairdata**

"Fair & smart é uma empresa francesa de SaaS fundada em 2016 que desenvolveu uma plataforma centrada no ser humano para a governança de dados pessoais. Ele permite o armazenamento, gerenciamento e transferência de dados pessoais entre indivíduos e organizações com total auditabilidade, conformidade de privacidade e criptografia de ponta a ponta.

> Myfairdata é o nome B2C da plataforma: um aplicativo web e móvel que permite aos indivíduos proteger e compartilhar dados, gerenciar permissões e enviar solicitações GDPR (portabilidade, acesso ...)". (Tradução nossa).

A transcrição de uma possível situação prática de uso descrita por este Operador é bastante relevante, pois já descortina um ponto chave destas tecnologias de aprimoramento da privacidade que é a operacionalização das "*solicitações GDPR*":

> "Um indivíduo precisa recuperar dados de uma ou várias organizações (por exemplo, registros de exames médicos de laboratórios independentes) para compartilhá-los com um serviço de uso de dados que ele ou ela considere útil (por exemplo, coaching pessoal para viver melhor com sua doença crônica). Graças ao Myfairdata, eles podem facilmente enviar solicitações de direitos de acesso para essas organizações. Elas já podem estar cadastradas na rede e utilizar ou não os serviços da nossa operadora. Caso não estejam cadastradas, as solicitações são enviadas por e-mail com o conjunto mínimo padrão de dados de identificação e a organização fica livre para responder por meio do canal de sua escolha. Mas se elas fizerem parte da rede, os dados exatos de identificação de que precisam para processar a solicitação são selecionados automaticamente no Armazenamento de Dados Pessoais do indivíduo (ou se faltarem, preenchidos e armazenados manualmente para reutilização) e a solicitação é enviada por meio de uma conexão dedicada segura (criptografia ponta a ponta).
>
> [...]Todos os atores são beneficiários: as fontes de dados se beneficiam de transferências seguras de dados e uma ferramenta de conformidade de última geração para gerenciar solicitações de direitos GDPR e manter o histórico, o serviço de uso de dados obtém um acesso seguro e fácil a dados qualificados coforme o estado-da-arte em plataforma de gerenciamento de consentimento. Os indivíduos se beneficiam de uma ferramenta gratuita e segura para armazenar e controlar seus dados pessoais, com a liberdade de reutilizá-los da maneira que quiserem. Somente eles avaliam o valor da compensação de acordo com seus critérios". (Tradução nossa).

Essas ferramentas em desenvolvimento e já colocadas à disposição dos titulares no mercado europeu podem ser classificadas como PETs, uma vez que buscam franquear ao titular instrumentos tecnológicos para o exercício da autodeterminação informacional. Situar estas PETs centradas no usuário no contexto do território europeu, onde vige a GDPR, é importante para destacar o ponto central que as diferencia das PETs anteriores. O *core business* destas PETs descritas sob a adjetivação de "centradas no usuário" somente é possível graças aos direitos dos titulares permitidos pela Lei Geral de Proteção de Dados europeia, as *"solicitações GDPR"*. A partir dos direitos previstos no Capítulo III da GDPR, os titulares podem conferir à pessoa jurídica operadora das PETs o poder de representá-las legalmente perante os controladores para então obter cópias dos seus dados, verificação de conformidade do escopo do tratamento, realização de auditorias e então, gerenciamento do consentimento. Percebe-se que algumas destas PETs desempenham mesmo a função das P3P (Platform for Privacy

Preferences), pois tenderão a se tornar, conforme a opção do titular, o centro gerenciador do seu consentimento, onde ele o poderá fornecer apenas uma vez, senvindo posteriormente para vários dos serviços de terceiros que venham a usar os seus dados.

Com isto, pode-se peceber que o atual momento é bastante promissor no que diz respeito à garantia da autodeterminação informativa e, por consequência, da pluralidade e da democracia. A regulação da proteção de dados tem realmente o potencial de permitir uma virada no paradigma da economia baseada em dados, conduzindo-a a uma trilha em que a preservação dos valores fundamentais da liberdade, da privacidade, da autodeterminação informativa e do livre desenvolvimento da personalidade possam conviver harmonicamente com o desenvolvimento econômico.

CONCLUSÃO

As considerações até aqui delineadas foram tentativas de demonstrar a necessidade de se abordar a Lei Geral de Proteção de Dados, Lei 13.709 de 14 da agosto de 2018 de forma a se extrair o seu conteúdo protetivo no que tange à operacionalização dos direitos dos titulares de dados pessoais. Da conjugação das situações fáticas protegidas, dos fundamentos principiológicos e das regras de direito material presentes na Lei, bem como dos princípios e normas ínsitos ao sistema jurídico como um todo, posto que uno, é possível construir caminhos procedimentais que retirem o direito do mundo abstrado condicionando o mundo da vida humana e resguardando os bens jurídicos protegidos na proporcão necessária à boa convivência social. No caso, trata-se de harmonizar a evolução tecnológica com direitos fundamentais indisponíveis como a autodeterminação informativa, a privacidade, o livre desenvolvimento da personalidade, inclusive em suas novas expressões ou critérios de aferição como a privacidade contextual.

A chegada do direito ao âmbito "virtual" da vida e das relações humanas, ou, melhor dizendo, à sociedade da informação e das plataformas virtuais, tem feito surgir valiosas contribuições, parâmetros normativos e doutrinários acerca das situações jurídicas que alí enredam as relações humanas. No presente trabalho buscou-se demonstrar, através de uma incursão discreta na relação entre a tecnologia computacional e o ser humano, como, devido à própria dinâmica e natureza dos processos computacionais envolvidos na "economia baseada em dados", os métodos ou procedimentos previstos na Lei para o exercício dos direitos do titular dos dados pessoais precisarão se instrumentalizar através de ferramentas análogas. Caso contrário, parece possível inferir que o sistema de proteção à privacidade e à autodeterminação informacional se tornaria insuficiente, pois adotaria uma "rede" cujas malhas são grandes demais para capturar as principais ameaças ao direito que se quer proteger. Da mesma forma, o objetivo de tornar os titulares senhores dos seus dados também cairia por terra, pois, um direito difícil de manejar e cujos resultados de possíveis tentativas de fazer valer a lei não sejam percebidos de forma clara e o mais imediata possível, tende a se tornar dispensável.

Da própria sistemática da LGPD se depreende a necessidade de que, para um bom funcionamento do sistema de direito à proteção de dados, a sindicabilidade deverá ocorrer em nível "macro", através da Autoridade Nacional de Proteção de Dados, passando por sistemas intermediários que podem ocorrer através de metodologias diversas como a certificação privada. Mas também de fundamental importância será a sindicabilidade privada e em nível

"micro", pelos próprios sujeitos do direito, daí a rica estrutura de direitos dos titulares previstos na Lei, que parece ter por fim esta sindicabilidade como expressão do deslocamento do *locus* de controle para o titular dos dados.

Assim, os grandes *players* e os seus principais serviços estariam sob o crivo do sistema "macro" de fiscalização e poderão ser pautados por regulações programáticas, conforme o caso. De outro lado, poderá haver um sistema "micro" de sindicância que contemplaria os interesses do titular no caso concreto, fornecendo a ele poder de controle sobre seus dados específicos, com capilaridade tal que lhe permita exercer este controle tanto perante os grandes *players*, quanto até mesmo perante controladores de menor tamanho.

Inerente à "economia baseada em dados" e à superestrutura de coleta e armazenamento de dados atuais, nas quais grandes companhias, governos e até micro enpresas têm buscado impulsionar seus negócios e interesses, estão as variáveis "volume", "velocidade" e "variedade", elencadas como características descritivas dos sitemas de "Big Data". Estas variáveis representam, como se tentou apontar, problemas que se colocam, e dos quais não se deve desviar o olhar, quando se busca pensar em um sistema de proteção do direito à privacidade e à autodeterminação, bem como em um sistema de promoção da autonomia e do empoderamento do titular, objetivo principal da LGPD.

As PETs parecem ser uma possível solução para esta questão, na medida em que podem ser desenhadas de forma a operacionalizar as requisições dos titulares perantes os agentes de tratamento e dar vazão à sindicabilidade permitida ao titular do dado pessoal pela Lei. A integração dos direitos dos titulares com a capacidade das PETs de trabalharem com o volume, a variedade e a velocidade que os sistemas de tratamento de dados requer, pode ser forma inovadora de oferta de serviço de exercício do direito à autodeterminação informacional aos cidadãos.

Os procedimentos jurídicos dispostos na LGPD e demais normas pertinentes podem demarcar um campo de atuação legítimo para estas ferramentas, tornando possível e obrigatória a interoperabilidade entre os sistemas dos controladores e removendo obstáculos contrários ao interesse geral de se garantir sistemas de fluxo de dados seguros, sindicáveis e consentâneos aos direitos fundamentais comentados. Nesse sentido, a LGPD será possivelmente, normativa suficiente ou inicial a permitir a existência de um sistema de *"open health"*, *"open consumer"*, *"open legal"*, além, é claro, do *"open banking"* que possui regulamentação própria. Ou seja, os direitos dos titulares permitirão ao indivíduo levar consigo seus dados de saúde, de consumo,

relativos a um serviço de advocacia e bancários, de um agente de tratamento para outro, dentro das possibilidade e requisitos legais.

Os casos descritos das soluções que já têm sido propostas no mercado europeu de operadores do ecossistema de dados com tecnologias que colocam o titular dos dados em posição central no gerenciamento dos mesmos aponta um marco inicial promissor e que pode ser buscado também pelos operadores do direito. A convergência entre tecnologia e direito na oferta de serviço ao titular de dados pessoais que lhe franqueie acesso facilitado aos procedimentos admitidos em Lei, que lhe garantam os direitos materiais à proteção à privacidade e à autoderminação, permitirão que esta seara protetiva se incorpore no dia a dia das pessoas, pois se tornaria um direito plenamente vivido, experimentado e atuado cotidianamente. Sem esta experiência prática, imediata e acessível o direito à proteção de dados tende a se tornar apenas tema acadêmico "*case* de tribunal" e permanecer distante do principal interessado, o titular.

REFERÊNCIAS BIBLIOGRÁFICAS

ALIMONTI, Veridiana. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Orgs.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para implementação da LGPD. São Paulo: Thomsom Reuters, 2020.

ARBIX, Daniel. A Importância da privacidade por Design e por Default (Privacy By Design And By Default). In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Orgs.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para implementação da LGPD. São Paulo: Thomsom Reuters, 2020.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais (p. 5). Forense. Edição do Kindle.

BIONI, Bruno. Regulação de dados é uma janela de oportunidade. 2019. Disponível em <https://dataprivacy.com.br/regulacao-de-dados-e-uma-janela-de-oportunidade/> Acessado em 28 out 2020.

BOYD, danah. Escrevendo a sua própria existência. Tradução de Francisco Brito Cruz e Mariana G. Valente. In Internet & Sociedade. Número 1. Volume 1. Fev. 2020.

COTS, Marcio; Oliveira, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: Thomson Reuters Brasil, 2018.

DEL PRETTE, Zilda A. P.; DEL PRETE, Almir. Psicologia das habilidades sociais: terapia, educação e trabalho. 9 ed. – Petrópolis, RJ: Vozes, 2012.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. Curso de direito civil: parte geral e LINDB. 15. ed. rev., ampl. e atual. – Salvador: Ed. JusPoivm, 2017.

LADEIRA, João Martins. Cientistas, militares e burocratas: o desenvolvimento da Arpanet e o Sistema Norte-Americano de inovação. C&S – São Bernardo do Campo, v. 40, n. 1, p. 213-237, jan./abr. 2018

MEDINA, José Miguel Garcia; MARTINS, João Paulo Nery dos Passos. A Era da Inteligência Artificial: As Máquinas poderão tomar Decisões Judiciais? Revista dos Tribunais | vol. 1020/2020 | Out / 2020 DTR\2020\11420

NUNES, Rizzato. Curso de Direito do Consumidor. 13 ed. – São Paulo: Saraiva Educação, 2019.

OSIA, Seyed Ali et al. A Hybrid Deep Learning Architecture for Privacy-Preserving Mobile Analytics. IEEE Internet of Things Journal, May 2020. Disponível em https://arxiv.org/abs/1703.02952.

SHARDA, Ramesh. Business Intelligence e Análise de Dados para Gestão do Negócio (p. 42). Edição do Kindle.

THEODORO JÚNIOR, Humberto. Curso de Direito Processual Civil – vol. I: teoria geral do direito processual civil, processo de conhecimento procedimento comum. – 60. Ed. – Rio de Janeiro: Forense, 2019

WIELSCH, Dan. Os ordenamentos das redes: Termos e condições de uso – Código – Padrões da comunidade. In: Abboud, Georges. Nery Jr., Nelson. Campos, Ricardo. Org. Fake News e regulação. – 2. Ed. São Paulo: Thomson Reuters Brasil, 2020.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Geraldo Rodrigo Soares de Souza

Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 41715691 , Período Noturno , Turma N ,

tendo realizado o TCC com o título: Direitos dos titulares de dados pessoais e procedimentos para sua operacionalização.

sob a orientação do(a) professor(a): Eduardo Altomare Ariente

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 10 de Novembro de 2020.

Assinatura do discente