

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO

**O PARADIGMA DA SOCIEDADE DA INFORMAÇÃO E A LEI
GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO
ANALÍTICO DOS DESAFIOS DO PODER JUDICIÁRIO NO
TRATAMENTO DE DADOS PROCESSUAIS**

GABRIELA MARSON SANDRI

Itajaí-SC, agosto de 2020

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO

**O PARADIGMA DA SOCIEDADE DA INFORMAÇÃO E A LEI
GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO
ANALÍTICO DOS DESAFIOS DO PODER JUDICIÁRIO NO
TRATAMENTO DE DADOS PROCESSUAIS**

GABRIELA MARSON SANDRI

Dissertação submetida ao Curso de Mestrado em
Ciência Jurídica da Universidade do Vale do Itajaí –
UNIVALI, como requisito parcial à obtenção do título
de Mestre em Ciência Jurídica.

Orientador: Professor Doutor Orlando Zanon Júnior
Coorientador: Professor Brett Bendistis

Itajaí-SC, agosto de 2020

AGRADECIMENTOS

Ao Criador, por tantos motivos para agradecer.

Aos meus pais, por toda a disponibilidade, amor e incentivo durante toda a minha caminhada e por continuarem sendo o meu alicerce. À minha mãe, em especial, durante o tempo em que estive nos Estados Unidos para cumprir o programa de estudos na Widener University, e em momentos cruciais do desenvolvimento desta dissertação, por ter deixado sua vida de lado e ter vindo viver a minha para que eu pudesse me dedicar à pesquisa.

Ao meu marido, por sempre abraçar os meus planos e não me deixar desistir. Pela paciência, compreensão e suporte que foram fundamentais para que eu conseguisse concluir esse tão desejado Mestrado. Agradeço, de forma especial, pelos momentos inesquecíveis em família vividos em Delaware. Obrigada por cuidar de nós. Obrigada por sempre “estar lá”.

Às minhas amadas filhas, que precisaram lidar, em tão pequena idade, com o sentimento de ausência e cooperar com uma mãe que, segundo elas, “só estuda e trabalha”. O meu desejo é ter conseguido lhes transmitir a mensagem, sublime e subliminar, de que lutar por nossos sonhos vale a pena, mesmo que o caminho pareça chato e difícil. Além disso, ao ver como estão crescendo hábeis na leitura e o quanto gostam de devorar livros, sinto que deixei um bom exemplo, assim como recebi de minha mãe. Então sigo tranquila, porque a “chatice” germinou o lindo fruto do amor pela leitura.

Ao meu irmão, João Fernando e à minha irmã, Annamaria, pelo cuidado com a saúde e recuperação de nossa mãe durante um momento crítico em que eu estava em longe e não pude ajudar.

Novamente aos meus irmãos e às minhas cunhadas, Ana Paula e Louyse, por todo o auxílio e carinho com minhas filhas e filho canino durante o tempo em que estive ausente.

À Dona Marli, anjo da guarda que cuidou da minha família como se fosse a sua, por nutrir o nosso lar com alimento para o corpo e para a alma.

Às colegas e amigas Nathalia e Mauriceia, por suportarem, com grande amizade, a sobrecarga de trabalho. Registro aqui meu agradecimento mais do que especial à amiga e mentora, a Advogada Me. Lola Pergher, que, mesmo sabendo do tempo que eu precisaria me ausentar dos afazeres cotidianos para cumprir com o programa do Mestrado, foi a grande incentivadora desta empreitada.

Aos grandes amigos que o Mestrado me presenteou, especialmente Tatiana Firmino Damas, Juliana Padrão Serra de Araújo, Fabrício d'Ambrosio,

Miguel Ortale e Aline Farhat, pelos ombros, ouvidos e risadas. A jornada não teria sido a mesma sem vocês!

Ao meu orientador, Professor Doutor Orlando Zanon Júnior, por seu estímulo e disponibilidade ao longo desta pesquisa e, também, pela paciência em aceitar as mudanças de percurso e firmeza em conduzi-las. Tive a honra de ser orientada pelo professor que, por meio de aulas instigantes e de notável saber, despertou em mim o desejo de continuar os estudos na área da Ciência Jurídica, dominada com maestria pelo excepcional jurista que é.

À Professora Doutora Emanuele Cristina Andrade Lacerda, uma grata surpresa reservada para o final deste Mestrado, quando decidi me inscrever para a disciplina optativa “Direito e a Sociedade Digital Transnacional”. Os temas tratados durante os seminários e seus valiosos ensinamentos seguirão comigo na próxima etapa, o Doutorado.

Aos demais professores, coordenadores e *staff* do programa de Mestrado em Ciência Jurídica da UNIVALI e da Delaware Law School da Widener University pelo excelente programa desenvolvido e pela oportunidade concedida.

Por fim, agradeço ao meu querido “filho” de quatro patas, Lennon, pelo amor que me permitiu viver durante sua existência e pela companhia fiel ao longo desta pesquisa. Sua recente partida deixou um vazio em meu coração e nas noites de estudo, que ficaram mais tristes e solitários sem a sua presença.

DEDICATÓRIA

À minha mãe e oráculo, Silvia, fonte inesgotável de sabedoria.
Ao meu pai, Edson, fonte inesgotável de juventude e irreverência.
A minhas filhas, Olivia e Nina, fontes inesgotáveis de aprendizado.
Ao meu marido, Junior, fonte inesgotável de amor, inspiração e encorajamento.

Congratulations, you are now hackable animals
Yuval Noah Harari

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, agosto de 2020

GABRIELA MARSON

SANDRI:03848053969

Assinado de forma digital por

GABRIELA MARSON

SANDRI:03848053969

Dados: 2020.11.16 19:26:26 -03'00'

Gabriela Marson Sandri

Mestranda

P Á G I N A D E A P R O V A Ç ã O

MESTRADO

Conforme Ata da Banca de Defesa de Mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica PPCJ/UNIVALI, em 17/09/2020, às 16 horas, a mestranda GABRIELA MARSON SANDRI, fez a apresentação e defesa da Dissertação, sob o título “O PARADIGMA DA SOCIEDADE DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO ANALÍTICO DOS DESAFIOS DO PODER JUDICIÁRIO NO TRATAMENTO DE DADOS PROCESSUAIS”.

A Banca Examinadora foi composta pelos seguintes professores: Doutor Orlando Luiz Zanon Junior (UNIVALI) como presidente e orientador, Doutor Orlando Celso da Silva Neto (UFSC) como membro, Doutor Marcos Leite Garcia (UNIVALI) como membro e Doutor Marcelo Buzaglo Dantas (UNIVALI) como membro suplente. Conforme consta em Ata, após a avaliação dos membros da Banca, a Dissertação foi Aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), dia 17 de setembro de 2020.



PROF. DR. PAULO MÁRCIO DA CRUZ
Coordenador/PPCJ/UNIVALI

ROL DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
CRFB	Constituição da República Federativa do Brasil de 1988 e emendas constitucionais posteriores
CC/2002	Código Civil de 2002
CNJ	Conselho Nacional de Justiça
DPO	<i>Data Protection Officer</i>
GDPR	<i>General Data Protection Regulation</i>
LGPD	Lei Geral de Proteção de Dados
LAI	Lei de Acesso à Informação
LPE	Lei do Processo Eletrônico
TJUE	Tribunal de Justiça da União Europeia
STF	Supremo Tribunal Federal
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

ROL DE CATEGORIAS

ANONIMIZAÇÃO: nos termos da LGPD, anonimização é 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 indivíduo¹.

BANCO DE DADOS: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico².

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável³.

DADOS PESSOAIS SENSÍVEIS: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural⁴.

DADOS PROCESSUAIS: informações e documentos cadastrados, registrados e armazenados nos sistemas de informação e bancos de dados dos tribunais do Poder Judiciário relacionados a processos judiciais submetidos à sua Jurisdição.

INFORMACIONALISMO: é o rejuvenescimento e transformação do Capitalismo Industrial, voltado para conhecimento da economia e maximização da produção, para o Capitalismo Informacional, com vistas ao desenvolvimento tecnológico, ou seja, a acumulação de conhecimentos e maiores níveis de complexidade do processamento da informação. No Informacionalismo é a busca por conhecimentos e informação que caracteriza a função da produção tecnológica, reforçando uma íntima ligação entre cultura e forças produtivas e entre espírito e matéria⁵.

¹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 5º, inciso XI.

² BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 5º, inciso IV

³ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 5º, inciso I

⁴ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 5º, inciso II

⁵ CASTELLS, Manuel. **A sociedade em rede: a era da informação**. Vol. I. 15ª impressão. 6 ed. Tradução Roneide Venancio Majer. São Paulo: Paz e Terra. 2012. Título Original: Rise of the Network Society: The Information Age. Original escrito em 1942. p. 70

INTERNET: sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes⁶.

PRIVACIDADE: o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada⁷.

PROTEÇÃO DE DADOS: é a possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados *per se*, mas a pessoa que é titular desses dados⁸.

PSEUDONIMIZAÇÃO: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro⁹.

SOCIEDADE DA INFORMAÇÃO: organização social em que a geração, o processamento e a transmissão da informação tornam-se fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico, caracterizada pela globalização das atividades econômicas decisivas do ponto de vista estratégico, por sua forma de organização em redes, pela flexibilidade e instabilidade no emprego e a individualização da mão-de-obra, o que o sociólogo define como “Sociedade em Rede”. Desta forma, a Sociedade Informacional emerge de um processo de transformação de base capitalista e também de base informacional¹⁰.

TRANSFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro¹¹.

⁶ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Art. 5º, inciso I.

⁷ LAFER, Celso. **A reconstrução dos direitos humanos**. São Paulo, Companhia das Letras, 1998.

⁸ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. (Posição 559)

⁹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 12, §4º.

¹⁰ CASTELLS, Manuel. **A sociedade em rede: a era da informação**. Vol. I. 15ª impressão. 6 ed. Tradução Roneide Venancio Majer. São Paulo: Paz e Terra. 2012. Título Original: Rise of the Network Society: The Information Age. Original escrito em 1942.p. 58 e 89

¹¹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 5º, inciso XV.

VIGILÂNCIA: monitoramento e controle de informações por meio da tecnologia no âmbito da Sociedade da Informação.

SUMÁRIO

RESUMO.....	XVI
RESUMO EM LINGUA ESTRANGEIRA	ERRO! INDICADOR NÃO DEFINIDO.
INTRODUÇÃO	18
Capítulo 1	23
A EVOLUÇÃO DO DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA SOCIEDADE DA INFORMAÇÃO	23
1.1 CONTEXTUALIZAÇÃO HISTÓRICA DA SOCIEDADE DA INFORMAÇÃO	23
1.1.1 A Internet como agente propulsor da Sociedade da Informação	27
1.1.2 As transformações advindas do trinômio <i>Cloud Computing</i>, <i>Big Data</i> e Inteligência Artificial	31
1.1.2.1 <i>Big Data</i>	32
1.1.2.2 <i>Cloud computing</i>.....	33
1.1.2.3 <i>Inteligência Artificial</i>	35
1.2 REVOLUÇÃO TECNOLÓGICA E ECONOMIA INFORMACIONAL: O INFORMACIONALISMO.....	37
1.2.1 O novo paradigma da economia de dados (<i>data economy</i>)	38
1.3 A EVOLUÇÃO DO DIREITO À PRIVACIDADE: RUMO A UM NOVO DIREITO FUNDAMENTAL?	43
1.3.1 O direito fundamental à privacidade.....	43
1.3.2 Os impactos à privacidade e à proteção de dados na Sociedade da Informação	49
1.3.3 Os desafios do Direito no tratamento da proteção de dados e prevenção do abuso de poder na Sociedade da Informação	51
1.3.4 A proteção de dados pessoais: um novo direito fundamental?	56
Capítulo 2	59
O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NO ÂMBITO DO PODER PÚBLICO	59

2.1 A POSITIVAÇÃO DAS REGRAS INERENTES AO TRATAMENTO E À PROTEÇÃO DE DADOS PESSOAIS.....	59
2.2 ASPECTOS DESTACADOS DA LEI GERAL DE PROTEÇÃO DE DADOS	64
2.2.1 Conceitos importantes.....	64
2.2.2 Objetivos e âmbito de aplicação material e territorial.....	66
2.2.3 Fundamentos.....	71
2.2.3.1 O respeito à privacidade.....	72
2.2.3.2 A autodeterminação informativa.....	73
2.2.3.3 A liberdade de expressão, de informação, de comunicação e de opinião.....	75
2.2.3.4 A inviolabilidade da intimidade, da honra e da imagem.....	78
2.2.3.5 O desenvolvimento econômico e tecnológico e a inovação.....	80
2.2.3.6 A livre iniciativa, a livre concorrência e a defesa do consumidor.....	82
2.2.3.7 Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.....	84
2.2.4 Princípios aplicados ao tratamento de dados pessoais	87
2.2.5 Justificativa legal	89
2.3 A APLICAÇÃO DA LGPD NO ÂMBITO DO PODER PÚBLICO.....	91
2.3.1 O tratamento de dados pessoais pelo Poder Público.....	91
Capítulo 3.....	106
PERSPECTIVAS DO TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DO PROCESSO JUDICIAL À LUZ DA LGPD	106
3.1 A ESTRUTURA NORMATIVA APLICÁVEL AO ACESSO, PUBLICIDADE E PROTEÇÃO DE DADOS NO PROCESSO JUDICIAL	106
3.1.1 Estrutura normativa processual: a publicidade é a regra, o sigilo é a exceção	106
3.1.1.1 Restrições à publicidade processual e o segredo de justiça	109

3.1.2 Controle de acesso aos dados processuais, direito à informação e o princípio da publicidade: uma revisitação à luz da LGPD	125
3.2 O COMPARTILHAMENTO DE DADOS PROCESSUAIS PELOS ÓRGÃOS DO PODER JUDICIÁRIO COM PESSOAS JURÍDICAS DE DIREITO PRIVADO ..	138
3.2.1 Compartilhamento de dados para fins de desenvolvimento de sistemas de tecnologia da informação e Inteligência Artificial	139
3.2.2 A transferência internacional de dados e a cloud computing	150
3.3 A (IN)SUJEIÇÃO DO PODER JUDICIÁRIO À AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS E OUTRAS (IN)CERTEZAS	161
3.3.1 O Poder Judiciário	162
3.3.2 A Autoridade Nacional de Proteção de Dados – ANPD	165
3.3.3 A figura do Encarregado: deverá o Poder Judiciário nomear um DPO?169	
CONSIDERAÇÕES FINAIS	172
REFERÊNCIA DAS FONTES CITADAS.....	180

RESUMO

A presente Dissertação está inserida na Linha de Pesquisa Direito e Jurisdição do Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da Universidade do Vale do Itajaí-UNIVALI em dupla titulação com a Widener University, de Wilmington, Delaware, Estados Unidos. Utilizou-se o método indutivo de pesquisa e a análise de bibliografia, legislação, jurisprudência e dados estatísticos como método procedimental. O objetivo foi o estudo dos reflexos da iminente entrada em vigor da Lei Geral de Proteção de Dados no tratamento dos dados processuais e a investigação dos limites da sujeição do Poder Judiciário aos ditames da referida lei. A investigação partiu das seguintes hipóteses: a) a evolução tecnológica que demarca a Sociedade da Informação contribuiu para a caracterização de um direito autônomo à proteção de dados pessoais e à necessidade de salvaguarda-lo por meio de regulação específica; b) o Poder Judiciário deverá observar e se sujeitar aos ditames da LGPD, dentro dos limites constitucionais e institucionais da atividade jurisdicional; c) a entrada em vigor da LGPD ensejará mudanças na publicidade dos atos processuais e nos critérios de acesso e compartilhamento de dados processuais. O primeiro capítulo tratou de contextualizar o marco histórico da evolução da Sociedade da Informação, cujas características axiológicas advindas da transformação tecnológica, marcada pela mercantilização de dados pessoais e pelo risco da vigilância estatal e mercadológica, fundamentaram o reconhecimento de um direito autônomo à proteção de dados pessoais. Ocupou-se o segundo capítulo de analisar a positivação das regras para o tratamento de dados pessoais a partir da norma paradigmática, consubstanciada no Regulamento Geral de Proteção de Dados da União Europeia, que serviu como inspiração, e pressão, para a promulgação da lei de proteção de dados pessoais brasileira. O terceiro e último capítulo, por sua vez, investigou os reflexos diretos das disposições da LGPD em cotejo analítico com as normas constitucionais e infraconstitucionais, no que se refere à publicidade, ao acesso e ao compartilhamento de dados pessoais no âmbito do processo judicial, inclusive em relação à transferência internacional de dados, assim como analisou os eventuais conflitos decorrentes das prerrogativas da Autoridade Nacional de Proteção de Dados face à independência do Poder Judiciário. Por fim, foi possível concluir que, embora a Sociedade da Informação seja marcada pelo compartilhamento expressivo de dados pessoais, facilitado pela tecnologia, os indivíduos ainda consideram a privacidade um direito que deve ser protegido de intervenção arbitrária, sendo que o reconhecimento da autodeterminação informativa como um direito fundamental pelo ordenamento jurídico da União Europeia, foi crucial para a implementação de leis de proteção de dados pessoais ao redor do mundo, notadamente no Brasil.

Palavras-chave: Sociedade da Informação. Proteção de Dados Pessoais. Publicidade de Dados Processuais.

ABSTRACT

This Thesis is encompassed in the Law and Jurisdiction line of research within the Stricto Sensu Post-Graduate Program in Legal Science at the University of Vale do Itajaí and the Master of Law (LLM) program at Widener University - Delaware Law School, as a result of the dual degree between both Universities. The inductive research approach method was used and the bibliographic, legislation and statistic data analysis were the chosen procedural method. The primary objective was to study the reflexes of the imminent come into force of the Lei Geral de Proteção de Dados – the Brazilian personal data protection general law – on the judicial proceedings data and whether the Judiciary Branch is subject to the provisions therein. The investigation started off with the following hypothesis: a) the technological evolution which demarcates the Information Society has contributed to the characterization of an autonomous right to the protection of personal data and the safeguard it through specific regulation; b) the Judiciary Branch must observe and be subject to the provisions set forth in the LGPD, within the constitutional and institutional limits of the jurisdictional activities; c) the implementation of the LGPD will lead to changes on the publicity of judicial procedural acts and on the criterion established for the access and sharing of judicial proceedings data. The first chapter contextualized the historical landmark originated from the evolution of the Information Society, with its axiological characteristics accrued from the technological transformation and the commercialization of personal data, as well as from the risks associated to the State and market surveillance, serving as the basis for the acknowledgement of an autonomous right to the protection of personal data. Afterward, the second chapter went through the positivation of the rules concerning the processing of personal data within the scope of the paradigm legal text, the General Data Protection Regulation of the European Union, which acted both as inspiration and international pressure that led to the promulgation of the Brazilian law related to the protection of personal data. Furthermore, the last chapter investigated the direct reflexes of the LGPD through the analysis of the constitutional and legal norms related to the publicity, access and sharing of personal data contained within the judicial proceedings, including the international data transfer. Additionally, this research analyzed the possible conflicts arising from the prerogatives of the Data Protection Authority and the independence of the Judiciary Branch. Finally, it became possible to conclude that, even though the Information Society is signaled by an outstanding sharing of personal data facilitated by technology, the individuals still hold their privacy as a right that must be protected from arbitrary intervention, where the informational self-determination, granted as a fundamental right in the European legal framework, played a crucial role on the implementation of data protection laws around the world, notably in Brazil.

Keywords: Information Society. Personal Data Protection. Judicial Proceedings Data. Publicity.

INTRODUÇÃO

A partir do século passado, o mundo tem experimentado uma revolução extraordinária impulsionada pelo avanço tecnológico. *Big data*, *machine learning* e Inteligência Artificial são algumas dessas ferramentas que transformaram a chamada Sociedade da Informação.

A possibilidade de cruzamento de informação, da utilização de dados pessoais como insumos que transformaram pequenas empresas de tecnologia em negócios multibilionários reacendeu as discussões sobre a proteção de dados pessoais, iniciada após a Segunda Guerra Mundial e consolidada após os escândalos de espionagem noticiados por Edward Snowden e o caso Cambridge Analytica.

Essa nova ordem mundial fez emergir legislações sobre a proteção de dados nos mais diversos países que se interligam no contexto do fluxo de informações, com caráter transnacional, oriundo das operações realizadas pelos diversos atores.

Uma exigência das leis nacionais de proteção de dados é que dados pessoais colhidos em seus territórios e que digam respeito a seus cidadãos somente sejam transferidos a países que possuam leis com grau de proteção de dados pessoais compatíveis com suas próprias legislações.

A LGPD, por ser uma lei de aplicação geral, deverá ser observada por toda e qualquer pessoa que realizar o tratamento de dados pessoais nos moldes previstos em seu texto normativo, atingindo todos os setores da Sociedade, ou seja, a LGPD uniformiza os direitos de proteção de dados pessoais para todos os cidadãos, em todos os segmentos, tanto no setor público quanto no privado. Em outras palavras, as pessoas passam a ter a mesma expectativa de proteção de dados, independentemente do tipo de relação jurídica que venham a estabelecer.

O Poder Público, destinatário da Lei, é detentor dos maiores bancos de dados contendo informações pessoais sobre a população, tendo em vista a

natureza de suas atividades. Dentre os três Poderes que formam o Estado Democrático de Direito brasileiro, o Poder Judiciário, é, sem dúvida, um grande fator de vulnerabilidade de exposição de dados pessoais, haja vista a sensibilidade de temas tratados em seus mais de 78 milhões de processos judiciais em trâmite em suas diversas Justiças, segundo dados extraídos do anuário Justiça em Números 2019¹², do Conselho Nacional de Justiça.

Considerando que o Poder Judiciário, apesar do dever de observar a lei e, portanto, a LGPD, também tem sua atuação vinculada a princípios constitucionais, como o da Publicidade, por exemplo, que norteiam a atividade estatal, não é difícil, pois, concluir que a adequação do Poder Judiciário com a LGPD será permeada de conflitos principiológicos e legislativos, o que demanda esforços de interpretação.

Nesse contexto, o objetivo científico do presente trabalho é investigar os reflexos da Lei Geral de Proteção de Dados no tratamento de dados pessoais pelo Poder Judiciário no âmbito no processo judicial processuais e os efeitos práticos de sua aplicação.

De outro lado, o objetivo institucional da presente Dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali com dupla titulação pela Widener University – Delaware Law School.

A presente pesquisa pretende contribuir para uma discussão inicial sobre o tema e responder ao seguinte problema de pesquisa: o Poder Judiciário está sujeito aos regramentos da LGPD no exercício de suas funções jurisdicionais, observadas as limitações constitucionais e institucionais inerentes às suas atividades?

Para a pesquisa foram levantadas as seguintes hipóteses:

¹² BRASIL, **Conselho Nacional de Justiça**. Justiça em Números 2019. Disponível em:< <https://www.cnj.jus.br/wp-content/uploads/conteudo/arquivo/2019/08/8ee6903750bb4361b5d0d1932ec6632e.pdf>> Acesso em: 05/03/2020. p. 79.

a) A evolução tecnológica que demarca a Sociedade da Informação contribuiu para a caracterização de um direito autônomo à proteção de dados pessoais e à necessidade de salvaguarda-lo por meio de regulação específica.

b) A entrada em vigor da LGPD ensejará mudanças na publicidade dos atos processuais, no acesso aos processos judiciais e no acesso às bases de dados dos tribunais para a incorporação de novos avanços tecnológicos ao Sistema de Justiça.

c) O Poder Judiciário, na qualidade de detentor de expressivo banco de dados pessoais decorrentes de processos judiciais, deverá observar e se sujeitar aos ditames da LGPD, haja vista as peculiaridades constitucionais e institucionais da atividade jurisdicional.

Os resultados do trabalho de exame das hipóteses estão expostos na presente dissertação, de forma sintetizada, como segue.

Ocupa-se o Capítulo 1 de contextualizar o marco histórico e sociológico da pesquisa que fundamentaram as bases para o reconhecimento de um direito à proteção de dados pessoais, impulsionado pelos avanços tecnológicos que culminaram com o que o se convencionou denominar de Quarta Revolução Industrial e sua conjugação com um formato renovado de capitalismo, o Informacionalismo, que sustenta a Sociedade da Informação.

Ainda sob o mesmo tópico, analisam-se os contornos jurídicos da Sociedade da Informação no que diz respeito à ruptura com os conceitos de privacidade tradicional que fomentaram discussões ao redor do mundo sobre os riscos da exposição dos indivíduos e da cultura de utilização massiva de dados pessoais, inclusive pelo Poder Público, que levaram ao reconhecimento de um direito autônomo dos indivíduos à proteção de seus dados pessoais.

O Capítulo 2 trata da positivação das regras para tratamento de dados pessoais no Brasil, cujas bases foram lançadas pelo Regulamento Geral de Proteção de Dados da União Europeia, atualmente tomado como *benchmark* em termos de proteção de dados pessoais e que vem atuando com forte pressão no âmbito transnacional para que as demais nações do globo terrestre adotem

medidas protetivas similares às suas para que seja autorizado o intercâmbio de dados com o referido bloco econômico.

Em continuidade, são apresentadas as bases legais da LGPD aplicáveis ao Poder Público e do arcabouço axiológico e deontológico que deverá ser levado em consideração na análise dos reflexos de sua aplicação ao tratamento de dados pessoais pelo Poder Judiciário. Além disso, adentra-se na análise dos princípios constitucionais aos quais o Poder Público está vinculado na garantia de publicidade de seus atos e acesso à informação.

O Capítulo 3 dedica-se a investigar os reflexos da LGPD no tratamento de dados pessoais pelo Poder Judiciário no âmbito dos dados processuais e suas implicações práticas e procedimentais com enfoque em quatro pontos de pesquisa: a publicação de atos processuais, os critérios de acesso aos dados processuais, o compartilhamento de dados processuais com entidades privadas e a (in)sujeição do Poder Judiciário à Autoridade Nacional de Proteção de Dados.

O presente Relatório de Pesquisa se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estímulos à continuidade dos estudos e das reflexões sobre (assunto tratado na dissertação).

Quanto à Metodologia empregada, registra-se que, na Fase de Investigação¹³ foi utilizado o Método Indutivo¹⁴, na Fase de Tratamento de Dados o Método Cartesiano¹⁵, e, o Relatório dos Resultados expresso na presente Monografia é composto na base lógica indutiva.

¹³ “(...) momento no qual o Pesquisador busca e recolhe os dados, sob a moldura do Referente estabelecido (...)” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018. p. 112-113.

¹⁴ “(...) pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 114.

¹⁵ Sobre as quatro regras do Método Cartesiano (evidência, dividir, ordenar e avaliar) veja LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

Nas diversas fases da Pesquisa, foram acionadas as Técnicas do Referente¹⁶, da Categoria¹⁷, do Conceito Operacional¹⁸ e da Pesquisa Bibliográfica¹⁹.

¹⁶ “(...) explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. p. 69.

¹⁷ “(...) palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. p. 41.

¹⁸ “(...) uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. p. 58.

¹⁹ “Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. p. 217.

Capítulo 1

A EVOLUÇÃO DO DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA SOCIEDADE DA INFORMAÇÃO

1.1 CONTEXTUALIZAÇÃO HISTÓRICA DA SOCIEDADE DA INFORMAÇÃO

A contemporaneidade é marcada por profundas transformações impulsionadas pelas novas tecnologias da informação e da comunicação, atingindo, indistintamente, todos os setores da Sociedade. Essas transformações têm produzido inovações nas práticas no cotidiano, nos estilos de vida, na esfera comunicativa e, cada vez mais, na forma de ensinar e aprender.

Na sociedade pré-industrial, era o produto agrícola que impulsionava a economia da época, sendo a terra a principal fonte de riqueza. Com a criação das máquinas a vapor e o advento da eletricidade, houve uma profunda transformação da Sociedade, sendo estes os insumos centrais da produção fabril que permeou a era industrial. Após a Segunda Guerra Mundial, na chamada Sociedade Pós-Industrial, observou-se a ascensão dos serviços como meio de destaque na produção de riquezas e mola propulsora da economia, de modo que a sociedade não se caracterizava mais pelo que se poderia produzir, mas sim pelos serviços que poderia ofertar²⁰.

Após a revolução industrial, com um aumento populacional considerável, relações comerciais complexas e de grande porte e a quebra de barreiras geográficas, porém, percebeu-se que a forma de as pessoas se relacionarem, especialmente em se tratando de aspectos contratuais, estava tornando-se obsoleto. A partir daí, viu-se a necessidade de uma coleta e armazenamento maior e mais eficiente de informações pessoais.

²⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 18

Cumpra aqui, consignar, que a coleta massiva de dados é um fenômeno da contemporaneidade. No período pré-industrial, uma base de dados contendo informações pessoais de cidadãos comuns era quase inexistente, uma vez que não se via a necessidade de armazenamento desses dados, os quais, em vias gerais, eram considerados inúteis²¹.

Nesse contexto, MENDES²² assevera que a utilização massiva de dados pessoais a partir da segunda metade do século XX pode ser associada a duas características principais do Estado pós-industrial: a burocratização, tanto do setor público, quanto do privado, e o desenvolvimento da tecnologia da informação, sendo que “ambos os fenômenos, que podem ser considerados transnacionais, suscitaram o processamento dos dados pessoais por governos das mais variadas ideologias políticas e por grandes corporações empresariais, com finalidades estatísticas, administrativas, negociais e investigativas”.

As mudanças sociais são tão drásticas quanto os processos de transformação tecnológica e econômica e, atualmente, é possível evidenciar a penetrabilidade da tecnologia em todas as esferas da vida humana²³.

Sobre a importância da informação no contexto contemporâneo, cumpre citar BIONI:

No estágio atual, a sociedade está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e pós-industrial.²⁴

O que se observa é que essa nova estrutura social teve como base os mecanismos criados pela evolução tecnológica, os quais, como se verificará ao

²¹ RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro; FINGER, Brunize. **O direito à proteção de dados pessoais e à privacidade**. In: Revista da Faculdade de Direito – UFPR. 53. 2011. p. 45.

²² MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. Saraiva: São Paulo, 2014. (Posição 572)

²³ CASTELLS, Manuel. **A sociedade em rede: a era da informação**. Vol. I. 15ª impressão. 6 ed. Tradução Roneide Venancio Majer. São Paulo: Paz e Terra. 2012. Título Original: Rise of the Network Society: The Information Age. Original escrito em 1942.p. 40

²⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 20

longo deste trabalho, adquiriram a capacidade de processar e transmitir informações em quantidade e velocidade que não se poderia imaginar.

Assim, conforme conclui BIONI²⁵, “a informação avoca um papel central e adjetivante da sociedade: 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”.

Segundo LASH²⁶, o poder não está mais localizado no capital como meio de produção material, e sim no complexo poder/conhecimento – vinculado a empresas supranacionais – do modo da informação. Para o Autor, nessa segunda modernidade, que é a evolução da Sociedade Industrial para a Sociedade Informacional, a classe média não é mais uma “classe de serviços”, mas uma classe “servida”, pois seu trabalho (processamento de informações) não está subsumido às necessidades da acumulação industrial, mas à acumulação de informação. Assim, os meios de produção, como capital constante fixo (hardware) e capital constante circulante (software) são informacionalizados, sendo a informação o recurso mais importante desta era.

O que caracteriza, portanto, a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso²⁷.

Nesse sentido, trata-se de uma verdade irrefutável de que o mundo passou por uma profunda transformação nas últimas cinco décadas, impactando de forma absoluta a comunicação: “a sofisticação da comunicação e das redes sociais se encarregaram de criar um processo global intenso no aumento –

²⁵ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. p. 21

²⁶ LASH, Scott. **A reflexividade e seus duplos**: estrutura, estética, comunidade. In: BECK, Ulrich; GIDDENS, Anthony Giddens; LASH, Scott. *Modernização Reflexiva: política, tradição e estética na ordem social moderna*. Tradução: Magda Lopes; revisão técnica de Cibele Saliba Rizek. 2 ed. São Paulo: Unesp. 2012. Título Original: *Reflexive Modernization*. p. 198

²⁷ CASTELLS, Manuel. **A sociedade em rede**: a era da informação. p. 69

assimétrico, é verdade – da complexidade nas mais diversas sociedades nacionais e estado-nacionais do planeta”, como bem apontam CRUZ e DANTAS²⁸.

Assim, conforme descrito anteriormente, a Sociedade atual não é a mesma de décadas atrás. Trata-se da nova Sociedade formada através da modernização tecnológica, a chamada “Sociedade da Informação”, cujas principais características, de acordo com MARQUES e CRESPO²⁹, são “a ausência de fronteiras e as distintas formas de comunicação relacionando-se constantemente com a produção e disseminação de conteúdo digital”, que se encontram em um estágio de absoluto dinamismo no que se refere à circulação de dados na Internet.

CASTELLS, por sua vez, faz uma importante distinção analítica entre as noções de “sociedade da informação” e “sociedade informacional” e correlaciona “economia da informação” e “economia informacional”. Ele destaca que o termo sociedade da informação enfatiza o papel da informação na sociedade e faz a ressalva de que a informação, em seu sentido mais amplo, como comunicação de conhecimentos, foi crucial a todas as sociedades. Já o termo informacional, por outro lado, indica “o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico”³⁰.

Essa Sociedade é caracterizada pela globalização das atividades econômicas decisivas do ponto de vista estratégico, por sua forma de organização em redes, pela flexibilidade e instabilidade no emprego e a

²⁸ DANTAS, Marcelo Buzaglo; OLIVIERO, Maurizio; CRUZ, Paulo Marcio. **Direito, transnacionalidade e sustentabilidade empática**. In: Revista do Direito, Santa Cruz do Sul, v. 2, n. 49, p. 29-45, set. 2016. ISSN 1982-9957. Disponível em: <<https://online.unisc.br/seer/index.php/direito/article/view/7911/5122>>. Acesso em: 27/10/2019.

²⁹ MARQUES, Gil da Costa, CRESPO, Marcelo Xavier de Freitas. **Um panorama sobre a Sociedade da Informação: o cloud computing e alguns aspectos jurídicos no ambiente digital**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015. p. 124

³⁰ CASTELLS, Manuel. **A sociedade em rede: a era da informação**. p. 89

individualização da mão-de-obra, o que o sociólogo define como “Sociedade em Rede”. Desta forma, a Sociedade Informacional emerge de um processo de transformação de base capitalista e também de base informacional³¹.

Pela abrangência da definição de Manuel Castells, que abarca a centralidade da informação no processamento e produção do conhecimento, este trabalho compreende a Sociedade da Informação nos parâmetros definidos pelo referido sociólogo.

A lógica do funcionamento de redes, no contexto da Sociedade em Rede, como uma característica da Sociedade da Informação, tem como símbolo a Internet, tecnologia que revolucionou os meios de comunicação e transmissão de dados.

1.1.1 A Internet como agente propulsor da Sociedade da Informação

COLOMBO e FACHINI NETO³² ressaltam a revolução da própria Internet nos últimos anos, que deixou de ser uma ferramenta de uso passivo, no qual as pessoas buscavam informações, para ser uma ferramenta de total interação e fabricação de conteúdo por seus usuários diariamente.

Essas interações possibilitaram um acesso a dados pessoais sem precedentes na história. A *World Wide Web*, criada em 1990 por Tim Berners-Lee, vem crescendo em proporções inimagináveis.

A título de conceituação do termo *Internet*, vale-se da definição constante do inciso I, do art. 5º do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), que conceitua Internet como: “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

³¹ CASTELLS, Manuel. **A sociedade em rede: a era da informação**. p. 58

³² COLOMBO, Cristiano; FACHINI NETO, Eugênio. **Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para a sua adequada implementação à luz do ordenamento brasileiro**. In: *Revista de direito, governança e novas tecnologias*. v. 3. n. 2. jul-dez 2017. p. 61.

Nesse contexto, o surgimento das ferramentas de digitalização, aumentada pela tecnologia de banda larga (Internet de alta velocidade), não somente estimulou a produção e disseminação de conteúdo em diversos formatos, mas especialmente permitiu que categorias como acesso, interação e conectividade se tornassem valores da vida contemporânea.

Nos últimos anos, especialmente com o crescimento do uso interativo da Internet, a detenção de certas informações pessoais passou a ter um valor econômico agregado, isto porque, em posse destes dados, empresas que fornecem bens e serviços tornaram-se capazes de avaliar melhor seus consumidores e atendê-los de forma mais específica e eficiente, entregando produtos cada vez mais personalizados com base nas preferências de sua clientela .

De acordo com KLOEPFER³³, a Internet evoluiu para uma das mais importantes fontes de informação da população, bem como um importante espaço de liberdade de expressão pessoal e, conforme se observa até o presente momento, o acesso a redes globais tem sido garantido de forma neutra e não discriminatória a todos, ou seja, tem-se garantido o uso da Internet como uma rede central de comunicação e conhecimento, acessível de qualquer parte do planeta e por todos.

Destaca-se que a organização da rede e a formatação de seu conteúdo é essencialmente um assunto privado, ainda que existam influências estatais que poderão ser reforçadas em virtude da tendência de controle estatal sobre conteúdos veiculados na Internet.

A respeito do controle estatal, KLOEPFER³⁴ faz uma ressalva de que, embora até o momento a Internet se valha do princípio internacionalizado da autorregulação social (ICANN), os progressos no desenvolvimento de técnicas de

³³ KLOEPFER, Michael. **Neutralidade na rede no âmbito da sociedade da informação**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 140.

³⁴ KLOEPFER, Michael. **Neutralidade na rede no âmbito da sociedade da informação**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 143.

filtragem que criam barreiras de acesso pode vir a acarretar um fortalecimento da influência estatal no âmbito da Internet .

O autor continua seu argumento expondo que a influência estatal se aplica não apenas aos países não democráticos e pré-democráticos (por exemplo, China, Singapura, Arábia Saudita), mas cada vez mais também a Estados democráticos na luta contra conteúdos contrários à ordem constitucional, que incitam a violência, e que envolvam pornografia infantil na Internet. Nas palavras do próprio autor, essa influência estatal “representa uma mudança fundamental no âmbito da até há pouco livre e errática formação das estruturas da Internet, que, em se tratando de Estados de direito, já em virtude de razões ligadas aos direitos fundamentais, não pode ser levada a efeito sem base legal”³⁵.

Acerca da interferência estatal na Internet e para contextualizar os objetivos deste trabalho, que nos próximos capítulos tratará da regulamentação estatal na proteção do direito à privacidade e à proteção de dados no âmbito da Sociedade da Informação, cumpre expor que, embora o Estado disponha de um significativo espaço decisório, especialmente no que concerne aos seus deveres de proteção, as medidas que visam resguardar os direitos fundamentais das pessoas naturais devem se manter em um nível mínimo que garanta a consecução de seus objetivos, embora não se possa deixar de considerar que terceiros (por exemplo, no contexto da concorrência econômica) podem também desfrutar de prerrogativas com base em direitos fundamentais.

Assim, o Estado acaba sendo colocado num contexto marcado por expectativas conflitantes por parte de distintos titulares de direitos fundamentais e deve, nesses casos, tentar resolver tais conflitos, os quais se tornam cada vez latentes e entrelaçados diante das transformações tecnológicas ocorridas nas últimas décadas.

³⁵ KLOEPFER, Michael. **Neutralidade na rede no âmbito da sociedade da informação**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015. p. 144.

CRUZ³⁶ aponta que são as mudanças sociais e políticas que influenciaram e ainda influenciam esta transformação. São os fenômenos sociais que desenham o cenário político à sua volta.

E é mesmo tarefa difícil imposta ao Direito acompanhar os avanços sociais em velocidade cada vez mais acelerada. CRUZ³⁷ lembra, ainda, que a Sociedade atual apresenta um ponto cada vez mais evidente de influência massiva, o desenvolvimento da tecnologia.

Atualmente, existe uma discussão no meio acadêmico sobre a necessidade de criar uma área própria – um direito digital ou algo similar – para regulamentar questões ligadas à Internet e ao espaço virtual. Conforme observam COELHO e SILVEIRA³⁸, “por um lado há o argumento de que valem os princípios vigentes, representando o ambiente digital um contexto onde ocorreriam os mesmos problemas e conflitos do ambiente físico, não virtual. Outra vertente, porém, afirma que a Internet implica novas abordagens, mesmo sobre temas antigos, e tem tamanha influência na atualidade que exigiria a criação de um ramo jurídico específico”.

Independentemente do léxico jurídico atribuído à disciplina da proteção de dados, fato é que o desenvolvimento de novas tecnologias que tornaram possível o processamento massivo de dados transformou a Sociedade contemporânea e o Direito, como produto social que é, deverá acompanhar essa transformação.

Para melhor compreensão da importância que se deve ser conferida a essa matéria, passa-se agora a tecer breves comentários e conceituações acerca de como essas tecnologias transformaram a Sociedade da Informação.

36 CRUZ, Paulo Márcio. **Política, poder, ideologia e estado contemporâneo**. 3 ed. Curitiba: Juruá, 2003. p. 35.

37 CRUZ, Paulo Márcio. **Política, poder, ideologia e estado contemporâneo**. p. 35.

38 COELHO, Alexandre Zavaglia Pereira; SILVEIRA, Vladimir Oliveira. **O processo de inovação tecnológica e elementos da sustentabilidade digital**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015. p. 182.

Como a indústria da tecnologia da informação está no núcleo dinâmico dessa revolução tecnológica, seus produtos têm a característica de “permeiar, potencialmente, todo o processo produtivo”. A mencionada indústria não apenas cria novos produtos ou serviços, como contribui para a reestruturação de todos os demais setores, interligando mercados pela via eletrônica e difundindo informações (e produtos) de maneira globalizada, aumentando, por conseguinte, a geração, a distribuição e a exploração do conhecimento³⁹.

Nesse sentido, a utilização de algoritmos para determinar o perfil dos usuários e as respostas pretendidas representa uma grande tendência no ambiente virtual. A observação de suas preferências, hábitos, ações etc. incrementa cada vez mais as ferramentas, e a rede de colaboração formada entre fornecedor e usuário é um dos principais combustíveis de tal inovação tecnológica, inclusive para desenvolvimento de produtos direcionados ao Poder Público, que passa a se beneficiar de tecnologias movidas por Inteligência Artificial para melhorar a eficiência de suas políticas e atividades-fim.

No mesmo viés, é essencial a utilização das mais modernas técnicas e softwares de gestão do conhecimento no que diz respeito à organização das informações sobre pessoas, processos, produtos, indicadores e dados, dentre diversos outros aspectos internos de uma organização, como forma de socializar o conhecimento, sendo que os principais serão abordados a seguir.

1.1.2 As transformações advindas do trinômio *Cloud Computing*, *Big Data* e Inteligência Artificial

A quantidade de dados criada mundialmente é avassaladora. Relatórios conduzidos pela revista *The Economist* demonstram que a quantidade de dados digitais globais expandiu tão rapidamente que novas tecnologias de armazenamento precisaram ser criadas para guardar essa enxurrada de dados.

³⁹ COELHO, Alexandre Zavaglia Pereira; SILVEIRA, Vladimir Oliveira. **O processo de inovação tecnológica e elementos da sustentabilidade digital**. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 179

1.1.2.1 Big Data

De forma geral, pode-se conceituar *Big Data* como uma tecnologia que permite o processamento de grande volume de informações, com alto desempenho e disponibilidade. Trata-se de ferramentas digitais que tornam a coleta, o processamento e a visualização de dados mais simples, padronizadas e eficazes.

A tecnologia *Big Data*, além de ser importante em decorrência do volume dos dados que é capaz tratar, sua importância também pode ser inferida do fato de que os dados advêm de uma imensa variedade de fontes. De acordo com informações obtidas da internet, somente o Facebook tem mais de 800 milhões de usuários ativos, sendo que mais da metade deles fazem log in todos os dias, e, através da referida rede social, acessam mais de 900 milhões de *web pages* e fazem o *upload* mais de 250 milhões de fotos diariamente. Outra grande fonte geradora diária de dados são as atividades financeiras realizadas pela Internet, tais como pagamentos com cartões de crédito, transferências e demais movimentações bancárias.

O conceito de *Big Data* pode implicar, ainda, a capacidade de transformar dados brutos em gráficos e tabelas que permitem a demonstração do fenômeno a ser demonstrado, sendo, portanto, de extrema importância garantir a veracidade das informações geradas, uma vez que as decisões estão sendo tomadas cada vez mais com base em dados⁴⁰.

Da mesma forma, o aumento no uso e na qualidade das redes de sensores, tais como as câmeras de vigilância, os veículos com computadores embutidos, os bilhões de telefones celulares que todos os dias registram localizações, movimentos e atividades, proporcionam a chamada “coleta ubíqua de dados”, em razão de que quase tudo que as pessoas fazem resultam na captura, armazenamento e, inclusive, a venda desses dados a terceiros.

⁴⁰ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019. Versão Kindle. Posição 206.

MAGRANI⁴¹ destaca, ainda, que a combinação entre objetos inteligentes e Big Data pode alterar significativamente a forma como se vive. Essa capacidade de conexão, chamada de Internet das Coisas, vem recebendo fortes investimentos do setor privado e surge como possível solução diante dos novos desafios de gestão pública, prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros.

1.1.2.2 Cloud computing

Nesse passo, o fato de todos os dados acima mencionados serem digitais é muito significativo, uma vez que eles podem ser armazenados, compartilhados, acessados, combinados e duplicados em velocidade extraordinária, a baixo custo, a partir de qualquer lugar do mundo, além de serem acompanhados de meta dados⁴². De acordo com SCHNEIER, há aproximadamente cinco vezes mais meta dados do que informações, os quais podem ser obtidos através do cruzamento de informações pela tecnologia Big Data e têm a capacidade de se mostrarem extraordinariamente reveladores.

Com o advento da computação em nuvem, as pessoas não têm mais a necessidade de armazenar informações em servidores pessoais, de maneira localizada. O armazenamento pode ser atualmente fornecido a um custo muito menor remotamente do que localmente.

As principais características do *cloud computing* são: serviços sob demanda, acesso de rede banda larga, *pool* de recursos, elasticidade e facilidade de expansão e serviço de mediação. De acordo com MARQUES e CRESPO⁴³, “a

⁴¹ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** Posição 223.

⁴² SCHNEIER define meta-dados da seguinte forma: *Data is content, and metadata is context. Metadata can be much more revealing than data, especially when collected in the aggregate. When you have one person under surveillance, the contents of conversations, text messages, and e-mails can be more important than the metadata. But when you have an entire population under surveillance, the metadata is far more meaningful, important, and useful.*

⁴³ MARQUES, Gil da Costa, CRESPO, Marcelo Xavier de Freitas. **Um panorama sobre a sociedade da informação: o cloud computing e alguns aspectos jurídicos no ambiente digital.** In:

computação em nuvem é, sem dúvidas, o novo paradigma na área de Tecnologia da Informação, não se resumindo a ser uma mera tendência”.

Os autores⁴⁴ advertem, ainda, que as empresas vão, hora mais, hora menos, migrar para o ambiente de *cloud*, uma tendência mundial decorrente do fenômeno *Big Data*, conceituado anteriormente, e da pressão sofrida pela área de Tecnologia da Informação para entregar aplicações com mais velocidade capazes de suportar os negócios pelos mais variados dispositivos, principalmente os sem fio.

Aqui, importante fazer a ressalva, que será revisitada mais adiante, de que o armazenamento remoto, em que pese seu baixo custo e conveniência, implica em riscos à proteção de dados, já que não se deve esquecer que “a nuvem” nada mais é do que o servidor de um terceiro.

Nesse aspecto, vale destacar a decisão do Conselho Nacional de Justiça, nos Autos do PROCEDIMENTO DE COMPETÊNCIA DE COMISSÃO - 0002582-36.2019.2.00.0000⁴⁵, que suspendeu um contrato de R\$ 1,34 bilhões, firmado entre a empresa Microsoft e o Tribunal de Justiça do Estado de São Paulo, para desenvolvimento do novo sistema de processo judicial eletrônico daquele tribunal, em razão de a contratação ter ocorrido sem licitação e sem observar Resoluções do próprio CNJ.

A decisão do CNJ, que será tratada com maior profundidade no Capítulo 2 deste trabalho, traz relevantes questionamentos acerca da segurança das informações e dos dados de pessoas e empresas constantes dos processos em tramitação perante o TJSP, uma vez que eles sejam transferidos a servidores terceiros, nacionais ou não, transferência essa facilitada pelo *cloud computing*.

Direito, Inovação e Tecnologia. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 132.

⁴⁴ MARQUES, Gil da Costa, CRESPO, Marcelo Xavier de Freitas. **Um panorama sobre a sociedade da informação:** o cloud computing e alguns aspectos jurídicos no ambiente digital. In: *Direito, Inovação e Tecnologia*. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 134.

⁴⁵ BRASIL, **Conselho Nacional de Justiça**. Procedimento de Competência de Comissão nº 0002582-36.2019.2.00.0000. Relator: Conselheiro Márcio Schiefler Fontes. Brasília, 2019. Diário da Justiça, Brasília, 17 jun. 2019

Quanto ao serviço de armazenamento de dados judiciais em ambiente de nuvem de provedor localizado em terras estrangeiras, o voto do Relator, Conselheiro Márcio Schiefler Fontes, ao tratar da segurança das informações na referida decisão, consigna o seguinte:

É dizer: potencialmente falando, empresa estrangeira, em solo estrangeiro, manterá guarda e acesso a dados judiciais do Brasil, onde a intensa judicialização reúne, nos bancos de dados dos Tribunais, uma infinidade de informações sobre a vida, a economia e a sociedade brasileira, o que, ressalvadas as cautelas certamente previstas, pode vir a colocar em risco a segurança e os interesses nacionais do Brasil, num momento em que há graves disputas internacionais justamente acerca dessa matéria.

Pelo exposto, a computação em nuvem propicia discussões fundamentalmente importantes acerca da segurança da informação, em especial no que concerne à eventual indisponibilidade do serviço que impeça o acesso aos dados, a possível violação a leis específicas de proteção de dados sensíveis ou sigilosos, dependendo do tipo de informação e dos países envolvidos etc. Ou seja, se por um lado o *cloud computing* pode custar menos, por outro é fundamental avaliar a segurança e legalidade dos servidores (*data centers*).

1.1.2.3 Inteligência Artificial

Ao se pensar na importância do Big Data, é crucial, também, ter em mente que o acesso a tantos dados, de tantas fontes diferentes, não teria a relevância que hoje se observa sem a aplicação do poder computacional para processar tais dados. Esse poder computacional capaz de produzir meta-dados se denomina Inteligência Artificial, e, através de seu uso, é possível inferir padrões, realizar descobertas e revelar segredos até então desconhecidos.

Segundo MAGRANI⁴⁶, a Inteligência Artificial, termo cunhado em 1956 pelo pesquisador da Universidade de Stanford, John McCarthy, é um subcampo da informática e tem como objetivo habilitar o desenvolvimento de computadores que sejam capazes de emular a inteligência humana ao realizar

⁴⁶ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** Posição 777.

determinadas tarefas, e se consubstancia em um programa de computador capaz de fazer algo normalmente atribuível à inteligência de seres humanos.

O pesquisador MACCAN⁴⁷ argumenta que:

“[...] this new-found power has already yielded fabulous successes in fields such as medical research, where drug interactions and the efficacy of treatments can be assessed in ways never before possible and without endangering lives through interventional research”.

Os algoritmos, base da Inteligência Artificial, por sua vez, tornaram-se essenciais no gerenciamento de nossas vidas digitais e na navegação pelo mundo digital. Sem eles, seria muito difícil fazer sentido da grande massa de informação digital disponível. Contudo, agora que os algoritmos empunham essa influência, deve-se acompanhar a responsabilidade de não fazer mal uso deles – especialmente para não fortalecer discriminações sociais e preconceitos⁴⁸ (assim como se tem visto na China, com o Crédito Social).

Observa-se, portanto, que, nos últimos anos, especialmente com o crescimento do uso interativo da internet, a detenção de certas informações pessoais passou a ter um valor econômico agregado, isto porque em posse destes dados, empresas que fornecem bens e serviços tornaram-se capazes de avaliar melhor seus consumidores e atendê-los de forma mais específica e eficiente, entregando um produto cada vez mais personalizado com base nas preferências de sua clientela⁴⁹.

⁴⁷ MACCANN, Duncan. **Power and accountability in the digital economy**. Data and big tech companies have more and more power. As the digital economy develops, we need to put people and society at the centre. Accessed 15/10/2019 <https://neweconomics.org/2019/10/power-and-accountability-in-the-digital-economy>.

⁴⁸ MACCANN, Duncan. **Power and accountability in the digital economy**. Data and big tech companies have more and more power. As the digital economy develops, we need to put people and society at the centre. Accessed 15/10/2019 <https://neweconomics.org/2019/10/power-and-accountability-in-the-digital-economy>.

⁴⁹ COLOMBO, Cristiano; FACHINI NETO, Eugênio. **Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para a sua adequada implementação à luz do ordenamento brasileiro**. p. 64-65.

Toda essa rede de dados disponível trouxe uma capacidade de aumentar lucros e diminuir desperdícios. Portanto, tais informações podem ser muito valiosas.

Esse segmento da Economia Digital, ao qual se tem referido como “Economia de Dados” ou *Data Economy*, tem como força motriz a tecnologia advinda do trinômio “Computação em Nuvem, *Big Data* e Inteligência Artificial”, anteriormente descrito.

1.2 REVOLUÇÃO TECNOLÓGICA E ECONOMIA INFORMACIONAL: O INFORMACIONALISMO

A expansão da Revolução Industrial foi seletiva e lenta pelos padrões atuais de difusão tecnológica. As novas tecnologias da informação, por sua vez, difundiram-se globalmente com grande velocidade em menos de duas décadas, entre meados dos anos 70 e 90, por meio da aplicação imediata no próprio desenvolvimento da tecnologia gerada, conectando o mundo através da tecnologia da informação⁵⁰.

CASTELLS⁵¹ denominou de Informacionalismo o rejuvenescimento e transformação do Capitalismo Industrial, voltado para conhecimento da economia e maximização da produção, para o Capitalismo Informacional, com vistas ao desenvolvimento tecnológico, ou seja, a acumulação de conhecimentos e maiores níveis de complexidade do processamento da informação. No Informacionalismo é a busca por conhecimentos e informação que caracteriza a função da produção tecnológica, reforçando uma íntima ligação entre cultura e forças produtivas e entre espírito e matéria.

[...] o fator histórico mais decisivo para a aceleração, encaminhamento e formação do paradigma da tecnologia da informação e para a indução de suas conseqüentes formas sociais foi/é o processo de reestruturação capitalista, empreendido desde os anos 80, de modo que o novo sistema econômico e tecnológico pode ser adequadamente caracterizado como capitalismo informacional.

⁵⁰ CASTELLS, Manuel. **A sociedade em rede: a era da informação.** p. 70

⁵¹ CASTELLS, Manuel. **A sociedade em rede: a era da informação.** p. 54

Segundo CASTELLS⁵², o Informacionalismo é caracterizado pela interdependência global dos mercados financeiros, o que resulta de cinco fatos principais: 1) a desregulamentação dos mercados financeiros na maioria dos países e a liberalização das transações internacionais; 2) a criação de uma infraestrutura tecnológica, capaz de processamento em alta velocidade dos modelos necessários para lidar com a complexidade das transações; 3) natureza dos novos produtos financeiros, como os derivativos, que geram capitalização de mercado oriunda da capitalização de mercado; 4) movimentos especulativos de fluxos financeiros para aproveitar diferenças em valorização ou evitar uma perda, assim ampliando tendências do mercado; 5) firmas de avaliação do mercado.

Neste capitalismo informacional cada vez mais globalizado, os verdadeiros agentes do comércio no âmbito internacional deixaram de ser os países e passaram a ser as redes de empresas, as quais, apoiadas nas novas tecnologias da comunicação e dos transportes, fazem uso de suas conexões com redes que operam no mercado mundial, não sendo, mais, necessário que se estabeleçam fisicamente em determinado país para terem atuação e operarem no mercado mundial⁵³.

1.2.1 O novo paradigma da economia de dados (*data economy*)

Diante da evolução da produção do capital no âmbito da economia informacional é possível identificar um novo fenômeno oriundo da tecnologia desenvolvida nos últimos anos. O cruzamento de dados pessoais com análises de comportamento em redes sociais, registros de compras efetuadas com cartões de crédito, o tempo que o indivíduo passa em determinadas páginas da internet e informações de geolocalização registrados podem estabelecer parâmetros fieis para identificar e traçar perfis consistentes de determinado indivíduo, seus gostos e interesses, quer seja para direcionar um produto ou serviço, contratar um profissional, ou até mesmo para identificar um potencial criminoso.

⁵² CASTELLS, Manuel. **A sociedade em rede: a era da informação.** p. 146-147.

⁵³ CASTELLS, Manuel. **A sociedade em rede: a era da informação.** p. 156.

Na Sociedade da Informação, verifica-se um rápido aumento na quantidade e na qualidade das informações que se consegue reunir através do acesso aos dados, amplamente espalhados e compartilhados na internet.

A produtividade e a competitividade na produção informacional baseiam-se na geração de conhecimentos e no processamento de dados, de modo que a capacidade tecnológica capaz de produzir inteligência pela conexão entre conhecimento e dados passa a ser uma das ferramentas fundamentais para a concorrência entre empresas, organizações de todos os tipos e, também, países⁵⁴.

O que se evidencia é que essa rede de dados transformada em conhecimento possibilitou aumentar lucros e diminuir perdas, e, portanto, tal informação tende a ser muito valiosa.

Os dados, atualmente, são uma característica constante da maioria das atividades econômicas, e é nesse contexto que uma nova economia, no âmbito do Informacionalismo visionado por Manuel Castells, está emergindo. Economia esta fomentada por um novo tipo de combustível: dados. De fato, a revista britânica *The Economist* compara a coleta de dados pessoais e sua transformação em informações úteis ao descobrimento do petróleo como combustível no século passado. O artigo menciona:

A NEW commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era⁵⁵.

Assim como o petróleo foi considerado a matéria-prima principal para muitas das atividades industriais desenvolvidas principalmente no pós-guerra, os dados passaram a ser considerados o insumo do qual se alimentam

⁵⁴ CASTELLS, Manuel. **A sociedade em rede**: a era da informação. p. 165.

⁵⁵ THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**: the data economy demands a new approach to antitrust rules. Disponível em: <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>>. Acesso em: 20/10/2019.

grande parte dos serviços e das indústrias que se interconectam no meio ambiente digital.

É cediço que uma economia tradicional é definida quando os fatores de produção – terra, mão de obra e capital – são usados em um formato preestabelecido, por meio do qual o produto final, seja ele um bem ou um serviço, é resultado da transformação de insumos utilizados no processo produtivo. A partir disto, cria-se, então, um mercado não só para esse produto final, como também para os insumos. À medida que o número de produtores muda, por meio de fusões e aquisições, por exemplo, podem surgir oligopólios ou monopólios para controlar a quantidade e o preço de determinados produtos. Como visto, os dados assumiram a posição de matéria-prima uma vez que se transformaram em moeda comum do Mercado e são produzidos por quase todas as transações, em que os resultados, anteriormente descartados em meio à vasta de gama de informações consideradas sem valor, como advento das tecnologias de Big Data tornaram-se, valiosos insumos capazes de gerar valor subsequente. Assim, a partir do reconhecimento da importância dos dados pelos indivíduos, por empresas e pelos próprios governos, emergiu um mercado para a comercialização de dados, que se constitui na Data Economy. Dessa forma, a intervenção governamental passa a ser necessária para prevenir abuso de poder de mercado e proteger o interesse público⁵⁶.

KUMAR, CHIK, NG e TEO⁵⁷ destacam, também, que não se deve confundir a economia baseada em dados, a data economy, com economia digital, apesar de as diferenças serem sutis. Em que pese ambas dependerem da tecnologia da informação e da capacidade computacional, a economia digital se refere à conversão dos processos manuais em processos digitais, nos quais os computadores realizam as tarefas que, anteriormente, eram desenvolvidas manualmente. Contudo, ainda há a necessidade de imputar o dado no computador de forma manual. Por exemplo: os dados referentes a resultados das

⁵⁶ KUMAR, Sree; CHIK, Warren B.; NG, See-Kiong; TEO, Sin Gee. **The data economy: implications from Singapore**. New York: Routledge, 2019. (versão Kindle). Posição 286

⁵⁷ KUMAR, Sree; CHIK, Warren B.; NG, See-Kiong; TEO, Sin Gee. **The data economy: implications from Singapore**. Posição 308

vendas, precificação, controle de estoque e outras variáveis precisam ser alimentados no computador para que este realize o trabalho para o qual foi programado. Se houvesse sensores que transmitissem a venda dos produtos e sua precificação diretamente do item até as caixas registradoras que também coletam os dados referentes à forma de pagamento, data e horário, e todos esses dados fossem automaticamente capturados por um sistema computacional que analisa as vendas, as receitas, os custos, entre outros, haveria, então, a migração do mundo digital para o mundo de dados.

Da mesma forma, pode-se considerar uma transação realizada com cartão de crédito. Tal transação, além de registrar dados como o nome do comprador, seus dados bancários, lugar, data e horário da transação, comerciante e produto ou serviço comprado, é capaz de fornecer um profundo conhecimento em relação às preferências e comportamentos do titular do cartão de crédito. Porém, quando esses dados são cruzados com as informações de inúmeros outros titulares de cartão de crédito, de diferentes partes do mundo, a operadora de cartão de crédito tem acesso a padrões comportamentais dos envolvidos nas negociações. Além disso, ao ter acesso aos dados pessoais, a referida operadora pode segmentar sua base de dados de titulares com base no gênero, idade, profissão, renda, comportamento, avaliação de crédito etc., e este cruzamento de dados se refere a um simples exemplo de uma transação básica de cartão de crédito. Outro exemplo, menos aparente, da diferença entre digitalização e o que os autores denominam “*datafication*” pode ser observado na forma em que a Google digitalizou textos e, então, transformou-os em dados (“*datafied*”) por meio do uso de caracteres ópticos de reconhecimento para identificar e reconhecer as letras, palavras, frases e parágrafos em um texto⁵⁸.

Este fenômeno é tão expressivo que fez surgir um nicho de mercado especializado na coleta de dados e informações de usuários da internet e de serviços remotos, via telefone, por exemplo, é a chamada “mineração de dados”.

⁵⁸ KUMAR, Sree; CHIK, Warren B.; NG, See-Kiong; TEO, Sin Gee. **The data economy: implications from Singapore**. Posição 323

Esta mineração de dados não é tão somente a coleta de informações aleatórias. Ela trata de gerar conhecimento vantajoso para certos setores da Economia, agregando a estas informações valor econômico⁵⁹.

O que essas empresas fazem, portanto, é a colheita de dados, incluindo dados pessoais, em escala industrial. E, por mais que o desenvolvimento da tecnologia tenha beneficiado os consumidores, que voluntariamente escolhem não viver mais sem o mecanismo de busca do Google, as comodidades de entregas de um dia da Amazon ou sem as atualizações sociais do *newsfeed* do Facebook e Instagram, para citar alguns, faz-se necessário destacar que há motivos para preocupação à medida em que o controle sobre os dados exercido por essas empresas concede a elas, e aos governos abastecidos pelos dados por elas gerados, uma grande quantidade de poder, assim como aconteceu com o petróleo, quando este era o mais importante combustível da economia de seu tempo, que ocasionou as grandes guerras pelo poder do último século.

Apoiando-se em LASH⁶⁰, as empresas de tecnologia atuais, caracterizadas por conglomerados multibilionários, podem ser consideradas as “vencedoras” da pós-modernidade, pelo acesso irrestrito a bancos de dados de valores inestimáveis e modos de processamento de Informação e Comunicação, com o consequente controle do capital e das tecnologias de que todos se tornaram dependentes.

⁵⁹ COLOMBO, Cristiano; FACHINI NETO, Eugênio. **Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para a sua adequada implementação à luz do ordenamento brasileiro.** p. 62.

⁶⁰ LASH, Scott. **A reflexividade e seus duplos: estrutura, estética, comunidade.** In: BECK, Ulrich; GIDDENS, Anthony Giddens; LASH, Scott. *Modernização Reflexiva: política, tradição e estética na ordem social moderna.* p. 199.

1.3 A EVOLUÇÃO DO DIREITO À PRIVACIDADE: RUMO A UM NOVO DIREITO FUNDAMENTAL?

A transformação da Sociedade que este trabalho se propôs a apresentar até o momento é o que BOBBIO⁶¹ chama de condições históricas que se traduzem em elementos sociais de cada época que geram a necessidade de modificação do entendimento acerca de certos direitos outrora elencados.

1.3.1 O direito fundamental à privacidade

Em 1890, o direito à privacidade foi tratado, de forma pioneira, nos Estados Unidos por Samuel Warren e Louis D. Brandeis, que posteriormente se tornaria *Justice* da Suprema Corte americana, no artigo intitulado “The Right to Privacy”⁶², publicado na Harvard Law Review, que trouxe a ideia de um direito básico à proteção da pessoa e de um direito de estar sozinho (*right to be let alone*). Partindo deste ponto inicial é que se desenvolveu o pensamento de que o indivíduo teria o direito de decidir sobre divulgação de informações pessoais relevantes sobre sua pessoa, que serviu como base para o que o Tribunal Constitucional Federal alemão, em 1983, definisse o direito à autodeterminação informativa, como se verá na sequência deste trabalho.

No que se refere à vida privada, impende destacar a conceituação de SILVA⁶³:

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

⁶¹ BOBBIO, Norberto. **A era dos direitos**. Tradução: Carlos Nelson Coutinho. Título original: L'età dei Diritti. Rio de Janeiro: Elsevier, 2004. p. 13.

⁶² WARREN, Samuel; BRANDEIS, Louis D. **The right to privacy**. Foreword by Steven Alan Childress. New Orleans: Quid Pro Law Books, 2010. (Versão Kindle). p. 5.

⁶³ SILVA, José Afonso. **Curso de direito constitucional positivo**. 13 ed. São Paulo: Malheiros, 1997. p. 204.

Já a privacidade, na definição de LAFER⁶⁴, é “o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada”.

Para BASTOS⁶⁵, o direito à privacidade é a “faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um e, também, impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano”.

Como visto anteriormente, ao tratar do tópico da Economia de Dados, foi possível verificar que, com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Conforme assevera Pablo Stolze *apud* LOPES⁶⁶: “não raro determinadas empresas obtêm dados pessoais dos usuários (profissão, renda mensal, hobbies), com o propósito de ofertar os seus produtos, veiculando as sua publicidade por meio dos indesejáveis spams, técnica ofensiva à intimidade e à vida privada”.

Há tempos a Sociedade civil demanda a imposição de limites na coleta e uso de dados pessoais por organizações públicas e privadas. Essas demandas e esforços têm forte embasamento na Declaração Universal dos Direitos Humanos de 1948, que reconheceu valores da proteção à privacidade e a liberdade de informação, opinião e expressão.

Faz-se importante contextualizar o processo pelo qual a Europa estava passando após a Segunda Guerra Mundial. As nações estavam reconstruindo e reestabelecendo suas instituições, firmemente convictas em deixar para trás as marcas da perseguição Nazista e dar ensejo a uma nova era

⁶⁴ LAFER, Celso. **A reconstrução dos direitos humanos**. São Paulo, Companhia das Letras, 1998.

⁶⁵ BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 21 ed. São Paulo: Saraiva, 2000.

⁶⁶ LOPES, Alan Moreira. **Lei 12.965, de 23.04.2014** – estabelece princípio, garantias, direitos e deveres para o uso da internet no Brasil (marco civil da internet). In TEIXEIRA Tarcísio; LOPES, Alan Moreira. **Direito das novas tecnologias**. São Paulo: Revista dos Tribunais, 2015. (p. 50)

de direitos para que os horrores da degradação humana e da perseguição se tornassem uma prática banida para sempre.

Cumpre lembrar que, no pós guerra, diversos governos na Europa mantinham dossiês contendo informações sobre uma grande parte da população, em sua maioria relacionado à etnicidade e orientação sexual e que serviram de base para a perseguição testemunhada pelo mundo.

O sentimento de medo deixado nas nações europeias em relação ao controle político e social oriundo do uso de informações coletadas sobre as pessoas é uma das explicações por que tais nações consideram a Privacidade um direito fundamental que deve ser protegido a todo custo.

Neste ponto, vale destacar as observações feitas por Scott Lash ao tratar da segunda modernidade, estabelecida no final do século XX e início do século XXI, que ele, juntamente com outros sociólogos, notadamente Anthony Giddens e Ulrich Beck, denominou de Modernidade Reflexiva. Em sua obra, LASH⁶⁷ assevera que o filósofo Zygmunt Bauman confere a esta modernidade um caráter étnico, tendo como simbolismo central a figura do “judeu” no sentido de ponto de reflexão da Sociedade, ou seja, de como as pessoas se observam e são representadas dentro de um contexto. Segundo o filósofo, o holocausto é entendido como o triunfo final do “conceito”, a vitória da modernidade cartesiana e identitária e afirma que, após o holocausto, a ética só pode ser uma ética de não identidade, com a ruptura das classificações⁶⁸.

O trecho acima corrobora a forma como o pensamento europeu acerca dos conceitos de intimidade e identidade se desenvolveu no pós-guerra e as marcas deixadas naquela Sociedade, onde, não só a privacidade, como também a proteção dos dados pessoais, são consideradas direitos fundamentais dos cidadãos.

⁶⁷ LASH, Scott. **A reflexividade e seus duplos**: estrutura, estética, comunidade. In: BECK, Ulrich; GIDDENS, Anthony Giddens; LASH, Scott. *Modernização Reflexiva: política, tradição e estética na ordem social moderna*. p. 218.

Em 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) emitiu um conjunto de diretrizes sobre a proteção da privacidade e o fluxo transfronteiriço de dados pessoais, as quais devem ser observadas por todos os Estados-membro. Essas diretrizes, atualizadas em 2013, englobam uma estrutura da Privacidade que estabelece os limites na coleta, armazenamento e uso de dados.

De acordo com o Prefácio das referidas diretrizes, escrito em 1980, ou seja, antes do advento da Internet e muito antes das tecnologias de *Big Data* e inteligência artificial terem sido desenvolvidas, chama à atenção a atualidade do texto, que foi capaz de prever as transformações tecnológicas dos anos seguintes ao dispor que:

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data. On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance⁶⁹.

Assim, ao se ter conhecimento da quantidade de poder que as organizações processadoras de dados pessoais, tanto públicas como privadas, estavam acumulando em decorrência do acesso e controle sobre as informações pessoais que transitam no âmbito da internet, o desenvolvimento de servidores

⁶⁹ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD guidelines on the protection of privacy and transborder flows of personal data**. Disponível em: <<http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm#preface>>. Acesso em: 20.11.2019.

que armazenavam não só informações pessoais, mas também perfis psicológicos e de hábitos dos indivíduos, fez com que a Europa saísse em frente e desenhasse uma legislação unificada que fosse aplicável a todo o bloco econômico.

Como VAINZOF⁷⁰ assevera, há uma premissa básica e essa é a de que não existem direitos absolutos, contudo, qualquer tipo de limitação imposta a um direito fundamental deve ser moderada, necessária e proporcional.

BOBBIO assevera que “não se concebe como seja possível atribuir um fundamento absoluto a direitos historicamente relativos”⁷¹.

O relativismo no caso da mineração de dados e utilização destes por gigantes empresariais concerne especificamente ao direito à privacidade previsto na Constituição da República Federativa do Brasil – CRFB em seu inciso X, art. 5º:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação⁷²;

Ao ler a norma não é difícil entender como o direito à privacidade e a mineração de dados estão intrinsicamente entrelaçadas e são inversamente proporcionais, isto é, quanto mais um lado cresce, o outro diminui.

O direito à privacidade já é muito bem consolidado. Não se necessita mais discutir sua validade, natureza ou fundamentos. Não é mais uma questão filosófica. É agora uma questão jurídica e política, especialmente diante dos

⁷⁰ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. LGPD: **Lei Geral de Proteção de Dados**. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019. p. 22.

⁷¹ BOBBIO, Norberto. **A era dos direitos**. p. 13.

⁷² BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF. Diário Oficial da União, Distrito Federal, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 01/10/2019.

relatos acima, concernente à forma de melhor proteger este direito a fim de impedir que ele seja constantemente violado⁷³.

A coleta “predadora” de dados pessoais gerou uma transformação no sentido clássico do direito à privacidade que, entendia-se, em última instância, ser “o direito de ser deixado em paz”, para ser, além do já proposto, também o direito de não ter sua vida pessoal invadida e posta à venda⁷⁴.

Novamente buscam-se os ensinamentos de BOBBIO em relação ao relativismo dos direitos fundamentais. O direito é dinâmico e plural devendo também o ser o sistema jurídico que o protege⁷⁵.

De acordo com os ensinamentos de SCHNEIER⁷⁶: *“the most common misconception about privacy is that it’s about having something to hide. If you aren’t doing anything wrong, then you have nothing to hide, the saying goes, with the obvious implications that privacy only aids wrongdoers”*. Basta pensar que alguns aspectos triviais da vida cotidiana incluem a existência de segredos tais como: mensagens íntimas a amantes e amigos; conversas com médicos sobre problemas que não se gostaria que outra pessoa soubesse; procuras por empregos sem o conhecimento do empregador, entre outros, que nada mais são do que aspectos da vida privada que nada têm de errado. Eles são somente parte da vida íntima. Outro aspecto inerente à natureza humana é agir de maneira diferente de acordo com quem ou onde as pessoas se encontram, se em uma reunião de negócios ou na privacidade de suas casas.

⁷³ BOBBIO, Norberto. **A era dos direitos**. p. 17.

⁷⁴ COLOMBO, Cristiano; FACHINI NETO, Eugênio. **Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para a sua adequada implementação à luz do ordenamento brasileiro**. p. 66.

⁷⁵ BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004. p. 13.

⁷⁶ SCHNEIER, Bruce. **Data and Goliath: the hidden battles to collect your data and control your world**. p. 127

A privacidade é, portanto, condição inerente à espécie humana. É a privacidade que possibilita às pessoas agirem de maneira apropriada dependendo do cenário em que se encontram⁷⁷.

Para LEONARDI⁷⁸, neste novo contexto, “o atributo básico do direito à privacidade seria, portanto, a capacidade de o indivíduo controlar a circulação de informações a seu respeito”.

Feitas estas breves notas introdutórias acerca da Privacidade, passa-se agora a identificar os impactos da tecnologia sobre este conceito.

1.3.2 Os impactos à privacidade e à proteção de dados na Sociedade da Informação

Como mencionado anteriormente, a Sociedade da Informação, cujas principais características segundo MARQUES e CRESPO⁷⁹, são “a ausência de fronteiras e as distintas formas de comunicação relacionando-se constantemente com a produção e disseminação de conteúdo digital”, encontra-se em um estágio de absoluto dinamismo em relação à circulação de dados na Internet.

Há milhares de perfis digitais de indivíduos, coletados dos rastros de dados deixados online. Acxiom, uma das grandes empresas negociadoras de dados do planeta estima que 30% dos dados de cada um desses perfis é incorreto. Dada à qualidade incerta dos perfis que estão sendo construídos e o crescente uso de perfis digitais pelos setores públicos e privados, resultados incorretos podem gerar uma série de implicações às vidas das pessoas⁸⁰.

⁷⁷ SCHNEIER, Bruce. **Data and Goliath: the hidden battles to collect your data and control your world**. p. 148

⁷⁸ LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p. 67

⁷⁹ MARQUES, Gil da Costa, CRESPO, Marcelo Xavier de Freitas. **Um panorama sobre a Sociedade da Informação: o *cloud computing* e alguns aspectos jurídicos no ambiente digital**. In: Direito, Inovação e Tecnologia. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. p. 124.

⁸⁰ KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B. **The challenge of 'big data' for data protection**. International Data Privacy Law, Vol. 2, No. 2. Oxford University Press, 2012. Disponível em: <<https://academic.oup.com/idpl/article-abstract/2/2/47/755343>>. Acesso em: 24/10/2019

Dessa forma, a Sociedade de hoje precisa estar apta a experimentar novas tecnologias e novos negócios baseados nessas tecnologias, e isso inclui tecnologias de vigilância. O truque será maximizar os benefícios gerados pela coleta, armazenamento e análise dos dados pessoais das pessoas, ao mesmo tempo que os riscos são diminuídos⁸¹.

Apenas a título de exemplificação, relacionam-se alguns danos em potencial gerados pelo mal uso de tecnologias de vigilância por Corporações, quais sejam: discriminação, manipulação e invasão de privacidade. Destacam-se os possíveis danos causados pelo mal uso (e abuso) dessas tecnologias pelo Poder Público, tais como: perseguições baseadas em dados digitais falsos ou desatualizados, censura governamental, *chilling effects*⁸², inibição de discordância⁸³, *secrecy creep*⁸⁴, abuso, e cerceamento da liberdade no ambiente da Internet.

Como a experiência tem demonstrado, a tecnologia *Big Data* posicionou a proteção de dados em um contexto diferente. Sendo os dados a “moeda” da sociedade da informação, mas em um mundo em que as pessoas são representadas em forma de dados, cujos cruzamentos com demais informações coletadas da rede fornecem as bases para as tomadas de decisão, faz-se importante levantar a questão se a correta acessibilidade, acuracidade e

⁸¹ SCHNEIER, Bruce. **Data and Goliath**: the hidden battles to collect your data and control your world. New York: W.W.Norton & Company, Inc., 2015. p. 224.

⁸² A expressão *Chilling Effect* (em tradução livre, “efeito inibidor” ou “efeito amedrontador”) utilizada em um contexto legal é a inibição ou desencorajamento do exercício legítimo de direitos legais e naturais pela ameaça de sanção legal. O direito que é mais comumente descrito como sendo suprimido por *chilling effect* é o direito constitucional de liberdade de expressão. Um *chilling effect* pode ser causado por ações legais como a aprovação de uma lei, a decisão de uma corte, ou a ameaça de um processo; quaisquer ações legais que causem às pessoas medo de repercussões legais pelo exercício de um direito legítimo, seja a liberdade de expressão ou qualquer outro

⁸³ SCHNEIER entende que o monitoramento em massa tem o poder de silenciar opiniões minoritárias e discordantes do *status quo*. De acordo com expert em segurança, é justamente a capacidade de discordar e expor opiniões contrárias que fomentam a evolução da Sociedade e, consequentemente, da legislação. O medo de represálias por parte do Governo inibe a exposição de novas ideias e a liberdade de experimentar coisas novas.

⁸⁴ *Secrecy creep* pode ser entendido como o medo de revelar e/ou expor informações governamentais sigilosas, diante das severas punições direcionadas a *whistleblowers* (denunciantes), de acordo com Schneier.

confiabilidade dos dados podem vir a importar tanto, ou talvez até mais, que a própria privacidade.

A proteção de dados pessoais é uma maneira indireta de atingir seu principal objetivo, que é a proteção da própria pessoa. É importante ter em mente que os dados pessoais são a pessoa e como tal devem ser tratados, justificando sua tutela pelo Direito de forma a afastar a utilização de um regime de livre apropriação e disposição contratual desses dados que não levem em conta seu caráter personalíssimo. É em razão, também, dessas características que diversos ordenamentos jurídicos consideram a proteção de dados pessoais como um direito fundamental, cujo objetivo é o de efetivar a liberdade da pessoa no âmbito da Sociedade da Informação⁸⁵.

Diante deste novo contexto, é função do Direito assegurar que os indivíduos não sejam responsabilizados por coisas que não fizeram, ou por serem alguém que não são, por meio da imposição de limites na aceitação como verdade absoluta dos resultados originados do tratamento dos dados pelo uso de algoritmos e demais tecnologias, uma vez que tais resultados podem não representar a realidade dos fatos.

É necessário, ainda, regular o mercado para prevenir o enriquecimento ilícito e antiético por meio da utilização indiscriminada de dados pessoais no desenvolvimento de perfis e produtos tecnológicos, cujas consequências e reações adversas ainda não são passíveis de ser mensuradas, a exemplo da utilização da energia nuclear que, embora apresente inúmeros benefícios, traz em seu bojo um poder tão destruidor que a transformou em objeto de regulação em âmbito global.

1.3.3 Os desafios do Direito no tratamento da proteção de dados e prevenção do abuso de poder na Sociedade da Informação

O Direito surge como o mecanismo de compreensão do mundo para organizar o caos potencial de todas as coisas.

⁸⁵ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** Posição 1207.

Sempre a reboque da realidade, quase sempre atrasado em seu intento, o Direito tem por fim ser a “solução prudente dentro da ordem” (segundo José de Oliveira Ascensão) ou, ainda, “um conjunto de regras obrigatórias que garante a convivência social graças ao estabelecimento de limites à ação de cada um de seus membros” (para Miguel Reale)⁸⁶.

Nesse sentido, o que se almeja, através do Direito, é o equilíbrio entre a liberdade de ação e a regulação jurídica, por meio da imposição de limites que visem assegurar o desenvolvimento ético e sustentável da Sociedade contemporânea, em que os efeitos da hiperconectividade já se fazem sentir.

Segundo leciona SCHNEIER, para que a maioria das sociedades se desenvolva, as pessoas devem dar a outras poder sobre si mesmas. A cessão de poder é uma coisa inerentemente arriscada de se fazer e, ao longo do último milênio, desenvolveu-se um sistema cuja finalidade é proteger o indivíduo que este entrega poderes a outrem: transparência, supervisão e prestação de contas. Ou seja, nas palavras de SCHNEIER⁸⁷: *“If we know how people are using the power we give them, if we can assure ourselves that they’re not abusing it, and if we can punish them if they do, then we can more safely entrust them with power. This is the fundamental social contract of democracy”*.

CRUZ⁸⁸ enfatiza que um dos mais importantes fenômenos da vida social é, de fato, o Poder. Pode-se dizer que praticamente não existe uma relação social em que a influência voluntária de uma pessoa ou grupo de pessoas sobre outra ou outros não esteja presente de alguma forma, “possui Poder ou aqueles que conseguem que os outros, pelo exercício deste Poder, façam o que ele quer. É dizer daquele que é capaz de impor aos demais uma definição de metas e um modelo de organização”.

O Jurista é também bastante assertivo ao discorrer que uma Sociedade tecnologicamente avançada exige soluções rápidas aos conflitos sociais. A falha do Direito em entregar tais soluções pode ensejar um fenômeno

⁸⁶ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**.

⁸⁷ SCHNEIER, Bruce. **Data and Goliath: the hidden battles to collect your data and control your world**. p. 189.

⁸⁸ CRUZ, Paulo Márcio. **Política, poder, ideologia e estado contemporâneo** p. 60

chamado *overshoot*, termo que significa o atraso ou a impossibilidade de resolver um conflito anteriormente ao ponto a partir do qual não haveria mais volta⁸⁹.

Ainda considerando os ensinamentos de CRUZ, “estes recursos ou esferas de atividade, controlados por grupos políticos ou econômicos, permitem o exercício de um Poder social suficiente para comandar indivíduos e números grupos, fazendo-os obedecer às suas decisões para que não tenham prejuízos, ou porque acreditam que devem fazê-lo, ou mesmo pela expectativa de obter alguma coisa em troca”⁹⁰.

Considerando o acima exposto, mister reforçar o papel da Ciência Jurídica na sistematização, disseminação, controle, revisão e segurança na produção do conhecimento moral, ético e jurídico, em especial as limitações ao uso da força e das ações arbitrárias, favorecendo, dessa forma, a previsibilidade⁹¹.

É uma verdade universal o conceito de que “informação é poder”. Através da junção de informações disponíveis, é possível exercer controle sobre indivíduos, grupos de pessoas e até mesmo sobre nações inteiras.

Na Era da Informação, houve um rápido crescimento na quantidade e na qualidade das informações que se consegue reunião em razão da facilidade de acesso aos dados, amplamente espalhados – e compartilhados – na internet.

Além do mais, a difusão de aparelhos digitais tais como *smartphones* contribuiu para a aceleração dos impactos sociais e econômicos decorrentes das tecnologias digitais, impactos esses tanto positivos, quanto negativos. Muitas das técnicas utilizadas por essas empresas, desde ter cada interação com o mundo digital gravada, analisada e comercializada, até a oferta de anúncios personalizados e constantemente pontuados e marcados por algoritmos, têm se tornado parte da prática cotidiana dessa indústria, mesmo sem

⁸⁹ CRUZ, Paulo. Paulo Márcio. **Política, poder, ideologia e estado contemporâneo** p. 61

⁹⁰ CRUZ, Paulo. Paulo Márcio. **Política, poder, ideologia e estado contemporâneo** p. 61

⁹¹ ZANON JUNIOR, Orlando Luiz. **Teoria Complexa do Direito**. 2 ed. Prismas: Curitiba, 2015. p. 51

que os usuários e a sociedade em geral sejam consultados e estejam de acordo com referida prática.

Outro problema decorrente da coleta massiva de dados pessoais refere-se à vigilância, não somente estatal, como também privada, muitas vezes exercida em forma de parceria público-privada, o que reforça os riscos da vigilância, por meio da pulverização das informações coletadas.

Em artigo publicado na revista *The Guardian*⁹², intitulado “*What does the panopticon mean in the age of digital surveillance?*”, o jornalista Thomas McMullan inicia sua narrativa expondo que o filósofo inglês Jeremy Bentham solicitou em seu testamento que, quando de sua morte, seu corpo fosse dissecado e posto em exibição pública. Vontade atendida, seu corpo, agora, fica em uma caixa de vidro na University College London, sentando em um banco de madeira, encarando os alunos de dentro de sua caixa de vidro. Seu cadáver contém uma webcam que grava o movimento de seus espectadores e os transmite ao vivo online, como parte do programa da Universidade denominado PanoptiCam, que testa, entre outras coisas, algoritmos de vigilância, cujo objetivo principal é o de aprender a melhor forma de identificar e contar diferentes pessoas em imagens fixas, com precisão.

Na obra de BENTHAM⁹³, o panóptico é descrito como uma edificação constituída de uma torre central rodeada por celas. Na torre central fica o vigia. Nas celas, encontram-se os prisioneiros – ou trabalhadores, crianças, a depender do objetivo da edificação. Da torre, brilha uma luz para que o vigia consiga enxergar todos nas celas e para que os indivíduos nas celas, ao contrário, não consigam enxergar o vigia, e, portanto, presumam que estão sendo observados a todo o tempo.

⁹² McMULLAN, Thomas. **What does the panopticon mean in the age of digital surveillance?** Disponível em: < <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham>>. Acesso em: 15/04/2020.

⁹³ BENTHAM, Jeremy; MILLER, Jacques-Alain; PERROT, Michelle; WERRETT, Simon. **O panóptico**. Org: Tomaz Tadeu. Traduções: Guacira Lopes Louro, M.D. Magno e Tomaz Tadeu. 3. ed. Belo Horizonte: Autêntica Editora, 2019.

O princípio é a inspeção central. Em seu livro *Vigiar e Punir*⁹⁴, Michel Foucault usou o Panóptico de Bentham como uma maneira de ilustrar como as sociedades disciplinadoras subjugam seus cidadãos. Ele descreve o prisioneiro de um panoptico como sendo o recebedor final de uma vigilância assimétrica: “ele é visto, mas não vê; ele é um objeto de informação, nunca um sujeito em comunicação”. Como consequência, o prisioneiro se autopolícia por medo da punição.

De diversas formas, a torre de vigilância no coração do panóptico é precursora das câmeras instaladas nos edifícios atuais, equipamentos propositalmente visíveis aos olhos humanos.

O paralelo entre o panóptico e a CCTV pode ser óbvio, mas o que acontece quando se o mundo da vigilância digital e da captura de dados? O jornalista questiona se ainda somos os “objetos da informação” ao trocarmos de “celas” nas telas de nossos smartphones? Ponto relevante neste paralelo é que, ao contrário do Panóptico, os indivíduos não sabem que estão sendo observados.

Jake Goldenfein, pesquisador da Universidade de Melbourne, adverte que é importante lembrar o propósito corretivo do panóptico de Bentham ao considera-lo uma metáfora com a vigilância moderna: “o fato de não sabermos que estamos sendo observados significa que estamos sendo “normalizados” da mesma forma que o panóptico foi concebido para corrigir comportamentos?”

Os questionamentos como os feitos acima invocam o princípio da precaução, emprestado dos riscos ambientais, para sua aplicação na tecnologia, pois, é importante enfatizar, a Internet e as aplicações de Inteligência Artificial estão apenas em sua infância e ainda não é possível mensurar o seu alcance.

⁹⁴ FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Título original: *Surveiller et Punir: Naissance de la prison*. Tradução: Pedro Elói Duarte. Lisboa: Edições Almedina, 1975. (Versão Kindle),

1.3.4 A proteção de dados pessoais: um novo direito fundamental?

De acordo com MENDES⁹⁵, no âmbito internacional, o direito à privacidade transformou-se para fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados. A transformação desse conceito pode ser percebida de forma mais clara a partir da década de 70, com a edição de legislações específicas e de decisões judiciais de diversos países, bem como a partir da aprovação de acordos internacionais e transnacionais em diferentes níveis. Todos esses instrumentos compartilham conceito segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela jurídica.

Na evolução do conceito de privacidade, importante destacar a decisão do Tribunal Constitucional alemão, no julgamento da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho” de 25 de março de 1982, que é considerada um paradigma no tratamento da proteção de dados. Nesse julgamento histórico, o Tribunal foi radical ao estabelecer o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade e decidiu pela inconstitucionalidade parcial da referida lei.

A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou um marco para a teoria da proteção de dados pessoais e para as subseqüentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais se baseia em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado⁹⁶.

⁹⁵ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. Saraiva: São Paulo, 2014. (Posição 510)

⁹⁶ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. (Posição 543)

A disciplina da proteção de dados pessoais emerge no âmbito da Sociedade da Informação, como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados *per se*, mas a pessoa que é titular desses dados⁹⁷.

Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade.

Assim, a proteção de dados pessoais pode ser compreendida como uma dimensão do direito à privacidade, que, por consequência, partilha dos mesmos fundamentos: a tutela da personalidade e da dignidade do indivíduo.

The legal community argued that pure self-regulation did not make sense in the area of data protection because of the great economic drive to exchange information. With the increasing sharing of governance responsibilities between public and private bodies, the traditional state-society boundaries had broken down. An unregulated private sector could provide a dangerous data warehouse for bureaucracies; the concentration of information in the hands of a few large corporations threatened to ossify power within society. The specter of large multinational corporations transferring personal information across borders further raised the stakes of uncontrolled private-sector data processing⁹⁸.

Nesse passo, a privacidade, antes compreendida, prioritariamente, como o direito de ser deixado em paz (*right to be let alone*), passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular. Ademais, conforme aponta MENDES⁹⁹, a disciplina da proteção de dados pessoais passa a envolver uma

⁹⁷ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. (Posição 559)

⁹⁸ NEWMAN, Abraham L. **Protectors of privacy: regulating personal data in the global economy**. Ithaca: Cornell University Press, 2008. p. 65

⁹⁹ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. (Posição 614)

outra questão, anteriormente ignorada: o problema da igualdade. A igualdade se apresenta como um tema para essa disciplina, na medida em que a vigilância realizada por organismos privados ou estatais, a partir de informações obtidas em bancos de dados, pode acarretar a seleção e a classificação dos indivíduos (*prática discriminatória*), de modo a afetar expressivamente as suas oportunidades de vida na sociedade.

Contudo, ao se tratar de definir uma legislação que imponha limites à coleta de dados e especialmente à vigilância estatal e corporativa, é necessário fazer uma ressalva e enfatizar que a sociedade como um todo se beneficia enormemente da coleta e uso de dados. A coleta de dados proporciona benefícios e conveniências que eram impossíveis antes do advento das novas tecnologias.

O Direito deve estar atento ao seu papel nesse contexto para, de um lado, não impor obstáculos excessivos que atravanquem o desenvolvimento econômico e tecnológico, como ocorrido na China nos séculos passados, e, por outro, coibir abusos e proteger os direitos constitucionalmente vigentes.

Faz-se necessário, portanto, analisar o cenário brasileiro para identificar se a legislação nacional está adequada aos novos desafios introduzidos pela tecnologia, especialmente no que se refere à coleta e tratamento de dados pessoais.

Capítulo 2

O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NO ÂMBITO DO PODER PÚBLICO

2.1 A POSITIVAÇÃO DAS REGRAS INERENTES AO TRATAMENTO E À PROTEÇÃO DE DADOS PESSOAIS.

Conforme restou demonstrado na parte inicial deste trabalho, o direito à proteção de dados pessoais surge como um novo direito autônomo, de grande relevância no contexto da Sociedade da Informação, haja vista a exposição e fragilidade dos indivíduos frente à evolução tecnológica que desafia o Direito na busca pela inovação de seus institutos.

Nesse contexto, as atividades e serviços que, de qualquer forma e por qualquer meio, utilizam dados pessoais estão sendo diretamente impactados por políticas de proteção à vida privada, à intimidade e ao livre desenvolvimento da personalidade humana, tais como a regulamentação advinda da Lei Geral de Proteção de Dados Pessoais.

No ponto e em análise ao que foi tratado no capítulo anterior, não há como negar que as discussões ocorridas ao longo do último século no que se refere à privacidade e ao correlato direito à proteção de dados pessoais são, em sua base, inegavelmente de cunho ético e moral: “o que é privacidade?”, “o que é vida íntima?”, “de que forma o ser humano se desenvolve sob vigilância?”, “o Estado tem o direito de vigiar a vida privada? Quais os limites?”, “estou disposto a disponibilizar meus dados pessoais em troca de serviços e praticidades? Em quais riscos estou incorrendo?”, “a utilização de dados pessoais como insumos para negócios milionários, à revelia do titular desses dados, deve ser tratada com fundamento na ética e na moralidade?”.

De forma sintética, os horrores da segunda grande guerra e os escândalos de espionagem, juntamente com a mercantilização da vida íntima dos indivíduos, são fatos sociais que invariavelmente levantaram questões sobre os anseios da Sociedade em termos de preservação da intimidade na consecução

do princípio da dignidade da pessoa humana, norteador de diversas constituições, notadamente a brasileira.

Todavia, em que pese a existência de princípios constitucionais que abarcam o direito à privacidade, bem como referência à proteção de dados em legislação infraconstitucional, tais como o Marco Civil da Internet, o Código de Defesa do Consumidor e a Lei do Cadastro Positivo, só para citar alguns, a ausência de um texto normativo formal, capaz de condensar um conjunto sistemático de regras para o tratamento e a proteção de dados pessoais, dificultam a realização desse direito, cuja aplicabilidade fica praticamente à dependência da interpretação judicial, o que acaba por gerar insegurança jurídica tanto aos titulares dos dados, quanto aos agentes de tratamento.

Foi nesse contexto, impulsionado pela edição do General Data Protection Regulation – GDPR, o regulamento europeu sobre a proteção de dados pessoais, que prevê condições para o compartilhamento transnacional e a transferência internacional de dados, condições estas capazes de afetar as relações comerciais com o bloco europeu, e pressionado pela sociedade civil, que se viu necessidade de se editar uma lei prevendo as regras para o tratamento de dados pessoais no Brasil.

Para uma melhor compreensão sobre como o conjunto de regras para o tratamento de proteção de dados adentrou o ordenamento jurídico brasileiro, precipuamente *code based* e de natureza majoritariamente positivista, teceremos breves comentários acerca da “normatização” de tais regras.

No ponto, ZANON¹⁰⁰ destaca três formas de produção jurídica: a positivação, da qual resultam os Textos Normativos, ou seja, a Legislação; a Aplicação Judicial, da qual resulta a Norma Jurídica e, por conseguinte, a Jurisprudência; e a Programação Governamental, que gera as Políticas Executivas.

¹⁰⁰ ZANON, Orlando Luiz Júnior. **Rediscutindo a teoria das fontes jurídicas**. Direito, democracia e constitucionalismo [recurso eletrônico] / Adriane Guasque ... [et al.]; organizadores, Francisco José Rodrigues de Oliveira Neto, Pedro Manoel Abreu, Orlando Luiz Zanon Júnior ; coordenadores, Maria Chiara Locchi, Maurizio Oliviero, Rafael Padilha dos Santos. - Itajaí: UNIVALI, 2017. – (Coleção principiologia constitucional e política do direito; t. 3). p. 242

ZANON¹⁰¹ descreve, ainda, as diferenças entre fontes jurídicas materiais e formais. O autor conceitua as fontes jurídicas materiais como sendo o conteúdo capaz de influenciar a tomada de decisões pelas pessoas em Sociedade e refletem a base sobre a qual é constituído o Ordenamento Jurídico. Por não terem passado pelo processo de produção estatal, o seu grau de eficácia é limitado, uma vez que dependem de uma análise antropológica ou sociológica para identificar limites e compreensão, sendo que os princípios éticos fazem parte das fontes jurídicas materiais.

Já as fontes jurídicas formais são aquelas decorrentes dos poderes estatais, por meio da positivação pelo Poder Legislativo, da aplicação pelo Poder Judiciário ou da programação pelo Poder Executivo, de modo a ampliar o grau de segurança jurídica, atingindo as forças decisiva, vinculante ou, mesmo, intransponível.

No que concerne à LGPD, vislumbra-se se tratar de Texto Normativo oriundo da positivação dos anseios da Sociedade diante dos impactos decorrentes da tecnologia e do uso de informações pessoais no âmbito da já referenciada Sociedade da Informação.

A LGPD é, portanto, fonte jurídica formal, na modalidade texto normativo, que incorporou em seu conteúdo, além das regras dispositivas, os princípios éticos, decorrentes de discussões públicas concernentes à temática de proteção de dados, e os fundamentos que deverão ser obrigatoriamente observados por todas *“as autoridades políticas (gestores públicos e juízes) e pessoas jurídicas e físicas com operações decisórias dentro da área abrangida pelo Estado, consoante a premissa máxima da submissão de todos à lei, basilar nas Sociedades democráticas modernas”*¹⁰².

¹⁰¹ ZANON, Orlando Luiz Júnior. **Formas jurídicas**. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), 8(3):303-317, setembro-dezembro 2016 – UNISINOS. p. 309

¹⁰² ZANON, Orlando Luiz Júnior. **Formas jurídicas**. p. 310

Nesta toada, o que se deflagra, pois, da positivação do direito à proteção de dados pessoais é a estreita correlação entre Fato e Direito, sendo o texto normativo em questão um produto dos fatos sociais.

Conforme assevera LAFER¹⁰³, a correlação entre Fato e Direito leva ao entendimento do Direito como um sistema aberto, dependente de outros que o abrangem e circunscrevem e leva à pergunta: “*Para que serve o Direito?*”

E continua:

Esta necessidade de encarar o Direito como um sistema aberto e, portanto, de desenvolver o campo da Filosofia do Direito encarada na perspectiva do ângulo externo tem também merecido destaque especial dos juristas com interesses filosóficos, por força de uma significativa metamorfose das funções do Direito Positivo e dos problemas práticos suscitados por estas metamorfoses. Como é sabido, o Direito contemporâneo não mais corresponde à concepção que dele fazia a Dogmática Jurídica tradicional. Com efeito, e como aponta Norberto Bobbio, o Direito Positivo contemporâneo deixou de ser apenas um instrumento de controle social *stricto sensu*, cumprindo funções predominantemente protetivas de interesses e preservadoras da ordem, tendo em verdade se convertido num instrumento de direção social. É um direito que, *ratione materiae*, não se ocupa apenas em proibir comportamentos por meio do Direito Penal, ou permitir comportamentos através da autonomia da vontade do Direito Privado. Trata-se de um Direito Promocional, que se interessa por comportamentos tidos como desejáveis e, por isso, não se circunscreve a proibir ou permitir, mas almeja estimular ou desestimular comportamentos através de medidas diretas ou indiretas. Um Direito deste tipo, que corresponde a novas funções de gestão da sociedade, exercidas pelo Estado, não pode, evidentemente, restringir-se ao tema da validade formal, mas requer, para uma apropriada consideração do princípio da efetividade, a análise da conduta dos destinatários das normas¹⁰⁴.

Seguindo o paradigma introduzido pela evolução tecnológica, o texto normativo relaciona as condutas aceitáveis e descreve as penalidades para aquelas reprováveis no atual contexto social no que concerne o tratamento de dados pessoais.

¹⁰³ LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hanna Arendt. São Paulo: Companhia das Letras, 1988. 406 páginas

¹⁰⁴ LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hanna Arendt. p. 59-60.

Imperioso enfatizar o posicionamento de BOBBIO¹⁰⁵ em relação às tarefas da sociologia do Direito, consubstanciadas na investigação da função do direito na mudança social e na análise da aplicação das normas jurídicas numa determinada sociedade, da aplicação das normas dos Estados particulares, ou do sistema internacional em seu conjunto, sendo que ambas as tarefas se dão na esfera do ordenamento jurídico que compreende o reconhecimento e a proteção dos direitos do homem.

BARROSO¹⁰⁶ destaca que:

O Estado ainda é a grande instituição do mundo moderno. Mesmo quando se fala em centralidade dos direitos fundamentais, o que está em questão são os deveres de abstenção ou de atuação promocional do Poder Público. Superados os preconceitos liberais, a doutrina publicista reconhece o papel indispensável do Estado na entrega de prestações positivas e na proteção diante da atuação abusiva dos particulares. [...]. O Estado é formado pela sociedade e deve perseguir os valores que ela aponta.

Feita, portanto, esta breve introdução, passaremos a analisar os aspectos da Lei Geral de Proteção de Dados que se entrelaçam e deverão ser observados pelo Poder Judiciário, na qualidade de agente de tratamento, tanto na posição de “Controlador”, quanto de “Processador”.

Antes de continuar, contudo, será necessário fazer uma ressalva. A LGPD foi publicada em 15 de agosto de 2018 e estava prevista para entrar em vigor no dia 15 de agosto de 2020, com exceção da Seção I, que trata da Autoridade Nacional de Proteção de Dados, vigente desde 25 de dezembro de 2018. Porém, em 29 de abril de 2020, o Presidente da República editou a Medida Provisória nº 959, a qual, dentre outras disposições, prorrogou a *vacatio legis* para 03 de maio de 2021¹⁰⁷.

A prorrogação tratada na Medida Provisória acima indicada já era tema de discussão no Congresso Nacional, com pedidos de adiamento para até 2022. Entretanto, em virtude da Pandemia Covid-19, a MP prorrogando o prazo foi publicada. Entendo haver, pelo menos, duas hipóteses para a confirmação dessa

¹⁰⁵ BOBBIO, Norberto. **A era dos direitos**. Versão Kindle. Posição 1501

¹⁰⁶ BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo**. São Paulo: Saraiva, 2010. 2ª Ed. p. 88-89

¹⁰⁷

prorrogação: a uma, considerando que os esforços públicos e privados devem ser direcionados ao enfrentamento da Pandemia e a LGPD é uma lei complexa que exige investimentos e conhecimentos técnicos especializados para a sua correta implementação e *compliance*, tanto na esfera pública como na privada, a prorrogação foi a coisa sensata a se fazer; ou, a duas, a vigência da LGPD representaria, no mínimo, uma barreira legal à coleta e utilização de dados pessoais, notadamente em relação à geolocalização dos cidadãos¹⁰⁸, por meio do monitoramento de dados celulares, prática que já vem sendo utilizada em países como a China, Coréia do Sul e Singapura no controle da contaminação por Covid-19. Países membros da União Europeia estão desenvolvendo aplicativos de geolocalização, enquanto o Departamento de Proteção de Dados da União Europeia está trabalhando nas diretrizes de impacto à Privacidade, em consonância com o disposto no Regulamento de Proteção de Dados Europeu.

Os próximos movimentos da Administração Pública possibilitarão as respostas.

2.2 ASPECTOS DESTACADOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Tratando-se o presente trabalho de um estudo analítico sobre a LGPD e suas implicações no tratamento de dados pessoais pelo Poder Judiciário no âmbito do processo judicial, passa-se, então, a destacar os preceitos legislativos cuja compreensão se torna necessária para que se possa atingir o objetivo desta pesquisa.

2.2.1 Conceitos importantes

Alicerçado em Aristóteles e Cícero, PASOLD¹⁰⁹ destaca que, para que uma comunicação seja eficaz e eficiente para aqueles nela envolvidos, será necessário estabelecer um acordo semântico entre si, por meio da compreensão mútua dos significados para as palavras e expressões utilizadas.

¹⁰⁹ PASOLD, Cesar Luiz. **Prática da pesquisa jurídica**. P. 27.

Em respeito à finalidade da Ciência Jurídica, PASOLD¹¹⁰ propõe a denominação de Categoria para identificar *“a palavra ou expressão estratégica à elaboração e/ou à expressão de uma idéia”*.

A LGPD traz em seu bojo importantes categorias que serão descritas na sequência, cujos conceitos são transcrições literais do próprio texto normativo, previstos no art. 5º da referida Lei, com a finalidade de garantir o acordo semântico necessário para a correta compreensão dos aspectos que serão abordados neste capítulo da pesquisa.

- a) **Dado pessoal:** informação relacionada à pessoa natural identificada ou identificável;
- b) **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado à uma pessoa natural;
- c) **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- d) **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- e) **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- f) **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

¹¹⁰ PASOLD, Cesar Luiz. **Prática da pesquisa jurídica**. p. 31.

- g) **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- h) **Agentes de tratamento:** o controlador e o operador;
- i) **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- j) **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- k) **Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Além das categorias acima descritas, o artigo 5º da LGPD anteriormente mencionado traz outras definições, as quais, para a finalidade da pesquisa, entende-se não haver relevância para serem destacadas neste momento.

2.2.2 Objetivos e âmbito de aplicação material e territorial

Passa-se, agora, a analisar os aspectos da Lei Geral de Proteção de Dados que se entrelaçam e deverão ser observados pelo Poder Judiciário, na qualidade de pessoa jurídica de direito público, tanto na posição de “Controlador”, quanto de “Processador”.

O primeiro destaque que deve ser feito refere-se ao escopo material da Lei Geral de Proteção de Dados. Como se observa do texto contido em seu artigo 1º¹¹¹, a LGPD trata unicamente sobre o tratamento de dados *personais*.

Outra questão que deve ser mencionada é que, apesar de a referida lei ter sido idealizada com foco nos meios digitais, consigna-se que seu alcance não se limita a eles, ou seja, a Lei também é aplicável ao tratamento de dados pessoais em ambiente físico. Nesse ponto, deve-se levar em consideração técnicas *off-line*, tais como o *dumpster diving*¹¹² e o *shoulder surfing*¹¹³, comumente utilizadas e que não dependem de qualquer sistema de informação. Aqui, vale, também, destacar os dados armazenados em arquivo físico como processos judiciais, que merecem tanta atenção quanto quaisquer registros digitais.

Ademais, a LGPD se aplica a pessoas físicas e jurídicas tanto de direito público, como de direito privado, que efetuem qualquer uma das operações consideradas como tratamento de dados pessoais. Note-se que é já no artigo 1º da Lei que se infere a sua aplicação ao Poder Judiciário, na qualidade de pessoa jurídica de direito público¹¹⁴.

A parte final do art. 1º dispõe sobre objetivo específico da lei, que é a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

¹¹¹ Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

¹¹² Técnica que consiste em vasculhar o lixo em busca de informações.

¹¹³ Denominação da técnica que consiste em “dar aquela olhadinha” por cima do ombro para ver a tela ou teclado do computador para obter senhas e outras informações.

¹¹⁴ Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei

De fato, como visto no Capítulo 1, e reforçado por VANZOIFF¹¹⁵, essa preocupação de tutelar de forma mais específica referidos direitos fundamentais tornou-se ainda mais necessária com a evolução da informática e das telecomunicações, e, especialmente após 1970, com o advento dos computadores, quando houve um incremento no uso de processamento de dados. Nota-se que esse período coincidiu com a formação de blocos econômicos regionais, que estimulou o compartilhamento de dados pessoais em grandes quantidades e em escala internacional.

Esse cenário revelou um aumento de produtividade e eficiência de empresas e governos e, por outro lado, também fez crescer a preocupação com a proteção da privacidade de indivíduos, sobretudo diante do fluxo transfronteiriço de dados. Por isso surgiram leis de proteção da privacidade do indivíduo, relativamente ao tratamento de seus dados pessoais, alinhadas com o sentimento de equilíbrio entre a proteção das liberdades individuais e a preservação de um fluxo aberto de dados pessoais capaz de sustentar o livre comércio internacional¹¹⁶.

Conforme se observou a partir da evolução do direito à privacidade e de proteção aos dados pessoais, tratados no primeiro capítulo, os postulados regulatórios em torno da questão revelam muito do desenvolvimento humano em torno do próprio conceito de privacidade, estimulando e permitindo um juízo de ponderação, baseado em parâmetros como necessidade e proporcionalidade, para modelar e contrabalançar o interesse privado e o interesse público, estabelecendo a possibilidade de ingerência do Estado sobre direitos fundamentais e liberdades civis, de forma a limita-los.

Há, contudo, de se fazer a ressalva de que premissa para ingerência do Estado sobre tais direitos é única, conforme assevera VANZOIFF¹¹⁷: “não

¹¹⁵ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. **LGPD: Lei Geral de Proteção de Dados**. p. 20

¹¹⁶ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 20

¹¹⁷ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 23

existem direitos absolutos, mas qualquer limitação a direitos fundamentais deve ocorrer de forma moderada, necessária e proporcional”.

Assim, a LGPD busca a proteção de direitos e garantias fundamentais da pessoa natural, de modo a mitigar riscos e estabelecer regras definidas sobre o tratamento de dados pessoais.

É de grande relevância, também, a informação constante no parágrafo único do artigo 1º, ao descrever que as normas gerais contidas na referida lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios, superando, portanto, qualquer dúvida sobre seu âmbito de aplicação.

O caput do art. 3º da LGPD dispõe sobre a sua aplicação material, deixando claro que não se importa com o tipo de tecnologia empregada para a realização do tratamento, se por meio digital ou analógico, com o uso de inteligência artificial, de forma automatizada ou manualmente. Assim, aplica-se a LGPD para dados existentes em papel, no histórico de uma clínica hospitalar, na memória do computador de uma instituição financeira que armazena os dados bancários de seu cliente; em uma fita guardada pelo departamento de atendimento ao cliente de um agente de viagens; ou em imagens gravadas em circuito fechado de TV, por exemplo.

No que se refere à aplicação da LGPD às pessoas jurídicas de direito privado, importa esclarecer que são aquelas estabelecidas no Código Civil, conforme seu art. 44¹¹⁸. Não importa para a LGPD o objetivo pelo qual tais entidades foram constituídas, se com foco principal e finalidade o tratamento de dados ou se o tratamento é só uma forma de apoio para a atividade principal, com fins lucrativos ou filantrópicos. A partir do momento em que a pessoa jurídica

¹¹⁸ Art. 44. São pessoas jurídicas de direito privado:

I - as associações;

II - as sociedades;

III - as fundações.

IV – as organizações religiosas;

V - os partidos políticos.

VI - as empresas individuais de responsabilidade limitada.

adquire personalidade jurídica, estará apta a responder por seus atos, incluindo o cumprimento da LGPD, quando tratar dados pessoais e não se enquadrar em alguma das exceções previstas no texto normativo.

Impende ressaltar que a LGPD também se aplica à pessoa natural, sempre que o tratamento de dados realizado guarde relação com alguma atividade profissional ou comercial, ou seja, que caracterize finalidade econômica.

De acordo com VANZOIFF¹¹⁹ e conforme prevê a lei, a aplicação da LGPD também independe do país da sede ou do país da localização dos dados tratados, ampliando, assim, de forma considerável, a sua jurisdição, instituto formulado tradicionalmente com base em sociedade com fronteiras territoriais geográficas e físicas bem delimitadas.

Acerca das hipóteses de aplicabilidade territorial e extraterritorial, que serão analisadas adiante, registra-se que são independentes entre si, de modo que bastará a presença de somente uma delas para que a LGPD tenha efeito sobre o responsável pelo tratamento, seja ele o controlador, pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais, seja o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Para aplicação da jurisdição, o espaço físico em que a operação de tratamento ocorre é o primeiro ponto fulcral, pois as fronteiras físicas correspondem aos limites de soberania das nações.¹²⁰

A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou estivessem no Brasil. Desse

¹¹⁹ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 53

¹²⁰ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 57

modo, o dado pessoal tratado por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD.

2.2.3 Fundamentos

Os fundamentos da LGPD, estabelecidos no art. 2º¹²¹ da Lei, buscam, basicamente, um equilíbrio na manutenção do desenvolvimento econômico e tecnológico de modelos de negócios inovadores, dos quais a Sociedade contemporânea se vale para garantir seu progresso e eficiência, tanto públicos como privados, com a inviolabilidade de direitos constitucionais dos cidadãos.

Segundo os ensinamentos de KANT¹²², em toda a legislação há dois elementos: uma lei e um motivo. A primeira representa a ação necessária que precisa ser realizada, fazendo da ação um dever, através de regras práticas. O segundo é o fundamento para a determinação das escolhas. Para o filósofo, a legislação que faz de uma ação um dever e faz deste dever o motivo, é uma legislação ética. Este dever, por sua vez, tem que ser extraído de fundamentos determinantes.

Os fundamentos sobre os quais a LGPD deverá ser compreendida e que decorrem dos fatos sociais aludidos anteriormente, consubstanciam as razões de ser da legislação, conferindo a ética descrita por KANT ao texto normativo.

No que concerne à diferença entre os conceitos de objetivos e fundamentos, vale trazer a definição de BASTOS¹²³, para quem “a ideia de

¹²¹ Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

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.

¹²² KANT, Immanuel. **A metafísica dos costumes**. 3ª ed. São Paulo: Edipro, 2017. p. 71-72

¹²³ BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 20. ed. atual. São Paulo: Saraiva, 1999. p. 159-160.

objetivos não pode ser confundida com a de fundamentos, muito embora, algumas vezes, isto possa ocorrer. Os fundamentos são inerentes ao Estado, fazem parte de sua estrutura. Quanto aos objetivos, estes consistem em algo exterior que deve ser perseguido.”

Para COMPARATO¹²⁴, o termo fundamento “designa o que serve de base ao ser, ao conhecer, ou ao decidir. Fundamento é, pois, a causa ou razão de algo (*ratio essenci, ratio cognoscendi, ratio decidiendi*)”.

A seguir serão abordados cada um dos fundamentos dispostos no art. 2º da LGPD, que deverão ser observados por todos aqueles que realizarem ou forem objeto de tratamento de dados pessoais.

2.2.3.1 O respeito à privacidade

Como amplamente discutido no Capítulo 1, as sociedades civilizadas perceberam que a proteção da privacidade é elemento indissociável da dignidade da pessoa, razão pela qual qualquer ato capaz de afetar a intimidade do cidadão seria também um ato atentatório à experiência humana de uma vida digna.

Tanto é assim que, em nosso ordenamento jurídico, o direito à privacidade está disposto em nossa Carta Magna como um direito fundamental¹²⁵, ao estabelecer que é inviolável a intimidade e a vida privada, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

A inviolabilidade de dados, independentemente do sigilo da correspondência, comunicações telegráficas e telefônicas, também está presente na CRFB, em seu art. 5º, inc. XII, e foi consolidado pelo entendimento do Supremo Tribunal Federal¹²⁶, embora a Suprema Corte, em julgado posterior¹²⁷,

¹²⁴ COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010, p. 41

¹²⁵ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

¹²⁶ BRASIL, **Supremo Tribunal Federal**. Ação Penal n. 307-3/DF. Relator: Min. Ilmar Galvão. Brasília, 1994. Diário da Justiça, Brasília, 13 dez. 1994.

¹²⁷ Brasil, **Supremo Tribunal Federal**. Recurso Extraordinário n. 418.416/SC. Relator: Min. Sepúlveda Pertence, por maioria, Brasília, 2006. Diário da Justiça, Brasília, 10 mai. 2006.

tenha consignado que a proteção existente na Constituição é na comunicação de dados, e não da informação pessoal propriamente dita. Conforme entendimento de FERRAZ JÚNIOR¹²⁸:

[...] a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc., condicionam o intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido.

Por essa razão, conforme expõe VANZOIFF¹²⁹, o que alguém faz ou pode fazer com dados pessoais de terceiros, no sentido de o próprio titular ter o direito de determinar quais predicados dele mesmo poderão ser utilizados por outros, passou a ser objeto de proteção em novos regimes jurídicos, deflagrando, certamente, a privacidade como fundamento da LGPD.

2.2.3.2 A autodeterminação informativa

Considerando o cenário atual da Sociedade da Informação, pensar que o cidadão possa ter o controle sobre seus próprios dados parece utopia. Porém, a autodeterminação informativa se apresenta como fundamento da LGPD, justamente nesse momento em que ainda predomina uma coleta e tratamento massivo e desenfreado de dados, com o objetivo de devolver ao titular o poder sobre o fluxo e o uso de seus próprios dados, mediante o estabelecimento de determinações objetivas aos agentes de tratamento.

De acordo com VANZOIFF¹³⁰:

a autodeterminação informativa, que é o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção

¹²⁸ FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados**: o direito à privacidade e os limites da função fiscalizadora do Estado. In: PIZOLIO, Reinaldo; GALVADÃO JÚNIOR, Jayr Viégas. **Sigilo fiscal e bancário**. São Paulo: Quartier Latin, 2005. p. 28.

¹²⁹ VANZOIFF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 26

¹³⁰ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 27

(proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular.

Nas palavras de RODOTÀ¹³¹, a autodeterminação informativa é um *“poder permanente de controle sobre seus próprios dados”*.

De acordo com CANOTILHO¹³², o direito à autodeterminação informacional ganha hoje dimensões particularmente significativas e leciona:

Por um lado, a doutrina tenta delimitar os contornos de um direito geral à autodeterminação informacional que se reconduz ao direito de o cidadão decidir, autónoma e livremente, quando e dentro de que limites, os dados de sua vida pessoal são susceptíveis de informatização ou publicidade. Por outro lado, a criação e conservação de memórias informatizadas é hoje cada vez mais frequente, por parte de entidades públicas e privadas. No caso referido, o direito à autodeterminação configura-se como um direito de defesa perante os <<Serviços Secretos do Estado>> e como um direito à proteção jurídica. Em que termos? A nível procedimental, o cidadão deve ter um procedimento para se dirigir a uma entidade competente (<<Comissão Nacional de Informática>>, <<Provedor de Informática>> e <<Autoridade Nacional do Habeas Data>>) no sentido de exigir que sejam rectificados, completados, clarificados, actualizados, os dados inexactos, incompletos, equívocos ou ultrapassados, ou que sejam eliminados do registro todos os dados cuja obtenção, comunicação ou conservação é interdita nos termos constitucionais. A nível processual, pode e deve construir-se uma acção Habeas Data perante um Tribunal, destinada a permitir que um cidadão obtenha a proteção do direito à proteção da autodeterminação informacional, caso não tenha obtido qualquer resultado através de um procedimento administrativo.

Assim, a corroborar o entendimento acima, vale-se do referencial teórico de WESTIN¹³³, para quem a privacidade deveria ser compreendida como a *“reinvindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros”*, conferindo o carácter de liberdade individual, consubstanciada na autodeterminação de assuntos privados. O autor vai além e

¹³¹ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

¹³² CANOTILHO, José Joaquim Gomes. **Estudos sobre direitos fundamentais**. 2ª Ed. Coimbra Editora, 2008. p. 84.

¹³³ WESTIN, Alan F. **Privacy and Freedom**. New York: IG Publishing, 1967. (ebook) p. 24: *“the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”*.

conceitua privacidade o direito de um indivíduo se retirar, voluntária e temporariamente, da Sociedade em geral, por meios físicos ou psicológicos, a um estado de solitude plena, ou à intimidade de pequenos grupos, e, quando em grupos maiores, à condição de anonimato ou espaço reservado, e faz a ressalva, de que o desejo pela privacidade não é absoluto, uma vez que participar da Sociedade é, da mesma forma, um desejo poderoso do indivíduo.

Dessa forma, a autodeterminação informativa pode ser considerada como o protagonismo do indivíduo na proteção dos seus dados pessoais, em que as normas de proteção de dados pessoais inferem a participação do titular sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento¹³⁴.

2.2.3.3 A liberdade de expressão, de informação, de comunicação e de opinião

DWORKIN¹³⁵ leciona que a liberdade de expressão do pensamento é vital e integra o próprio desenvolvimento humano, de tal forma que a manutenção desse fundamental direito garante a autodeterminação dos indivíduos.

Em artigo sobre o romance futurístico e distópico *Fahrenheit 451*, escrito por Ray Bradbury em 1953, e sua correlação com a teoria jurídica advinda da Primeira Emenda à Constituição dos Estados Unidos, garantidora da liberdade de expressão, direito tão caro aos americanos como o próprio direito à vida, SMOLLA¹³⁶ argumenta sobre a necessidade de preservar sua integridade e que foi através da evolução da jurisprudência naquele país que eles têm conseguido combater a censura.

No mencionado romance¹³⁷, embora o perigo de bombardeios esteja sempre à espreita e os bombeiros estejam sempre alerta, os bombeiros de *Fahrenheit 451* não apagam incêndios. Ao contrário, eles os ateiam. Diante da

¹³⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento p. 205

¹³⁵ DWORKIN, Ronald. **Uma questão de princípio**. São Paulo: Martins Fontes, 2000, p. 504

¹³⁶ SMOLLA, Rodney. **The life of the mind and a life of meaning**: reflections on Fahrenheit 451. Michigan Law Review, Vol. 107, No. 6, 2009. Survey of Books Related to the Law, pp. 895-912. Michigan Law Review Association, 2009. p. 901

¹³⁷ BRADBURY, Ray. **Fahrenheit 451**. 1953

evolução tecnológica, as casas são construídas com materiais modernos à prova de fogo e os únicos incêndios são aqueles iniciados pelos próprios bombeiros na queima de livros, os quais foram banidos da sociedade e passaram a ser artigos de contrabando, da mesma forma que drogas ilícitas e moeda falsa.

Os avanços na tecnologia auxiliam os bombeiros em suas tarefas através dos equipamentos de vigilância e monitoramento que cobrem a cidade, enquanto o *Mechanical Hound*, uma fera robótica com superpoderes de detecção, velocidade e destruição, farejam à procura de infratores. A publicidade comercial e a propaganda política são onipresentes. Até que um dia o protagonista da história, um bombeiro, começa a questionar sua vida e investigar a causa do banimento dos livros. Ao questionar seu superior no trabalho, recebe a informação de que a censura não foi iniciativa do governo, e sim do próprio povo, com o apoio da tecnologia, da exploração das massas e da pressão feita pelas minorias, que se sentiam ofendidas e provocadas pelas ideias que apareciam nos livros.

Conforme SMOLLA¹³⁸ observa, *Fahrenheit 451* sugere que a censura é frequentemente iniciada pela população e, após, abraçada pelo governo, quando, então, ela se torna mais efetiva. SMOLLA discorre que a censura, em muitos aspectos, é própria do ser humano, diante de sua dificuldade em tolerar opiniões discordantes. Contudo, desde a Inquisição Espanhola, até o Terceiro Reich, a queima de livros foi um precursor gráfico da histeria de massa, controle mental e paranoia. Como o Ministro Brandeis, da Suprema Corte dos Estados Unidos, dispôs: “homens temiam bruxas e queimaram mulheres” e argumentou que a melhor forma de combater o medo que levou os homens a queimarem mulheres é dar liberdade aos discursos sobre bruxas e caça às bruxas¹³⁹.

Diante do contexto tecnológico atual, a menção ao romance *Fahrenheit 451* serve para ilustrar os desafios que deverão ser superados sempre que há a necessidade de restringir liberdades. Assim, observa-se que o grande

¹³⁸ SMOLLA, Rodney. **The life of the mind and a life of meaning**: reflections on Fahrenheit 451. p. 902

¹³⁹ SMOLLA, Rodney. **The life of the mind and a life of meaning**: reflections on Fahrenheit 451. p. 904

desafio da LGPD é definir as regras inerentes à proteção dos dados pessoais, ao mesmo tempo em que deve garantir que as medidas previstas na Lei não suprimam a liberdade de expressão, a livre manifestação do pensamento e o direito à informação.

Um dos debates mais relevantes sobre o tema, entre tantos outros, e que impacta diretamente nas conclusões advindas da pesquisa ora objetivada no que concerne à publicização de dados processuais na Internet, versa sobre a sujeição de buscadores da Internet aos ditames de leis de proteção de dados, em razão da responsabilidade pelo tratamento de dados pessoais e atuação como intermediário.

Sobre o assunto, vale trazer à baila o *leading case* europeu de 2014, citado por VANZOIFF¹⁴⁰, em que o Tribunal de Justiça da União Europeia decidiu pela possibilidade de desindexação quando o tratamento de dados leva a um resultado que atente contra a dignidade da pessoa *lato sensu*, sopesando liberdade de expressão e direito à informação *versus* honra e imagem de uma pessoa. No caso em questão, os dados de um cidadão, cujo débito já havia sido saldado há tempo, ainda constavam nos resultados de busca da Internet.

Como resultado da democratização das relações de poder, podemos identificar a existência de um “direito humano ao saber” resultado – primeiramente, no plano político – das liberdades públicas conquistadas no processo civilizatório. A liberdade de informação e os correlatos direitos à informação e de acesso à informação, além de direitos humanos e fundamentais de alta relevância, representam técnicas democráticas de alta densidade na conformação das relações humanas numa determinada comunidade política e social. Na atualidade, é possível reunir tais direitos e os deveres que lhes são inerentes numa disciplina jurídica que acabou por ser denominada Direito da Informação¹⁴¹.

¹⁴⁰ VANZOIFF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 32

¹⁴¹ SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. **O direito à informação na ordem constitucional brasileira: breves apontamentos**. In: Acesso à informação como direito

2.2.3.4 A inviolabilidade da intimidade, da honra e da imagem

Da mesma forma que a LGPD enfatiza como fundamento a privacidade, também o faz com a inviolabilidade da intimidade, da honra e da imagem, direitos igualmente fundamentais previstos no mesmo art. 5º, X, da Constituição Federal.

O direito à intimidade já foi tratado mais detalhadamente no capítulo anterior. Apesar disso, vale tecer alguns comentários neste ponto da pesquisa. Conforme entendimento de DONEDA¹⁴², há uma proliferação de termos distintos doutrinariamente para se referir à privacidade, como “vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada [...]”, o que pode gerar insegurança jurídica, em que pese o próprio Tribunal Europeu de Direitos Humanos “não considerar possível, nem necessário, procurar uma definição exaustiva para a noção de vida privada.”

É por isso que, na visão arendtiana¹⁴³:

[...] um dos mais importantes direitos privados, que se coloca igualmente na perspectiva *ex parte populi*, é o direito à intimidade. É *the right to be let alone* de que falava Brandeis, que ela cita com toda a propriedade, pois foi Brandeis, num artigo escrito em parceria com Samuel Dennis Warren e publicado em 1890 na Harvard Law Review, um dos juristas que impulsionou a elaboração doutrinária e jurisprudencial em torno deste direito, realçando a importância, para as pessoas, do estar só¹⁴⁴.

LAFER¹⁴⁵ destaca que o direito à intimidade atualmente é considerado parte integrante dos direitos da personalidade, tutelando o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do

fundamental e dever estatal. Coordenadores: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla; RUARO, Regina Linden. Porto Alegre: Livraria do Advogado, 2016. (p. 11)

¹⁴² VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 37

¹⁴³ Em referência à Hanna Arendt, filósofa e teórica política contemporânea. Judia nascida na Alemanha, Arendt vivenciou os horrores da perseguição nazista, o que motivou a sua pesquisa sobre o fenômeno do totalitarismo. Suas principais obras são “As Origens do Totalitarismo”, “Eichmann em Jerusalém”, “Entre o Passado e o futuro” e “A Condição Humana”. Disponível em <https://mundoeducacao.bol.uol.com.br/biografias/hannah-arendt.htm>, acessado em 13/04/2020.

¹⁴⁴ LAFER, Celso. **A reconstrução dos direitos humanos**. p. 239

¹⁴⁵ LAFER, Celso. **A reconstrução dos direitos humanos**. p. 240

conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada.

A demanda por um direito à intimidade, continua LAFER¹⁴⁶, é uma consequência das novas realidades sociais do mundo contemporâneo, em que se observa a interferência crescente na esfera da vida privada por parte do poder público – por meio do poder de polícia, assim como da atividade judiciária – e por parte de terceiros, como resultado da inovação tecnológica.

E daí, justamente, começa a deflagrar a necessidade da defesa desses direitos fundamentais em termos de proteção de dados pessoais, pois, de acordo com Stefano Rodotà *apud* VANZOIFF¹⁴⁷:

[...] cada um dos dados, considerados em si, pode ser pouco ou nada significativo: ou melhor, pouco ou nada diz além da questão específica a que diretamente se refere. No momento em que se torna possível conhecer e relacionar toda a massa de informações relativas a uma determinada pessoa, do cruzamento dessas relações surge o perfil completo do sujeito considerado, que permite sua avaliação e seu controle por parte de quem dispõe do meio idôneo para efetuar tais operações.

Para HARARI¹⁴⁸, os algoritmos do Big Data representam um risco, também, ao livre arbítrio dos seres humanos:

When the biotech revolution merges with the infotech revolution, it will produce Big Data algorithms that can monitor and understand my feelings much better than I can, and then authority will probably shift from humans to computers. My illusion of free will is likely to disintegrate as I daily encounter institutions, corporations and government agencies that understand and manipulate what was hitherto my inaccessible inner realm.

Interessante *insight* extraído da obra de VANZOIFF¹⁴⁹ é a de que quando tecnologias existentes podem ler mentes ou detectar células cancerosas, como proteger a intimidade e esses demais direitos fundamentais? Uma coisa é

¹⁴⁶ LAFER, Celso. **A reconstrução dos direitos humanos**. p. 240

¹⁴⁷ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 36

¹⁴⁸ HARARI, Noah Yuval. **21 lessons for the 21st century**. London: Jonathan Cape, 2018. E-book. p. 54.

¹⁴⁹ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 37

continuar fumando apesar das estatísticas que ligam o fumo ao câncer de pulmões. Outra é continuar fumando apesar da advertência concreta de um sensor biométrico que acabou de detectar 17 células cancerosas na parte superior de seu pulmão esquerdo. E, se você quiser desafiar o sensor, o que vai fazer quando o sensor repassar a advertência a sua seguradora, seu chefe e sua esposa?

Uma das respostas certamente é prever a inviolabilidade da intimidade, da honra e da imagem como fundamento e dissecar as mais variadas obrigações de proteção de dados pessoais em lei, como a LGPD o faz, buscando, também, uma modificação cultural no tratamento dos dados pessoais. Nesse ponto, é possível inferir o caráter promocional – no sentido de Direito Promocional abordado anteriormente – da LGPD.

2.2.3.5 O desenvolvimento econômico e tecnológico e a inovação

A evolução tecnológica forma as bases da quarta revolução industrial por meio de soluções inovadoras como ocorre com a inteligência artificial, internet das coisas e o acúmulo expressivo de dados e informações, conformando a chamada economia digital.

Se a Revolução Industrial foi um marco em que a tecnologia passou a ocupar destaque na dinâmica social, a sua rápida evolução nas mais diversas áreas, como informática, eletrônica e telecomunicações, passou a condicionar diretamente a sociedade como instrumento de produção, distribuição do tempo e de espaço. A tecnologia deixou de ser vista apenas como situação de fato, isolada de uma conjuntura, para ser um vetor condicionante da sociedade e, em consequência, do próprio direito¹⁵⁰, exercendo grande influência sobre a arquitetura jurídica nacional e internacional.

É verdade que medidas como a promulgação de leis voltadas ao incentivo à inovação, nos moldes do que vem ocorrendo no Brasil, por exemplo, desde 2004, tem o objetivo de envidar esforços na implementação de um sistema

¹⁵⁰ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 37

nacional e inserir o país na economia global, com vistas a recuperar o déficit tecnológico e promover o reconhecimento da inovação como fator de desenvolvimento¹⁵¹.

No que concerne o Poder Judiciário, é notório o fato de que a inovação tecnológica foi uma grande aliada na consecução do direito fundamental à celeridade processual, previsto no art. 5º da Constituição Federal, advindo da Reforma do Judiciário, introduzida pela Emenda à Constituição nº 45/04, que assegurou a todos, no âmbito judicial e administrativo, a razoável duração do processo e os meios que garantam a celeridade de sua tramitação.

Assim, em 19 de dezembro de 2006, foi editada a Lei nº 11.149, que introduziu a informatização do processo judicial e estabeleceu a possibilidade de utilização do meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais, inovação esta que trouxe grandes avanços e contribuiu com os objetivos de desburocratizar e acelerar os procedimentos judiciais.

Nesse passo, o Sistema Nacional para a Transformação Digital (SNTD), criado através do Decreto 9.319/18, prevê que o desenvolvimento da economia digital requer confiança no ambiente digital. Assim, a ação governamental deve estar focada em proteção de direitos e privacidade e defesa e segurança no ambiente digital, mediante o aprimoramento de mecanismos de proteção de direitos no meio digital, inclusive nos aspectos relativos à privacidade e à proteção de dados pessoais, assim como fortalecer a segurança cibernética no País, estabelecendo mecanismos de cooperação entre entes governamentais, entes federados e setor privado, com vistas à adoção de melhores práticas, coordenação de resposta a incidentes e proteção da infraestrutura crítica.¹⁵²

Observa-se, no entanto, que a Sociedade que consegue ter a abertura necessária para manipular dados, inovando e gerando novos modelos de

¹⁵¹ BENACCHIO, Marcelo; MACIEL, Renata Mota. **A LGPD sob a perspectiva da regulação do poder econômico**. In: Comentários à Lei Geral de Proteção de Dados. Coordenadora: LIMA, Cíntia Rosa Pereira. São Paulo: Almedina, 2020. Versão Kindle. Posição 754

¹⁵² VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 38

negócios, produtos e serviços, automaticamente provoca o desenvolvimento e, conseqüentemente, alavanca a economia.

Sendo assim, há que se ter cuidado para equilibrar a imposição de restrições legais ou regulatórias para o fluxo de dados para que estas restrições não se tornem limitadoras do desenvolvimento econômico e, conseqüentemente, da inovação na era digital. Por essa razão, ambos constam como fundamentos da LGPD.

2.2.3.6 A livre iniciativa, a livre concorrência e a defesa do consumidor

Segundo dispõe BIONI¹⁵³, com a “inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação”.

O mercado do tratamento dos dados pessoais, assim, deve estar aberto a todos os que busquem empreender, nos termos do art. 170 da Constituição Federal, que prevê que a ordem econômica, fundada na valorização do trabalho humano e na livre-iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados princípios, entre os quais o da livre concorrência e o da defesa do consumidor.

Sem a garantia da livre-iniciativa no tratamento de dados pessoais, poderia haver compressão do uso de tecnologias e, conseqüentemente, prejuízos aos usuários, motivo pelo qual o tratamento jurídico equilibrado para as atividades desenvolvidas no mercado é condição para se evitar a retração da economia pautada em dados.

¹⁵³ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento** p. 12

LEONARDI¹⁵⁴ enumera alguns dos fatores econômicos, sociais e jurídicos que evidenciam referida importância, tais como a função social das ferramentas digitais; a promoção da liberdade de expressão, o acesso à informação, à educação e à cultura; variedade de papéis econômicos, gerando empregos e tributos por meio de novos modelos de negócio e constante inovação; e a segurança jurídica no ambiente *on-line* fomentar a inovação nacional.

Assim, a proteção de dados e os interesses de privacidade e dos direitos da personalidade dos indivíduos são relevantes para qualquer avaliação de potencial abuso de poder, bem como em eventuais fusões de empresas, que podem acumular poder informativo.¹⁵⁵

Assim, a livre concorrência e a livre-iniciativa são previsões legais que precisam ser analisadas em conjunto com as demais normas que possam traçar limites e estabelecer parâmetros para as decisões empresariais, em especial aquelas que podem acarretar prejuízos à sociedade, tais como nos casos de vazamento ou tratamento ilícito de dados, motivo pelo qual a proteção ao consumidor se apresenta como forma de impor referido equilíbrio. Conforme SANTOS e MORAES¹⁵⁶, “uma empresa que se utilize de práticas abusivas no relacionamento com o consumidor, aproveitando-se de sua situação de vulnerabilidade, possivelmente corresponderá, também, em desequilíbrio no âmbito concorrencial”.

Na mesma linha, REMEDIO e SILVA¹⁵⁷, em artigo no qual comentam a aquisição do Waze pelo Google, salientam que, sem a adoção de

¹⁵⁴ LEONARDI, Marcel. **Marco Civil da Internet e Proteção de Dados Pessoais**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. *Direito & Internet III: Marco civil da internet*. São Paulo: Quartier Latin, 2015, p. 536-537.

¹⁵⁵ VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 42

¹⁵⁶ SANTOS, Felipe Augusto dos; MORAES, Ana Paula Bagaiolo. **O direito concorrencial e a proteção ao consumidor na era do big data**. In: BAGNOLI, Vicente. *Concorrência e Inovação: anais do congresso internacional para a promoção de debates acerca do direito da concorrência e inovação tecnológica diante da realidade e desafios da economia digital*. São Paulo: Scortecci, 2018. p. 122.

¹⁵⁷ REMÉDIO, José Antonio; SILVA, Marcelo Rodrigues da. **O uso monopolista do Big Data por empresas de aplicativos: políticas públicas um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e livre concorrência**. Disponível em

políticas públicas de longo prazo, a racionalidade empresarial continuará utilizando-se de estratégias anticoncorrenciais sensíveis envolvendo *big data*, criando monopólios em determinados setores em que o interesse não é o consumidor e questões relacionadas à mobilidade urbana, por exemplo, mas sim a obtenção de dados e a possibilidade de impedir que concorrentes ganhem força no setor. Concluem que a economia criativa, que tem por centralidade os ativos intangíveis, torna-se a principal estratégia de desenvolvimento dos municípios, territórios, estados e países, pois são os únicos recursos que não se esgotam, mas se multiplicam com o uso, gerando não apenas resultados financeiros, mas também resultados sociais, ambientais e culturais, sendo necessária revisão de políticas públicas concorrenciais no setor tecnológico, de forma a criar novos concorrentes.

Em relação à proteção do consumidor, destaca-se que leis como o Código de Defesa do Consumidor, além do Decreto 7.962/13, que regulamentou o CDC para o comércio eletrônico, e também a Lei do Cadastro Positivo (Lei 12.414/2014), já tutelavam, antes ainda da LGPD, a privacidade e a máxima transparência nas relações negociais com os consumidores. Contudo, a ausência de regras claras relativas aos tratamentos de dados realizados e a dependência da interpretação judicial em relação à aplicabilidade das previsões normativas até então existentes, acabam por gerar insegurança jurídica tanto aos consumidores, quanto aos agentes de tratamento.

2.2.3.7 Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais

A proteção da pessoa humana deve ser entendida como valor máximo do ordenamento jurídico, conforme fundamento estampado no art. 1º, inciso III, da Constituição Federal. Segundo VANZOIFF¹⁵⁸, não levar em consideração novos problemas oriundos da evolução tecnológica, que influencia na experiência científica, política e cultural de uma sociedade, significaria abater o

<<https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4966/3651>>. Acesso em: 20/03/2020.

¹⁵⁸ VANZOIFF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. p. 46

direito ao seu próprio tempo, tornando-o automaticamente obsoleto, insuficiente e incapaz de garantir os preceitos da pessoa com a velocidade característica da revolução tecnológica, o que é fundamental.

BOBBIO¹⁵⁹, ao questionar a existência de um fundamento absoluto para os direitos do homem – o que ele considera uma ilusão, argumentando, dentre outras justificativas, que o que parece fundamental numa época histórica deixa de ser fundamental em outras, não sendo, portanto, concebível atribuir um fundamento absoluto a direitos historicamente relativos – assevera que o problema fundamental em relação aos direitos do homem, atualmente, não é justificá-los, e sim protegê-los. Na hermenêutica de BOBBIO¹⁶⁰, trata-se de um problema não filosófico, mas político:

Com efeito, o problema que temos diante de nós não é filosófico, mas jurídico e, num sentido mais amplo, político. Não se trata de saber quais e quantos são esses direitos, qual é a sua natureza e seu fundamento, se são direitos naturais ou históricos, absolutos ou relativos, mas sim qual é o modo mais seguro para garanti-los, para impedir que, apesar das solenes declarações, eles sejam continuamente violados.

Como visto anteriormente, a Declaração Universal de Direitos Humanos, da Organização das Nações Unidas (ONU), em seu art. 12, prevê que ninguém sofrerá intromissões arbitrárias na sua vida privada, bem como que, contra tais intromissões ou ataques, toda a pessoa tem a proteção da lei.

No ponto, impende trazer a indagação de LAFER¹⁶¹ sobre como conciliar a pessoa humana como “valor-fonte” legitimador dos ordenamentos jurídicos, segundo a tradição, com o risco permanente de sua descartabilidade. Ou seja, como garantir que os direitos humanos possam continuar sendo o núcleo da reflexão acerca da legitimidade do poder e da justiça da norma?

É sabido, no entanto, que o processo de positivação das declarações de direitos não desempenhou esta função estabilizadora, pois do século XVIII até os nossos dias, o elenco dos direitos do homem contemplados nas constituições e nos

¹⁵⁹ BOBBIO, Norberto. **A Era dos Direitos**. Versão Kindle. Posição 651-713

¹⁶⁰ BOBBIO, Norberto. **A Era dos Direitos**. Versão Kindle. Posição 758.

¹⁶¹ LAFER, Celso. **A reconstrução dos direitos humanos**. p. 113

instrumentos internacionais foram-se alterando com a mudança das condições históricas. [...] Daí a crítica proposta no âmbito do paradigma da Filosofia do Direito à fundamentação jusnaturalista dos direitos humanos, baseada num conceito como o de natureza humana – que se evidenciou ambíguo e plurívoco – e a sua substituição por uma fundamentação historicista. Neste ângulo, o problema acabou se colocando como o da razoabilidade dos direitos do homem na História, não se tratando, conseqüentemente, na palavras de Croce, “de demandas eternas, senão apenas de direitos históricos, manifestação das necessidades de tal ou qual época e intentos de satisfazer essas necessidades”.¹⁶²

Portanto, resta claro que os dados pessoais de cada indivíduo, ainda que dispersos nos diversos meios de coleta e armazenamento de informações, fazem parte do conjunto de representação da personalidade da pessoa, de modo que, quando conjugados com outros dados existentes por meio do uso da tecnologia, podem passar a representar, perante terceiros, a identidade desse indivíduo. Desta forma, verifica-se que a proteção de dados pessoais tem um papel de fundamental importância para que o indivíduo se realize e se relacione na sociedade, o que é um traço marcante dos direitos da personalidade.

A respeito da identidade, todo esse cruzamento de informações leva a concluir que a identidade das pessoas estará, em algum ponto, disponível na Internet. É possível citar, como exemplos, os registros de saúde, os detalhes bancários, título de eleitor, carteira de motorista, mídias sociais e e-mails. Ainda que possam estar protegidos por algum tipo de tecnologia, essas informações criam uma identidade digital. E é essa identidade digital que pode ser rastreada até algum indivíduo e, portanto, ela é análoga à identidade pessoal no contexto social¹⁶³.

JUSTEN FILHO aduz, também, que a dignidade humana é um compromisso da nação consigo mesma e não um preceito a ser observado e garantido somente pelas instituições governamentais:

A sociedade tornou-se muito complexa para que suas necessidades sejam satisfeitas exclusivamente por parte do

¹⁶² LAFER, Celso. **A reconstrução dos direitos humanos**. p. 124

¹⁶³ WALTERS, Robert; TRAKMAN, Leon; ZELLER, Bruno. **Data protection law: a comparative analysis of asia-pacific and european approaches**. Singapore: Springer, 2019. (eBook). p. 35

Estado. A cidadania impõe que os indivíduos e as empresas se organizem e atuem concretamente para minorar os problemas e combater as carências. A dignidade humana e a solidariedade são compromissos da Nação consigo mesma, e não um fardo a ser carregado pelas instituições governamentais.¹⁶⁴

Diante do exposto, a LGPD, ao fundamentar sua existência também no livre desenvolvimento da personalidade e na dignidade, demonstra preocupação com a projeção da personalidade do ser humano, ao prever como direito do titular a correção de dados incompletos, inexatos ou desatualizados. Esses direitos demonstram que a proteção de dados vai além da proteção à privacidade, atingindo, também o direito da personalidade.

2.2.4 Princípios aplicados ao tratamento de dados pessoais

A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não será atendido¹⁶⁵.

Pela LGPD, as atividades de tratamento legítimo, específico e explícito de dados pessoais, previamente informado ao titular ou legalmente justificado, devem estar orientadas pelos seguintes princípios: finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas, conforme preceitua e descreve, de forma conceitual e explicativa, seu artigo 6º.

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

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

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

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados

¹⁶⁴ JUSTEN FILHO, Marçal. **Curso de direito administrativo**. 2. ed. rev. e atual. São Paulo, Saraiva: 2006. p. 31

¹⁶⁵ PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018 (LGPD). Versão Kindle. Posição. 326

pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

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

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

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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

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

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

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

A compreensão dos princípios da LGPD é de fundamental importância para a delimitação da legalidade do tratamento dos dados pessoais.

Para ÁVILA¹⁶⁶, os princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementaridade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção.

¹⁶⁶ ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. 4. ed. São Paulo: Malheiros, 2005.p.70

Desta feita, conhecer os princípios basilares da Lei auxiliará na tarefa de interpretação e aplicação de seus dispositivos quando em conflito com demais princípios e normas previstos em nosso ordenamento jurídico.

Feita esta breve apresentação dos princípios gerais previstos na LGPD, há de se ressaltar que o Poder Público está sujeito a princípios especiais, dispostos na Carta Magna e no Capítulo IV da Lei, e que serão tratados com maior detalhamento na sequência deste trabalho.

2.2.5 Justificativa legal

A linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas. No entanto, há outras 09 (nove) situações em que o tratamento de dados pessoais ocorre sem necessidade de consentimento expresso, em conformidade com o disposto no art. 7º da LGPD, a saber:

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

I - mediante o fornecimento de consentimento pelo titular;

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

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

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

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

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

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

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

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Como se observa, apesar de o consentimento ainda ser considerado a principal base legal para o tratamento de dados pessoais, o consentimento passa a ser apenas uma das dez hipóteses legais trazidas na legislação, sendo que todas as outras nove hipóteses existentes independem do consentimento para que sejam tidas como válidas.

Novamente, para os fins deste trabalho, descreveremos com maior detalhamento a base legal para o tratamento de dados pessoais pelo Poder Judiciário.

Diante das previsões constitucionais de inafastabilidade da apreciação pelo Poder Judiciário (artigo 5º, XXXV, da Constituição Federal) e ampla defesa e contraditório (artigo 5º, LV, da Constituição Federal), a LGPD traz a expressa possibilidade para o tratamento de dados pessoais para o exercício de direitos em processos em geral (judiciais, administrativos ou arbitrais).

Não há, portanto, necessidade de consentimento para utilizar os dados pessoais da contraparte num processo judicial, administrativo ou arbitral. A ausência de uma base legal para essa finalidade levaria ao absurdo de ser necessária a autorização da parte contrária para que permitisse a utilização de seus dados para ser iniciado o processo¹⁶⁷.

¹⁶⁷ LIMA, Caio César Carvalho. **Capítulo II: Do tratamento de dados pessoais**. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019. p. 184

Assim, nas situações em que se entender que determinados dados pessoais poderão servir como elemento para exercício de direitos em demandas em geral, eles poderão ser armazenados, desde que para essa única e exclusiva finalidade, enquanto subsistir tal necessidade.

Desta forma, a base legal expressa no inciso VI do art. 7º da LGPD também legitima o Poder Judiciário a realizar a guarda e gestão dos dados pessoais constantes de processos judiciais.

Ademais, podem ser utilizados como parâmetros para retenção da informação os respectivos prazos prescricionais previstos na legislação civil e penal. Havendo discussão judicial, haverá fundamento para armazenamento dos dados durante todo o prazo em que subsistir possibilidade de discussão da demanda¹⁶⁸.

É possível depreender, em um primeiro momento, que o tratamento de dados descrito no referido dispositivo legal autoriza o Poder Judiciário a utilizar os dados pessoais nos limites de suas funções jurisdicionais, tema que será tratado mais adiante.

2.3 A APLICAÇÃO DA LGPD NO ÂMBITO DO PODER PÚBLICO

Considerando as particularidades institucionais e premissas constitucionais a que estão submetidas as pessoas jurídicas de direito público, mormente no que diz respeito ao Poder Judiciário, o foco neste ponto da pesquisa é o Capítulo IV da LGPD, que trata de sua aplicação ao e pelo Poder Público.

2.3.1 O tratamento de dados pessoais pelo Poder Público

Aspecto de grande relevância no cenário constitucional contemporâneo brasileiro é, sem dúvida, a delimitação estrita da separação dos três Poderes, quais sejam o Poder Executivo, o Poder Legislativo e o Poder Judiciário, expressamente prevista na CRFB:

¹⁶⁸ LIMA, Caio César Carvalho. **Capítulo II: Do tratamento de dados pessoais**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; LGPD: Lei Geral de Proteção de Dados. p. 184

Art. 2º São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário.

Estes Poderes coexistem em par de igualdade, sem que haja uma hierarquia entre eles. Há, porém, uma divisão bem estabelecida de funções precípuas de cada um.

MENDES e BRANCO¹⁶⁹ esclarecem que a separação dos Poderes tem por objetivo dividi-los entre pessoas distintas a fim de impedir a concentração do poder em uma única esfera.

Em última instância, é uma proteção aos cidadãos de que aqueles que se encontram à frente do Estado não poderão sobrepor suas vontades às dos seus governados, pois haverá sempre certa vigilância sobre suas ações. É o Estado controlando e limitando o próprio Estado, no denominado sistema de freios e contrapesos (*checks and balances*).

Sobre as incumbências de cada um dos Poderes:

[...] Na experiência brasileira, a doutrina mais autorizada extrai dessas ideias centrais dois corolários: a especialização funcional e a necessidade de independência orgânica de cada um dos Poderes em face dos demais. A especialização funcional inclui a titularidade, por cada Poder, de determinadas competências privativas. A independência orgânica demanda, na conformação da experiência presidencialista brasileira atual, três requisitos: i) uma mesma pessoa não poderá ser membro de mais de um Poder ao mesmo tempo; ii) um Poder não pode destituir os integrantes de outro por força de decisão exclusivamente política; e iii) a cada Poder são atribuídas, além de suas funções típicas ou privativas, outras funções (chamadas normalmente de atípicas), como reforço de sua independência frente aos demais Poderes.¹⁷⁰

Assim, esta divisão dos Poderes representa também a divisão de funções, o que significa que cada ente tem suas atribuições bem delineadas, bem como tem autonomia para desenvolvê-las.

¹⁶⁹ MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. p. 43.

¹⁷⁰ BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo**, p. 197.

A Lei Geral de Proteção de Dados aplica-se, como dito anteriormente, não só às pessoas naturais e jurídicas de direito privado, como também às de direito público e prevê, dentre outras regras, que o tratamento de dados pessoais deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, com informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizados para a execução dessas atividades, em veículos de fácil acesso.

O legislador dedicou o Capítulo IV da LGPD para estabelecer as regras às quais o Poder Público deve se submeter quando realizar o tratamento de dados pessoais dos cidadãos. Considerando que um dos objetivos da Lei é a proteção do titular de dados contra intromissões em sua vida privada e o uso arbitrário de suas informações pessoais, nada mais salutar que a LGPD preveja, também, a proteção contra o Estado, de modo a evitar o comprometimento dos direitos de personalidade.

Há uma preocupação legítima no que se refere à vigilância perpetrada pelo Estado, aos moldes daquela descrita na obra 1984, de George Orwell, um clássico da literatura que descreve um futuro distópico no qual o Estado, o grande *Big Brother*, exerce o controle social através de uma vigilância ostensiva possibilitada pela tecnologia.

Em relação ao conceito de “vigilância”, vale trazer a explicação de BIONI, para quem o termo *surveillance*, na língua inglesa, seria mais abrangente e teria um significado mais adequado com o conceito atualmente advindo do uso da tecnologia, que seria a vigilância através do monitoramento e controle de informações:

[...] essa abordagem foi estabelecida com base na diferença semântica e polissêmica entre os termos *surveillance* e vigilância. O termo em inglês guardaria um sentido maior a cobrir, mais satisfatoriamente, o fenômeno contemporâneo. Embora o termo vigilância seja linguisticamente adequada, a palavra em língua inglesa possui uma polissemia que não é alcançada pelo termo em português. Isso fica nítido quando o teórico dos estudos sobre

a *surveillance* faz a distinção entre ‘*surveillance*’ e ‘*new surveillance*’, respectivamente associadas à modernidade tradicional e a modernidade líquida. A maturidade do debate no exterior, contudo, permite que os autores anglófonos ressignifiquem a palavra em inglês. Como a regra semântica do vocábulo ‘vigilância’ é demasiadamente forte no Brasil – por vários motivos, inclusive por estar muito ligada, etimologicamente, à palavra ‘*vigilance*’, na ausência de tradução que compartilhe o mesmo sentido, preferimos utilizar o termo diretamente do inglês.

Lisa Sotto, eminente advogada estadunidense, com forte atuação global na área do Direito à Privacidade, em evento¹⁷¹ que teve como objetivo fomentar a discussão se os Estados Unidos deveriam adotar uma legislação federal sobre a temática da proteção a dados pessoais nos moldes do regulamento europeu, posição que ela defende, fez uma observação emblemática ao explicar a razão pela qual a proteção de dados tem status de direito fundamental na União Europeia, ao contrário do que ocorre nos Estados Unidos. A jurista asseverou que, por meio do uso dos dados pessoais de indivíduos, “in America, we *market* people to death. In Europe, they *put* people to death”. Ela destacou, também, que na Europa e na América Latina, dados pessoais sensíveis foram largamente utilizados para objetivos persecutórios durante os períodos ditatoriais.

Vale destacar que os *framers* da Constituição dos Estados Unidos, ao cunharem pela primeira vez no ordenamento jurídico norte-americano uma versão do que hoje pode ser interpretado como o direito à privacidade e inviolabilidade da intimidade na quarta emenda à Constituição, conferiram ao povo o direito de inviolabilidade de sua pessoa, casas, papeis e haveres, protegendo-os contra buscas e apreensões feitas pelo Estado de maneira arbitrária.

De acordo com TASSO¹⁷², a relação jurídica estabelecida entre o Poder Público e o titular de dados pessoais é marcada pela assimetria de poder, tanto em decorrência da natureza jurídica do ente público, que atua com poder de

¹⁷¹ Evento *Data Done Right*, realizado na cidade de Washington D.C., em 11.07.2019.

¹⁷² TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. *LGPD: Lei Geral de Proteção de Dados*. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019. p. 245.

império, quanto pela circunstância de que o ente público detém grande quantidade de dados pessoais em seu poder.

Nota-se que, conforme anteriormente aludido, o Direito tem, também, como função limitar os poderes do Estado para que não haja interferência desarrazoada nas liberdades individuais e garantias fundamentais dos cidadãos.

É nesse contexto de proteção às liberdades individuais dos cidadãos, afetadas pela coleta e uso de seus dados pessoais pelo Poder Público, haja vista a disparidade entre a capacidade de tratamento e controle que um cidadão possui em relação ao Estado, que se definem as regras do Capítulo IV.

O fato de a LGPD destinar um capítulo específico para o tratamento de dados pelo Poder Público corrobora os ensinamentos de BARROSO¹⁷³, ao dispor que a presença do Estado em uma relação jurídica “exigirá, como regra geral, um regime jurídico específico, identificado como de direito público”.

O artigo 23¹⁷⁴, logo de início, prevê que o tratamento de dados pessoais pelas pessoas jurídicas de direito público previstas na Lei nº 12.527, de

¹⁷³ BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. p. 88

¹⁷⁴ Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e

IV - (VETADO)

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de

18 de novembro de 2011 (Lei de Acesso à Informação), deve sempre ser realizado para o “atendimento de uma finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, e define que as informações sobre o tratamento realizado devem ser claras e expostas em veículos de fácil acesso, dado preferência a sítios eletrônicos.

O caput do art. 23 estabelece dois princípios da Administração Pública que vinculam o tratamento de dados pelo Poder Público: a **finalidade pública** e a **supremacia do interesse público**.

O princípio da finalidade está contido no princípio da legalidade e dispõe que as atividades da Administração Pública deverão ser focadas e limitadas aos dispositivos normativos autorizadores de tais atividades, ou seja, este princípio limita o poder da Administração Pública ao exigir que atue dentro dos limites de suas normas, de modo a impedir atos abusivos contra os cidadãos¹⁷⁵.

O princípio da supremacia do interesse público, por sua vez, tem como objetivo preservar e realizar o interesse de toda a sociedade. É dizer que o interesse público se sobrepõe aos interesses privados.

Conforme prescreve BARROSO¹⁷⁶, o debate contemporâneo divide o interesse público em primário e secundário. O interesse público primário se consubstancia nos fins a que cabe promover no interesse de toda a sociedade, quais sejam a justiça, a segurança e o bem-estar social. Já o interesse público secundário se refere ao interesse da pessoa jurídica de direito público que é parte

1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

¹⁷⁵ AGRA, Walber de Moura. **Curso de direito constitucional**. p. 437

¹⁷⁶ BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. p. 90

em determinada relação jurídica, e pode ser traduzido como o interesse do erário, composto pela maximização da arrecadação e pela minimização das despesas.

É dessa distinção que decorrem as esferas constitucionais de atuação do Ministério Público, a quem cabe defender o interesse público primário, e da Advocacia Pública, a quem cabe a defesa do interesse público secundário¹⁷⁷.

Desta feita, em que pese a LGPD prever em seu art. 6º os princípios que devem reger o tratamento de dados de forma geral, o Poder Público está vinculado a observar, precipuamente, os princípios da finalidade e interesse públicos, de modo que a atuação do Poder Público é excepcional e condicionada.

Em continuidade à análise do referido artigo, depreende-se sua aplicação ao Poder Judiciário, uma vez que se subordinam ao regime da Lei de Acesso à Informação¹⁷⁸ todas as pessoas jurídicas de direito público, inclusive os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo e Judiciário, bem como do Ministério Público.

Ainda, o art. 23 prevê expressamente que o tratamento de dados pessoais pelo Poder Público deverá ter como objetivo a execução de suas competências legais ou o cumprimento das atribuições legais do serviço público.

A disposição acima decorre da prerrogativa de que uma das funções do Poder Público é administrar a vida em sociedade e somente o pode fazer em

¹⁷⁷ BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. p. 90

¹⁷⁸ Art. 1º. Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

observância e na medida em que a lei lhe dá investidura, ou seja, o Poder Público deve cumprir sua função legal¹⁷⁹.

O inciso I do art. 23, a seu turno, preconiza a transparência no tratamento de dados pessoais pelo Poder Público ao dispor que devem ser informadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, as hipóteses em que o tratamento de dados pessoais são realizados, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.

Importante ressaltar aqui que, não é porque os dados serão expostos em ambiente eletrônico que o ente público deverá informar aos titulares apenas os dados coletados naquele meio. A informação deverá abranger todos os dados tratados, ainda que não sejam coletados em meio físico, expondo aos titulares como e para quem utiliza os dados pessoais. A ANPD, todavia, poderá dispor sobre as formas de publicidade das operações de tratamento.

Importa ressaltar a necessária interseção da LGPD com a Lei de Acesso à Informação. A LAI regulamentou, em seu art. 8º, o direito fundamental do cidadão de obter dos órgãos públicos informações de seu interesse, uma vez observados os procedimentos previstos em lei, conforme lhe garante o inciso XXXIII do art. 5º da Constituição Federal¹⁸⁰. Vislumbra-se, no ponto, que a LGPD e a LAI convergem ao exigir que os entes públicos promovam a divulgação em local de fácil acesso de informações de interesse coletivo ou geral, que estejam sob sua custódia, contudo é possível identificar um conflito de interesses na identidade entre o Encarregado da LGPD e a Autoridade responsável pela

¹⁷⁹ TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. **LGPD: Lei Geral de Proteção de Dados**. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019. p. 252.

¹⁸⁰ Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

custódia da informação da LAI, tema que será abordado com maior profundidade no terceiro e último capítulo.

O art. 25, por sua vez, estabelece que os dados deverão ser mantidos sempre de forma estruturada e interoperável para uso compartilhado com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Esse artigo deve ser analisado com cautela. Ao tratar, genericamente, de “dados”, é possível entender que o dispositivo legal é mais abrangente do que intencionava ser, transbordando o escopo da norma inserida em lei de tratamento de dados pessoais e dados pessoais sensíveis, conforme definições legais constantes dos incisos I e II, do art. 5º da LGPD.

Em que pese a descrição genérica de “dados”, a conclusão a que se chega, considerando a especificidade e o objeto da LGPD, é de que o art. 25 trata somente de dados pessoais e dados pessoais sensíveis.

Cabe, aqui, pontuar que a incorporação de tecnologias da informação no setor público sofre maiores limitações do que o setor privado, tornando evidente o descompasso entre o nível de informatização não somente entre os setores público e privado, mas entre os próprios órgãos da Administração Pública de um mesmo Poder ou nível federativo¹⁸¹.

Esta heterogeneidade resulta em que cada órgão utiliza recursos de tecnologia da informação compatíveis com seus recursos disponíveis, muitas vezes com baixa eficiência, com cada órgão reunindo uma grande quantidade de dados repetidos, não estruturados, sem qualidade, não reutilizáveis e, conseqüentemente, incapazes de gerar valor na atividade administrativa, além de inviabilizar, por vezes, a execução de políticas públicas, a eficiência dos serviços públicos e a disseminação e o acesso das informações pelos cidadãos em geral.

¹⁸¹ TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 268.

A solução tecnológica preconizada pela LGPD para enfrentar o problema de fluxo informacional entre os órgãos públicos está na interoperabilidade e estruturação de dados.

No que se refere à interoperabilidade, esta pode ser entendida como uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente, conceituação obtida no sítio eletrônico do Governo Digital¹⁸².

Ao promover a interoperabilidade, a LGPD prescreve que o dado deve ser passível de tratamento por qualquer sistema, além de poder transitar pela Internet. Para tanto, é necessário que os dados estejam em padrão aberto e que os sistemas que efetuarão o tratamento estejam aptos a fazê-lo.

O artigo 26 deixa expresso que o uso compartilhado de dados pessoais pelo Poder Público deve atender os princípios de proteção de dados pessoais elencados no artigo 6º da LGPD.

Não basta, portanto, que o compartilhamento possua base legal, atenda às finalidades específicas de execução de políticas públicas e provenha de atribuição legal do órgão ou entidade pública.

É característica de normas que tratam da garantia de direitos em contexto fático permeado pela utilização de tecnologia da informação o forte atrelamento da aplicação das regras e à observância da base principiológica¹⁸³.

Os princípios do art. 6º da LGPD servem como filtros de validade e legitimidade das regras de proteção de dados pessoais, que se materializam quando se verifica que a execução das políticas públicas e o exercício das competências legais estão em equilíbrio com as liberdades positivas,

¹⁸² BRASIL. Governo Digital. Disponível em <https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade_eping>. Acesso em: 28/04/2020.

¹⁸³ TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 275

caracterizadas pelo controle da atividade pública, e negativas, que se consubstanciam na preservação dos direitos e garantias fundamentais do titular de dados¹⁸⁴.

Segundo TASSO¹⁸⁵, os princípios da finalidade, da adequação e da responsabilização e prestação de contas, previstos, respectivamente, nos incisos I, II e X do art. 6º da LGPD, buscam fundamento de validade nos princípios constitucionais da legalidade, da impessoalidade e da moralidade e se materializam quando, cumulativamente, o ato administrativo de tratamento ou compartilhamento de dados pessoais: (i) está previsto em leis e regulamentos ou respaldado em contratos, convênios ou instrumentos congêneres, conforme prevê o art. 7º, III, da LGPD; (ii) é praticado no exercício de suas competências ou atribuições, nos termos do art. 23, da LGPD; e (iii) o ato praticado busca o atendimento do interesse público, segundo prevê o art. 23 da LGPD.

Já os princípios de transparência e do livre acesso, previstos nos incisos VI e IV do art. 6º da LGPD, respectivamente, possuem direta relação com o princípio da publicidade e são observados quando o órgão público: (i) pratica a transparência ativa, combinados o art. 23, I, da LGPD com o art. 8º¹⁸⁶ da LAI; (ii) viabiliza a transparência passiva, combinados o art. 23, I da LGPD com o artigo 10¹⁸⁷ da LAI; (iii) implementa outras formas de publicidade das operações de tratamento preconizadas pela ANPD, previstas no art. 23, §1º¹⁸⁸, da LGPD; e (iv) expede os informes e comunicados previstos no art. 26, §2º e art. 27, II, da LGPD.

Os princípios da necessidade ou da mínima coleta, qualidade dos dados e da segurança, dispostos, respectivamente, nos incisos III, V e VII do art.

¹⁸⁴ TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**. p. 274

¹⁸⁵ TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; **LGPD: Lei Geral de Proteção de Dados**.p. 274

¹⁸⁶ Art. 8º. É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

¹⁸⁷ Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

¹⁸⁸ A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

6º da LGPD, possuem fundamento no princípio constitucional da eficiência, que juntamente com o princípio da não discriminação, previsto no inciso XI do referido artigo, fundamentado no princípio da legalidade e da boa-fé¹⁸⁹, fecham o escopo principiológico da LGPD.

Superados os princípios, verifica-se que o parágrafo 1º do artigo 26¹⁹⁰ enumera, exhaustivamente, as hipóteses autorizadoras da transferência de dados para entidades privadas, sendo vedada a transferência não fundamentada na forma estabelecida na lei. Este ponto voltará a ser abordado no Capítulo 3, ao tratar especificamente das exigências e necessidades do Poder Judiciário no que se refere à transferência de dados, inclusive internacional.

Assim, cabe ao Poder Público garantir que o uso compartilhado de dados segue os propósitos especiais que concernem à execução das políticas públicas e que, ao mesmo tempo, a ponderação entre a necessidade de

¹⁸⁹ Segundo Maria Sylvia Zanella di Pietro, “[n]a Constituição, o princípio da boa-fé não está previsto expressamente, porém pode ser extraído implicitamente de outros princípios, especialmente do princípio da moralidade administrativa e do própria exigência de probidade administrativa que decorre de vários dispositivos constitucionais (arts. 15, V, 37, 4º, 85, V). A Lei nº 8.429, de 2-6-92 (Lei da Improbidade Administrativa), considera como ato de improbidade que atenta contra os princípios da Administração Pública “qualquer ação ou omissão que viole os deveres de honestidade, imparcialidade, legalidade e lealdade às instituições” (art. 11). In: DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 26. ed. São Paulo: Atlas, 2013. p. 88

¹⁹⁰ Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

publicidade das informações disponíveis ao acesso garante que os direitos dos titulares sejam respeitados¹⁹¹.

Ademais, os órgãos públicos estão sujeitos a medidas administrativas específicas. Em razão disso, cabe à Agência Nacional de Proteção de Dados (ANPD), garantir que medidas cabíveis e proporcionais sejam adotadas quando da violação do tratamento de dados pessoais nos órgãos públicos.

Segundo MELLO¹⁹², os órgãos públicos estão no âmbito do regime administrativo, logo estão sujeitos às normas e aos parâmetros deste e, conseqüentemente respondem administrativa e não judicialmente, advindo daí mais uma razão para tratamento específico dentro dos limites das normas administrativas.

O art. 27 da LGPD dispõe que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado deverá ser informada à autoridade nacional e dependerá de consentimento do titular, salvo se dispensado nos termos da lei, nos casos em que a publicidade já é decorrente do tratamento realizado no exercício das competências legais do Poder Público, e nas exceções do §1º do art. 26.

A delimitação da aplicabilidade da lei em relação aos tipos de dados que são considerados regulados pela LGPD, nos termos dispostos no art. 4º da Lei,¹⁹³ demonstra que o tratamento de dados pessoais deve seguir um propósito

¹⁹¹ PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD)**.

¹⁹² MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**.

¹⁹³ Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência

certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado, conforme leciona PINHEIRO¹⁹⁴.

Além disso, ainda utilizando-se das observações feitas por PINHEIRO¹⁹⁵, “há sempre a necessidade de equilibrar a proteção da privacidade (como um direito individual) e a proteção da segurança pública (como um direito coletivo), especialmente diante da obrigação de fortalecer o combate ao crime organizado, à fraude digital e ao terrorismo”.

O exercício dos direitos dos titulares perante o Poder Público, na qualidade de Controlador, observará legislação específica, em especial a Lei de Acesso à Informação e a Lei do Habeas Data.

Qualquer compartilhamento, no entanto, deve ser respaldado pelos princípios e regras da LGPD, o que por certo terá um grande impacto e exigirá muitas implementações e uma política pública para adequação e conformidade do setor público à nova regulamentação.

Conforme PINHEIRO, o que se quer evitar é ter uma legislação que seja eficaz apenas no setor privado e não consiga ser implementada no setor público

internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

¹⁹⁴ PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD)**. Posição. 657

¹⁹⁵ PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD)**. Posição. 672

Capítulo 3

PERSPECTIVAS DO TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DO PROCESSO JUDICIAL À LUZ DA LGPD

3.1 A ESTRUTURA NORMATIVA APLICÁVEL AO ACESSO, PUBLICIDADE E PROTEÇÃO DE DADOS NO PROCESSO JUDICIAL

Para que se possa dar sequência à investigação dos reflexos da LGPD ao tratamento de dados no âmbito do processo judicial, cumpre-se, primeiramente, analisar as regras vigentes neste campo de aplicação de modo a possibilitar o cotejo posterior com a finalidade de confirmar, ou não, as hipóteses formuladas no início desta pesquisa.

3.1.1 Estrutura normativa processual: a publicidade é a regra, o sigilo é a exceção

A atual opção nos Estados Democráticos de Direito pela publicidade dos atos processuais como regra decorre do desenvolvimento das práticas judiciais que se deram em milênios de amadurecimento das civilizações¹⁹⁶.

Norberto Bobbio *apud* RUARO¹⁹⁷, ao tratar das relações da democracia com o poder invisível, estatui que a publicidade é entendida como uma categoria tipicamente iluminista, na medida em que representa um dos aspectos da batalha de quem se considera chamado a derrotar o reino das trevas. Utiliza-se, por isso, a metáfora da luz, do clareamento para contrastar o poder visível do invisível. A visibilidade vai fornecer a acessibilidade e a possibilidade de controle dos atos públicos. Originando-se, daí, o embate do Iluminismo contra o Estado absoluto, a partir da exigência da publicidade com relação aos atos do monarca, que eram fundados no poder divino.

¹⁹⁶ KEHDI, Andre; CORDANI, Dora Cavalcanti. **CNJ deve impedir processos em sites de busca.** Disponível em: <https://www.conjur.com.br/2010-out-22/cnj-impedir-sites-busca-encontrarem-informacoes-processuais#_ftn1_7163> Acesso em: 30/05/2020.

¹⁹⁷ RUARO, Regina Linden; LIMBERGER, Têmis. **Administração pública e novas tecnologias: o embate entre o público e o privado - análise da Resolução 121/2010 do CNJ.** Revista NEJ – Eletrônica, vol. 16 – n. 2. Revista Novos Estudos Jurídicos, 2011. p. 123

O triunfo dos Iluministas tem como resultado o art. 15 da Declaração dos Direitos do Homem e do Cidadão, que prevê o direito da sociedade de pedir contas a todo o agente público incumbido da administração. Este direito evoluiu e se consolidou na Carta dos Direitos Fundamentais da União Europeia, que em seu art. 41 prevê o direito a uma boa administração¹⁹⁸.

Nesta toada, a publicidade mostra-se como princípio norteador do Estado Democrático de Direito, conferindo transparência e propiciando o controle da legalidade e legitimidade dos atos da Administração Pública.

A realização do princípio da publicidade constitui-se em um dever da administração e se complementa com o direito à informação do cidadão. Desta conjugação, tem-se a satisfação dos demais princípios que regem a administração pública. Constata-se que a administração agiu ao amparo da legalidade, busca-se a moralidade e é satisfeita a efetividade, princípios estes todos que servem à realização do Estado Democrático de Direito¹⁹⁹.

Desta forma, a publicidade torna-se pressuposto necessário para a democracia, tendo em vista que esta se mostra como o canal de comunicação entre o Governo e os governados²⁰⁰.

A CRFB, em seu texto normativo, apresenta o princípio da publicidade nos seguintes dispositivos:

Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;

¹⁹⁸ BOBBIO, Norberto. **O futuro da democracia**. 7. ed. São Paulo: Paz e Terra, 2000, p. 103

¹⁹⁹ RUARO, Regina Linden; LIMBERGER, Têmis. **Administração pública e novas tecnologias: o embate entre o público e o privado - análise da Resolução 121/2010 do CNJ**. p. 125

²⁰⁰ BRASIL E SILVA, Vívian. **A necessidade de relativização do princípio da publicidade no processo eletrônico como garantia da dignidade da pessoa humana**. Disponível em <<http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3653.pdf>> Acesso em: 01/06/2020.

Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, **publicidade** e eficiência [...];

Art. 93. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios:

[...]

IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação; (grifou-se).

Denota-se que o princípio da publicidade dos atos processuais está disposto no art. 93, IX, da CRFB. A publicidade, juntamente com a motivação das decisões, disposta no inciso X do art. 93 da CRFB, são normas de observância obrigatória no Estatuto da Magistratura e complementam o direito ao devido processo legal, uma vez que possibilitam o direito ao contraditório e a ampla defesa e atuam como pressupostos para o controle das decisões do Poder Judiciário e a prestação jurisdicional real e efetiva²⁰¹.

Além da Constituição Federal, a publicidade permeia os diversos textos normativos que tratam do processo judicial no Brasil, tais como o Código de Processo Civil, o Processo Penal²⁰² e a Lei do Processo Eletrônico. No que concerne às regras aplicáveis à publicidade dos atos processuais, o CPC estabelece em seu artigo 1º²⁰³, que o processo civil será ordenado, disciplinado e **interpretado** de acordo com os valores e as normas fundamentais dispostos da Constituição Federal.

²⁰¹ PADILHA, Rodrigo. **Direito Constitucional**. 5. ed. Rev. Ampl. Rio de Janeiro: Forense, São Paulo: Método, 2018. p. 805

²⁰² O Código de Processo Penal estabelece em seu art. 792 que “as audiências, sessões e os atos processuais serão, em regra, públicos e se realizarão nas sedes dos juízos e tribunais, com assistência dos escrivães, do secretário, do oficial de justiça que servir de porteiro, em dia e hora certos, ou previamente designados”.

²⁰³ Art. 1º O processo civil será ordenado, disciplinado e interpretado conforme os valores e as normas fundamentais estabelecidos na Constituição da República Federativa do Brasil, observando-se as disposições deste Código.

Ao tratarem da Publicidade dos atos processuais, vale transcrever os ensinamentos de MARINONI, ARENHART e MITIDIERO²⁰⁴:

A administração da Justiça Civil é pública, de modo que o processo civil segue esse mesmo destino. Não só os pronunciamentos judiciais são públicos (art. 93, IX, CF, e 11, CPC), mas também todos os atos processuais que compõem o procedimento destinado à distribuição de justiça. Conjuntamente com o direito ao contraditório e com o dever de fundamentação das decisões, a publicidade forma o núcleo duro de uma administração judiciária permeada por uma ideologia democrática.

O direito à publicidade como norma fundamental do processo civil tem como finalidade caracterizar a administração da justiça no Brasil a partir de uma ideologia democrática, em razão da necessidade de controle de poder pelas partes e pela sociedade em geral.

A sociedade democrática reivindica o pluralismo informativo, o livre acesso e a circulação de informações como regra geral a propiciar o controle. No entanto nem sempre o que é “publicizado” na rede mundial compõe a transparência. Tal fato impele à necessidade de estudar-se em que medida o princípio da publicidade e a transparência da administração devem coexistir com os direitos à intimidade e à privacidade dos cidadãos. A discussão passa, certamente, pela definição do que está na esfera do público ou do privado. O que faz parte da transparência e o que não a integra para se chegar a uma intersecção entre o princípio da publicidade, transparência dos atos da Administração e direito fundamental à proteção de dados pessoais.

3.1.1.1 Restrições à publicidade processual e o segredo de justiça

A publicidade não se trata de um princípio absoluto e poderá ser restringida como forma de garantir direitos fundamentais, a fim de que um bem individual seja protegido. Não obstante, essa limitação deverá ser aplicada com a máxima cautela para evitar que um dos pilares do Estado Democrático de Direito venha a ruir, dando ensejo a atos arbitrários praticados pelo próprio Estado.

²⁰⁴ MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Novo código de processo civil comentado**. 3. ed. rev. ampl. São Paulo: Revista dos Tribunais, 2017. p. 170

Ademais, há atos que não podem ser publicados, por força de lei, o que decorre da circunstância de que nenhum princípio é absoluto, como se observa das regras de sigilo previstas no Estatuto da Criança e do Adolescente e no próprio Estatuto da Advocacia, no caso de sigilo profissional.

Há de se destacar, ainda, que, nas lições de TAVARES²⁰⁵, as restrições à publicidade dos atos processuais devem ser fundamentadas no direito à intimidade do interessado e que a limitação imposta não prejudique o direito público à informação, o que demanda a aplicação dos postulados da ponderação, da concordância prática e da proporcionalidade entre o interesse ao processo público e o direito à informação, de um lado, e o direito à intimidade, de outro, para fazer incidir o princípio mais adequado.

TAVARES²⁰⁶ assevera, ainda, que, ao analisar em cada caso concreto a relativização ao princípio da publicidade, por meio da ponderação se deverá aferir eventual e verdadeiro prejuízo do interesse público à informação.

A publicidade expressa no art. 11 do CPC possui duplo significado, quais sejam: (i) a publicidade geral, que confere a qualquer do povo, como regra, acesso ao conteúdo dos autos do processo; e (ii) a publicidade imediata, que confere, também a todos, o direito de estar presente no momento da prática de atos processuais, ressalvados, logicamente, os casos em há segredo de justiça, na forma estabelecida pelo art. 189 do CPC²⁰⁷.

O art. 189 do CPC, por seu turno, enumera, de forma não exaustiva, os processos que deverão tramitar em segredo de justiça:

Art. 189. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos:

I - em que o exija o interesse público ou social;

²⁰⁵ TAVARES, André Ramos. **Curso de direito constitucional**. 18. ed. São Paulo: Saraiva, 2020. p. 420

²⁰⁶ TAVARES, André Ramos. **Curso de direito constitucional**. p. 421.

²⁰⁷ MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Novo código de processo civil comentado**. p. 174

II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes;

III - em que constem dados protegidos pelo direito constitucional à intimidade;

IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

§ 1º O direito de consultar os autos de processo que tramite em segredo de justiça e de pedir certidões de seus atos é restrito às partes e aos seus procuradores.

§ 2º O terceiro que demonstrar interesse jurídico pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e de partilha resultantes de divórcio ou separação.

Da mesma forma, o Código de Processo Penal estabelece as situações em que a publicidade deverá ser mitigada:

Art. 201. Sempre que possível, o ofendido será qualificado e perguntado sobre as circunstâncias da infração, quem seja ou presuma ser o seu autor, as provas que possa indicar, tomando-se por termo as suas declarações.

[...]

§ 6º O juiz tomará as providências necessárias à preservação da intimidade, vida privada, honra e imagem do ofendido, podendo, inclusive, determinar o segredo de justiça em relação aos dados, depoimentos e outras informações constantes dos autos a seu respeito para evitar sua exposição aos meios de comunicação.

[...]

Art. 792.

[...]

§ 1º Se da publicidade da audiência, da sessão ou do ato processual, puder resultar escândalo, inconveniente grave ou perigo de perturbação da ordem, o juiz, ou o tribunal, câmara, ou turma, poderá, de ofício ou a requerimento da parte ou do Ministério Público, determinar que o ato seja realizado a portas fechadas, limitando o número de pessoas que possam estar presentes.

Conforme se verifica, os atos processuais são públicos, só podendo ser restringida a publicidade dos processos quando exigir o interesse social ou a defesa da intimidade das partes. Correndo, porém, em segredo de justiça, o

direito de consultar os autos, participar de audiências e pedir certidões é restrito às partes e aos seus procuradores, ou a terceiros juridicamente interessados.

3.1.1.2 A Lei do Processo Eletrônico

A chegada da Internet revolucionou, de maneira extraordinária, o processo judicial no Brasil e trouxe grandes discussões acerca da publicidade e seus reflexos nos direitos relativos à personalidade.

Os avanços tecnológicos proporcionados pela Internet e a transformação nas formas de se relacionar na Sociedade Digital, que se tornou hiperconectada aos sistemas de rede e exigiu do Poder Público maior eficiência e transparência em suas entregas, aliados com o preceito constitucional disposto no art. 5º, LXXII, da CRFB²⁰⁸, que garante a todos a razoável duração do processo, administrativo ou judicial, e os meios que garantam sua celeridade, a entrada do Poder Judiciário no mundo digital foi inevitável.

Assim, diante da necessidade de adequação do Poder Judiciário à nova realidade da Sociedade Digital, em 19 de dezembro de 2006 editou-se a Lei nº. 11.419, conhecida como a Lei do Processo Eletrônico, que alterou, por conseguinte, disposições constantes do CPC.

A Lei do Processo Eletrônico, aplicável, indistintamente aos processos civil, penal e trabalhista, dispõe sobre a informatização do processo judicial e disciplina, por meio de seus artigos, as regras de acesso e publicidade das informações e dos dados, destacados a seguir:

Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para **publicação de atos judiciais e administrativos próprios** e dos órgãos a eles subordinados, bem como comunicações em geral.

[...]

²⁰⁸ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

LXXVIII - a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação.

§ 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.

[...]

Art. 8º Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e **acesso por meio de redes internas e externas**.

[...]

Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

[...]

§ 6º Os documentos digitalizados juntados em processo eletrônico estarão disponíveis para acesso por meio da rede externa pelas respectivas partes processuais, **pelos advogados, independentemente de procuração nos autos**, pelos membros do Ministério Público e pelos magistrados, sem prejuízo da possibilidade de visualização nas secretarias dos órgãos julgadores, à exceção daqueles que tramitarem em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)

§ 7º Os sistemas de informações pertinentes a processos eletrônicos devem possibilitar que advogados, procuradores e membros do Ministério Público cadastrados, **mas não vinculados a processo previamente identificado**, acessem automaticamente todos os atos e documentos processuais armazenados em meio eletrônico, **desde que demonstrado interesse para fins apenas de registro**, salvo nos casos de processos em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)

[...]

Art. 12. A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.

[...]

§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a **preservação e integridade dos dados**, sendo dispensada a formação de autos suplementares.

§ 2º Os autos de processos eletrônicos que tiverem de ser remetidos a outro juízo ou instância superior que não disponham de sistema compatível deverão ser impressos em papel, autuados na forma dos arts. 166 a 168 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, ainda que de natureza criminal ou trabalhista, ou pertinentes a juizado especial.

§ 3º No caso do § 2º deste artigo, o escrivão ou o chefe de secretaria certificará os autores ou a origem dos documentos produzidos nos autos, acrescentando, ressalvada a hipótese de existir segredo de justiça, **a forma pela qual o banco de dados poderá ser acessado para aferir a autenticidade das peças e das respectivas assinaturas digitais.**

Art. 13. O magistrado poderá determinar que sejam **realizados por meio eletrônico a exibição e o envio de dados e de documentos** necessários à instrução do processo.

§ 1º Consideram-se cadastros públicos, para os efeitos deste artigo, dentre outros existentes ou que venham a ser criados, ainda que mantidos por concessionárias de serviço público ou empresas privadas, os que contenham informações indispensáveis ao exercício da função judicante.

§ 2º O acesso de que trata este artigo dar-se-á por qualquer meio tecnológico disponível, preferentemente o de menor custo, considerada sua eficiência.

Da análise textual dos dispositivos constantes da Lei do Processo Eletrônico, dentro do contexto apresentado na parte inicial desta pesquisa em relação à evolução da Sociedade da Informação, sua constante evolução tecnológica e o intenso e massivo fluxo de dados na Internet, não é difícil constatar que a publicidade e o acesso à informação, garantidos constitucionalmente, foram amplificados, enquanto o direito à intimidade foi proporcionalmente reduzido.

A facilidade de acesso aos dados processuais e sua reprodução em meios eletrônicos, muito embora confirmem transparência, parecem ter levado a um desequilíbrio das garantias constitucionalmente previstas.

Conforme destacou o advogado especialista em proteção de dados, Danilo Doneda²⁰⁹, os dados judiciais apresentam uma problemática particular

²⁰⁹ TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. **Lei Geral de Proteção de Dados** - Vigência e Implementação. Disponível em: <<https://www.youtube.com/watch?v=MP9bYR2fGMY>>. Acesso em: 18/06/2020.

no Brasil, haja vista o alto grau de transparência e disponibilidade dos dados se comparado a outros países do mundo, transparência esta que foi pensada em uma época em que não se poderia imaginar o alcance atingido pela tecnologia da informação.

Verifica-se que, atualmente, o único gatilho formal para que os dados processuais e documentos correlatos não sejam disponibilizados é por meio da afetação do processo pelo segredo de justiça, que, se aplicado em desmedida, acabará banalizando o instituto.

Em interessante matéria jornalística intitulada “Quem precisa de vazamento de dados que já estão disponíveis no processo eletrônico?”, Felipe Medon discorre justamente sobre a situação retro abordada. Em sua argumentação, destaca que o Brasil está buscando construir uma cultura de proteção aos dados pessoais e as discussões acerca de questões complexas previstas na LGPD, como legítimo interesse de controladores, tratamento automatizado de dados, responsabilidade dos agentes de tratamento, estão em voga no meio jurídico e empresarial²¹⁰.

Contudo, a quantidade de dados e documentos pessoais que instruem os processos judiciais, acessíveis, indiscriminadamente, por advogados e estagiários cadastrados nos sistemas dos Tribunais, ainda que não vinculados a determinados processos, representa uma fragilidade ao direito que se objetiva proteger com a LGPD.

No artigo em questão, há menção, inclusive à propositura de ações judiciais movidas em todo o país sem o consentimento de seus autores, em prática denominada “estelionato judiciário”, em que criminosos utilizam documentos verdadeiros para ingressar com demandas de indenização, e conclui que o ponto em questão não é a possibilidade de acesso, em si, mas sim a

²¹⁰ MEDON, Felipe. **Quem precisa de vazamento de dados que já estão disponíveis no processo eletrônico?** Disponível em: <https://www.jota.info/paywall?redirect_to=https://www.jota.info/opiniao-e-analise/artigos/quem-precisa-de-vazamento-de-dados-que-ja-estao-disponiveis-no-processo-eletronico-14062020>. Acesso em: 15/06/2020.

indagação se realmente há a necessidade de publicação de *todos* os documentos das partes.

3.1.1.3 A problemática da Resolução nº 121 do CNJ

Diante da exposição massificada de dados na Internet e a necessidade de proteção da intimidade das partes no processo, em 05 de outubro de 2010, o CNJ editou a Resolução nº 121, alterada pela Resolução nº 143, de 30 de novembro de 2011, que estabeleceu regras uniformes para a divulgação de dados processuais eletrônicos na rede mundial de computadores e expedição de certidões judiciais.

No que concerne o objeto desta pesquisa, é de grande relevância destacar alguns dos fundamentos da referida Resolução, expressos em seus 07 (sete) *Consideranda*, os quais estão a seguir delineados:

- (i) princípio da publicidade como garantia da prestação de contas da atividade jurisdicional;
- (ii) a necessidade de divulgação dos atos processuais como forma de conferir transparência e garantir o direito de acesso à informação;
- (iii) a garantia do exercício da publicidade restrita ou especial dos atos processuais;
- (iv) a exigência de tratamento uniforme da divulgação dos atos processuais judiciais no âmbito de toda a magistratura nacional, preservando o direito à intimidade, à vida privada, à honra e à imagem das pessoas;
- (v) as dificuldades enfrentadas pela justiça brasileira em razão da estigmatização das partes pela disponibilização na rede mundial de computadores de dados concernentes aos processos judiciais que figuraram como autoras ou rés em ações criminais, cíveis ou trabalhistas;

- (vi) a necessidade de consolidação de um padrão nacional de definição dos níveis de publicidade das informações judiciais;
- (vii) o disposto no art. 11, § 6º, da Lei 11.419/2006, estabelece que os documentos eletrônicos “somente estarão disponíveis para acesso por meio da rede externa para suas respectivas partes processuais e para o Ministério Público, respeitado o disposto em lei para as situações de sigilo e de segredo de justiça”;

Em seu art. 1º, a Resolução 121 define que a consulta aos dados básicos dos processos judiciais será disponibilizada na Internet e assegurou o direito de acesso a informações processuais a **toda e qualquer pessoa**, independentemente de cadastro ou demonstração de interesse, salvo no caso de processos em sigilo ou segredo de justiça.

Os dados básicos do processo considerados de livre acesso estão descritos no art. 2º da Resolução e compreendem:

Art. 2.º Os dados básicos do processo de livre acesso são:

I – número, classe e assuntos do processo;

II – nome das partes e de seus advogados;

III – movimentação processual;

IV – inteiro teor das decisões, sentenças, votos e acórdãos.

O acesso ao conteúdo completo do processo eletrônico é reservado ao advogado cadastrado e habilitado nos autos, às partes cadastradas e ao Ministério Público. Ressalvados os casos em segredo de justiça, os sistemas devem possibilitar, por sua vez, que advogados, procuradores e membros do Ministério Público, cadastrados mas não vinculados a processo previamente identificado, acessem automaticamente todos os atos e documentos processuais, salvo nos casos de segredo de justiça, devendo ser registrado cada acesso efetuado, conforme prevê o art. 3º da Resolução.

Contudo, com a simples inclusão dos dados básicos de livre acesso é possível obter a informação se determinada pessoa é parte em alguma demanda judicial, o que, por si só, choca-se com o fundamento da referida resolução no tocante à estigmatização das partes pela disponibilização na rede mundial de computadores de dados concernentes aos processos judiciais.

Insta, ainda, reproduzir, na íntegra, os artigos da Resolução 121 a seguir delineados, que definem as regras para as consultas públicas realizadas nos sistemas dos tribunais:

Art. 4.º As consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, devem permitir a localização e identificação dos dados básicos de processo judicial segundo os seguintes critérios:

I – número atual ou anteriores, inclusive em outro juízo ou instâncias;

II – nomes das partes;

III – número de cadastro das partes no cadastro de contribuintes do Ministério da Fazenda;

IV – nomes dos advogados;

V – registro junto à Ordem dos Advogados do Brasil.

§ 1º. A consulta ficará restrita às seguintes situações: (Redação dada pela Resolução nº 143, de 30.11.2011)

I - ao inciso I da cabeça deste artigo, nos processo criminais, após o trânsito em julgado da decisão absolutória, da extinção da punibilidade ou do cumprimento da pena; (**Redação dada pela Resolução nº 143, de 30.11.2011**)

II - aos incisos I, IV e V da cabeça deste artigo, nos processo sujeitos à apreciação da Justiça do Trabalho. (**Redação dada pela Resolução nº 143, de 30.11.2011**)

Pela análise conjunta do art. 1º com o art. 4º, observa-se que, dentre os demais critérios para a consulta aos dados básicos do processo na Internet, é possível efetuar a consulta e o acesso aos processo pelo **nome das partes**, o que possibilita a, qualquer pessoa, em qualquer lugar do mundo, saber se alguém é parte em processo judicial, com exceção das ações em trâmite perante a

Justiça do Trabalho, dos processos criminais e em casos de sigilo e segredo de justiça.

O art. 5º, no entanto, ressalva a consulta às bases de decisões judiciais pelo nome das partes:

Art. 5.º A disponibilização de consultas às bases de decisões judiciais impedirá, quando possível, a busca pelo nome das partes.

[...]

Art. 7º. A certidão judicial deverá conter, em relação à pessoa a respeito da qual se certifica:

I - nome completo;

II – o número do cadastro de contribuinte no Ministério da Fazenda;

III – se pessoa natural:

a) nacionalidade;

b) estado civil;

c) números dos documentos de identidade e dos respectivos órgãos expedidores;

d) filiação; e

d) o endereço residencial ou domiciliar.

[...]

É possível inferir que os artigos 1º e 4º da Resolução 121 do CNJ discrepam do contido no quarto Considerando, segundo assevera RUARO²¹¹, “na medida em que este apresenta um sopesamento entre o dever de transparência da Administração Pública combinado com o direito à informação e com os direitos fundamentais da intimidade e privacidade”, uma vez que passou a permitir a consulta de processos judiciais na Internet pelo nome das partes, sem a necessidade de prévio cadastramento.

²¹¹ RUARO, Regina Linden; LIMBERGER, Têmis. **Administração pública e novas tecnologias: o embate entre o público e o privado - análise da Resolução 121/2010 do CNJ.** p. 126

Já em relação ao fundamento constante do quinto Considerando, muito embora o Poder Judiciário deva observar os ditames constitucionais do direito à informação, regulamentado pela Lei de Acesso à Informação à qual, também, está sujeito à possibilidade de cruzamento dos dados armazenados, ainda mais acentuada pelas tecnologias de *Big Data* no contexto social contemporâneo, leva à estigmatização das partes, já que seus dados pessoais indisponíveis permanecem em constante exposição na Internet, extrapolando as razões de sua disponibilização, que é de dar transparência aos atos judiciais e facilitar o acompanhamento das demandas pelas partes e seus advogados.

A publicidade dos atos processuais, inquestionavelmente, oferece maior segurança jurídica ao que é realizado pelo Poder Judiciário, sendo uma inestimável garantia do indivíduo no tocante ao exercício jurisdicional.

Depreende-se, assim, que a publicidade é uma garantia democrática, em que se permite a participação da população como forma de fiscalizar a atuação dos agentes públicos. Segundo BOBBIO²¹², "pode-se definir a democracia das maneiras as mais diversas, mas não existe definição que possa deixar de incluir em seus conotativos a visibilidade ou transparência do poder".

Contudo, nenhuma época como a que hoje se vive clamou tanto o respeito e a proteção à dignidade da pessoa humana, tendo em vista a facilidade da violação da intimidade dos seres humanos, conforme amplamente abordado no primeiro capítulo deste trabalho. Em assim sendo, entende-se que a publicidade de dados pessoais constantes das informações processuais devem ser limitadas como forma de promoção do supracitado fundamento, agora regulamentado por meio da LGPD.

Neste ponto, cumpre salientar o a fala do juiz do Tribunal de Justiça do Estado de São Paulo, Fernando Antonio Tasso, para quem:

A Lei de Acesso à Informação (12.527/2011) visou tornar públicos dados produzidos pela entropia da máquina pública, mas há uma categoria de dados de que não podemos dispor, porque não

²¹² BOBBIO, Norberto. **A era dos direitos**. p. 70

somos os titulares, somos os guardiões. A LGPD nos atribuiu a missão de zelar por esses dados [...]²¹³

Entende-se que este será um dos grandes desafios do Poder Judiciário, mormente em relação ao estabelecimento de uma cultura institucional capaz de imbuir em seus órgãos a compreensão de que os princípios da publicidade e da transparência se referem exclusivamente às suas atividades, decorrentes do dever de prestar contas e garantir o controle dos atos administrativos pela Sociedade, e não englobam a disponibilização de dados pessoais confiados a seus cuidados, salvo mediante critérios rigorosamente definidos.

3.1.2 O princípio da dignidade humana como limitador da publicidade

Não se pode olvidar, ainda, que o direito processual está subordinado aos princípios constitucionais gerais, dentre os quais se ressalta o princípio da dignidade humana, expresso no art. 1º, III, da CRFB:

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

[...]

III - a dignidade da pessoa humana;

Segundo NERY JUNIOR²¹⁴, o respeito e a proteção da dignidade humana como dever fundamental do Estado Constitucional constitui a premissa para todas as questões jurídico-dogmáticas particulares. O autor assevera que a dignidade humana “constituiu *norma fundamental do Estado*, porém é mais do que isso: ela fundamenta também a sociedade constituída e eventualmente a ser constituída” e sustenta que a dignidade humana é resistente à ponderação.

No que concerne o limite imposto pela dignidade humana ao princípio da publicidade, o CPC reproduziu a norma constitucional em seu art. 8º.

²¹³ Disponível em <https://epm.tjsp.jus.br/Noticias/noticia/56470?pagina=1>. Acesso em 23/07/2020.

²¹⁴ NERY JUNIOR, Nelson. **Princípios do processo na constituição federal**. 12 ed. rev. atual. ampl. São Paulo: Editora Revista dos Tribunais, 2016. p. 105

Para melhor compreensão, utiliza-se das lições de MARINONI, ARENHART e MITIDIERO²¹⁵, para quem:

O art. 8, primeira parte, do CPC, refere que o juiz ao aplicar o ordenamento jurídico deve resguardar e promover a dignidade da pessoa humana - a qual constitui sabidamente um dos fundamentos do Estado Constitucional (art. 1.º, III, CF). Em primeiro lugar, **a dignidade da pessoa humana determina a compreensão do processo civil como um meio para tutela dos direitos**. Vale dizer: o processo civil não pode ser visto como um instrumento a serviço do Estado, como um instrumento que não se encontre orientado à realização dos fins da pessoa humana. Em outras palavras, o processo civil serve para realização dos direitos e para orientação das pessoas a respeito do significado do direito. Em segundo lugar, **a dignidade da pessoa humana conecta-se com o direito à liberdade e à autonomia privada, o que explica a necessidade de respeito, dentro dos limites constitucionais e legais, aos negócios processuais realizados entre as partes** (art. 190, CPC) e constitui estímulo à realização de calendários processuais entre o juiz e as partes como instrumento para eficiente gestão do tempo no processo civil (art.191, CPC). Em terceiro lugar, **a dignidade da pessoa humana veda a transformação das partes em objeto da atividade jurisdicional**. E por essa razão que a dignidade da pessoa humana tem estreita ligação com o direito de participação das partes na construção dos provimentos jurisdicionais - isto é, na previsão do direito ao contraditório como direito de influência (arts. 9 e 10, CPC) e o dever de fundamentação como dever de debate (arts. 11e489, §§ 1.0 e 2.0 , CPC). **O JUIZ ao aplicar o ordenamento jurídico e ao conduzir o processo deve resguardar e promover a dignidade da pessoa humana, o que significa encarar o processo como um meio para tutela dos direitos, respeitar a liberdade das partes nos seus espaços de autodeterminação** e adotar o contraditório como método de trabalho.

Contudo, apesar de sua essencialidade e do comparecimento maciço em diversos dispositivos legais, mostra-se uma árdua tarefa obter uma conceituação clara acerca da dignidade da pessoa humana.

BARROSO²¹⁶ expõe que a compreensão atual de dignidade humana está embasada no pressuposto de que cada ser humano possuiu um valor intrínseco e desfruta de uma posição especial no universo, tendo como marcos a

²¹⁵ MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Novo código de processo civil comentado**. p. 170

²¹⁶ BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**. p. 14

tradição judaico-cristã, o Iluminismo e o período imediatamente posterior ao fim da Segunda Guerra Mundial. Assim, a dignidade humana foi incorporada ao discurso jurídico em razão de ter sido incluída em diferentes tratados e documentos internacionais – como na Declaração Universal dos Direitos do Homem (1945) e na Convenção Americana de Direitos Humanos (1978), tratadas no Primeiro Capítulo –, assim como em diversas constituições nacionais.

Segundo discorre o Ministro, a dignidade é compreendida como o alicerce de todos os direitos fundamentais e como fonte de seu conteúdo essencial. Em sendo assim, ela não deve ser considerada um direito em si. Caso o fosse, ela necessariamente precisaria ser ponderada com outros direitos fundamentais. Já como princípio, ela pode precisar ser ponderada com outros princípios ou metas coletivas²¹⁷.

Segundo assevera BARROSO²¹⁸, cumpre destacar que a ética kantiana, baseada na ideia de dignidade humana e construída nas noções de razão e dever e na noção da autonomia, tornou-se parte crucial dos estudos sobre a dignidade humana. De extrema importância para o contexto deste trabalho é a filosofia ética de Kant de que todo homem é um fim em si mesmo e **não deve ser instrumentalizado por projetos alheios** e de que os seres humanos não têm preço nem podem ser substituídos por serem dotados de um valor intrínseco absoluto, a que se dá o nome de dignidade.

Ponto crucial para o desafio ora apresentado é, portanto, identificar se a LGPD, apoiada no limite constitucional da dignidade humana, imposto à publicidade dos atos processuais, produzirá efeitos e ensejará a alteração de procedimentos relacionados a esta temática.

Nesse sentido, repisa-se que nenhum direito fundamental é absoluto, de modo que, em havendo choque entre dois ou mais, tem-se a

²¹⁷ BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**. p. 67-68

²¹⁸ BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**. p. 69

necessidade de relativização. Dos ensinamentos de CANOTILHO²¹⁹ extrai-se que:

Uma notável mutação de sentido da reserva da lei verifica-se no esquema relacional **lei-direitos fundamentais**. Inicialmente, a reserva de lei compreendia-se como “reserva da liberdade e da propriedade dos cidadãos”. A reserva geral de lei tinha como intenção primária defender os dois direitos básicos do indivíduo – a liberdade e a propriedade.

No actual contexto constitucional este esquema deixou de ser uma construção aceitável. Em primeiro lugar, a reserva de lei no âmbito dos direitos fundamentais (máxime no âmbito dos direitos, liberdades e garantias) dirige-se contra o próprio legislador: só a lei pode restringir direitos, liberdades e garantias, mas a lei só pode estabelecer restrições se observar os requisitos constitucionalmente estabelecidos (cfr. *Supra*). Daí a relevância dos direitos fundamentais como elemento determinante do âmbito da reserva de lei. (grifos no original)

A discussão quanto à exposição da esfera íntima e privada do indivíduo por meio de uma simples busca na Internet não é nova.

Aliado ao direito à intimidade e à proteção de dados pessoais, os riscos oriundos da exposição excessiva dos indivíduos em demandas judiciais fazem com que seja necessário relativizar o princípio da publicidade dos atos processuais, ao mesmo tempo em que garante a preservação de sua função constitucional, conforme destacam CINTRA, DINAMARCO e PELLEGRINI²²⁰, para quem “toda precaução há de ser tomada contra a exasperação do princípio da publicidade. Os modernos canais de comunicação de massa podem representar um perigo tão grande como o próprio segredo”.

Hodiernamente verifica-se que, apesar das tentativas normativas de regular o acesso a dados processuais meio da Internet, inclusive por meio de Resoluções do CNJ, a disponibilização indiscriminada, nos sítios dos Tribunais de Justiça, de nomes de pessoas envolvidas em processos judiciais tem revelado

²¹⁹ CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra, Portugal: Edições Almedina, 2003.p. 729

²²⁰ CINTRA, Antonio Carlos de Araújo, GRINOVER, Ada Pellegrini, DINAMARCO, Cândido Rangel. **Teoria Geral do Processo**. 21. ed. São Paulo: Malheiros, 2004. p. 70

para toda a sociedade (uma vez que o acesso à internet é livre para todos) situações que colocam os indivíduos em posições constrangedoras.

3.1.3 Controle de acesso aos dados processuais, direito à informação e o princípio da publicidade: uma revisitação à luz da LGPD

A Portaria Nº 63, de 26 de abril de 2019, do CNJ, instituiu o Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais, em especial, quando se trata de sua utilização para fins comerciais.

O CNJ noticiou que editará uma norma para disciplinar o acesso a dados pessoais extraídos de sistemas de tribunais, em especial quando as informações são usadas para fins comerciais. A preocupação principal, segundo Toffoli, é com “a cautela que se deve guardar quanto ao acesso irrestrito a informações relevantes sobre o cidadão”²²¹. Ainda, o ministro disse que consultas processuais feitas por empresas, desde *startups* até grandes grupos econômicos, sobrecarregam os sistemas do Judiciário e aumentam o gasto público com o setor de tecnologia da informação.

A discussão não se cinge à consulta de meros andamentos processuais. É foco de preocupação e atenção, com ressalva a processos em segredo de Justiça, o amplo e irrestrito acesso aos hábitos do indivíduo, sua privacidade patrimonial, suas preferências de toda ordem. Segundo a reportagem veiculada no editorial JOTA, Toffoli declarou: “*Trata-se da vida de todos nós*”.

No mesmo pronunciamento, o Presidente do STF ressaltou, também, que os contribuintes brasileiros acabam pagando a conta das crescentes consultas empresariais aos sistemas de informação, que levam a despesas cada vez maiores com ampliação das áreas de TI dos tribunais.

Contudo, o fato de os tribunais terem se tornado digitais, o que trouxe benefícios indiscutíveis aos administradores da Justiça e aos

²²¹ CNJ fará norma sobre acesso a dados pessoais extraídos de tribunais, diz Toffoli. Disponível em: <<https://www.jota.info/justica/cnj-norma-dados-pessoais-tribunais-27052019>> Acesso em: 01/06/2020.

jurisdicionados, a Era Digital e sua tecnologia de *Big Data* fazem emergir novas discussões no cenário jurídico relacionadas aos limites da publicidade de modo aberto na Internet.

É inegável que a publicação de dados em massa proporcionada pelas novas tecnologias traz à tona a invasão à esfera íntima e privada dos indivíduos causadas pela simples busca de um nome no Google.

A título de exemplificação, expõe-se a seguinte situação fictícia: Luiz conheceu Ana e decidiu pesquisar seu nome na Internet. Surgiram algumas páginas de resultados e, dentre dados de suas redes sociais, participação societária em empresas e, inclusive, artigos publicados, havia, também, 03 (três) processos judiciais indexados: um relacionado a danos morais, uma execução fiscal e uma ação penal que continham, na própria página do buscador de Internet, além dos dados do processo e do nome completo de Ana, os nomes dos pais de Ana, sua data de nascimento e seu endereço, tendo sido oferecido ao Luiz a possibilidade de acompanhar o andamento do processo através do simples cadastro de e-mail no *site* de busca, bem como o de acessar as informações publicadas no Diário Oficial, pelo valor R\$ 3,90 (três reais e noventa centavos) por ato pesquisado²²².

O buscador que raspou²²³ os dados processuais da execução fiscal e da ação de danos morais direcionou Luiz aos sítios eletrônicos dos respectivos Tribunais de Justiça, sítios que Luiz sequer conhecia ou havia tido prévio interesse em conhecer, e lá ele teve acesso aos dados do processo.

Embora essa não tenha sido a razão pela qual Luiz decidiu consultar o nome de Ana na Internet, a existência de demanda judicial, inclusive em matéria

²²² DOinet Brasil Dados Públicos. Consultas a bases de dados. Disponível em https://www.doinet.com.br/bdpv2/pesquisa_v2.aspx. Acesso em 23/07/2020.

²²³ A raspagem de dados (*data scraping*) é uma técnica por meio da qual um programa de computador extrai dados gerados por outros programas ou computadores, dados estes que, via de regra, não estão disponíveis para serem baixados e reutilizados para fins não autorizados e são protegidos por tecnologia específica. Os *scrapers* (raspadores), por outro lado, estão interessados em obter dados do site, independentemente de qualquer tentativa de limitar o acesso. Como resultado, existe um jogo de gato e rato entre o Web Scraping e várias estratégias de proteção de conteúdo, com cada um tentando superar o outro. Disponível em <https://juristas.com.br/foruns/topic/o-que-e-data-scraping/>. Acesso em 20/06/2020.

criminal, foi o suficiente para que o interesse deixasse de existir e Luiz nunca mais procurou Ana.

Agora, será considerado o mesmo caso fictício, mas quem realiza a busca pelo nome de Ana são robôs (*bots*), os mesmos utilizados anteriormente, porém, agora, contratados e/ou desenvolvidos por empresas privadas e para fins econômicos, tais como bancos, fornecedores de cartão de crédito, recrutadores e empresas que realizam a análise reputacional de todas as pessoas com quem realizam qualquer tipo de negócio, análises estas feitas de forma automatizada por sistemas que respondem a padrões previamente programados para “bloquear” indivíduos que apresentem resultados de busca considerados desabonadores.

Assim, efetuada a consulta na Internet, na velocidade de um *click*, Ana terá seu cartão de crédito ou pedido de financiamento negado, perderá o direito de disputar por uma vaga de emprego ou terá problemas para realizar negócios com determinadas empresas, independentemente de os processos virem a ser julgados procedentes ou não porque, em sua maioria, os *bots* não fazem análise de mérito, mas tão-somente indicam que Ana é parte em demandas judiciais, o que é suficiente para macular sua reputação.

Esses buscadores se cobrem no manto do “banco de dados público” e acabam atentando contra a dignidade das pessoas.

Imprescindível destacar que, anteriormente à informatização do Poder Judiciário, para saber se alguém tinha pendências criminais, por exemplo, era preciso requisitar uma certidão de antecedentes. Isso requeria o comparecimento do interessado a determinado órgão público, o pagamento de taxa específica e a apresentação de diversas informações da pessoa cujas informações se deseja. Ao se pensar a publicidade dos atos processuais pelo constituinte originário, não se poderia imaginar o alcance das tecnologias de informação e comunicação atualmente existentes e que, frisa-se, ainda estão em desenvolvimento.

Verifica-se a mesma tendência nos Estados Unidos da América, onde organizações civis, tais como a EPIC – Electronic Privacy Information Center²²⁴, têm peticionado a cortes estaduais com vistas a estabelecer procedimentos para garantir a proteção dos dados pessoais relacionados em processos judiciais, com restrição de acesso remoto pela Internet. Um dos pareceres formulados, direcionado à Suprema Corte do Estado da Florida, a EPIC afirma que, embora seja uma grande apoiadora do amplo acesso à informação governamental, a presença de informações pessoais nas bases de dados públicas fragiliza a privacidade das pessoas e destaca sua preocupação principal:

The very purpose of public records – the ability of the individual to learn about the government – is turned on its head when the records include excessive personal information. Instead of being citizens' window into government activities, public records are giving the government, law enforcement, and data brokers a window into our daily lives. Without privacy protections, court and other public records will be commodified for commercial purposes unrelated to government oversight.

Além dessa inversão do objetivo do acesso à informação pública acima descrito, a organização destacou, ainda no ano de 2006²²⁵, exatamente o que se tem evidenciado na atual *Data Economy*: os *data brokers* se utilizam do manto da “informação disponível em bancos de dados públicos” para negociar no mercado dados pessoais, inclusive dados pessoais sensíveis, sem se obrigarem a obter o consentimento dos titulares, tampouco de observar regras mínimas de proteção à privacidade, tais como a de informar os titulares dos dados no caso de roubo ou perda dessas informações. Em outra recomendação²²⁶ direcionada ao Judiciário Federal dos Estados Unidos, a EPIC demandou mudanças nas regras procedimentais, com vistas a blindar as informações contidas nos sistemas dos Tribunais do acesso feito por corretores comerciais, que garimpam essas informações e depois as revendem no mercado. Segundo a organização civil, os arquivos dos Tribunais se tornaram combustíveis para a construção de dossiês

²²⁴ EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/>>. Acesso em: 18/08/2020

²²⁵ EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/>>. Acesso em: 18/08/2020

²²⁶ EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/frcpcom21506.html>>. Acesso em: 18/08/2020

sobre os cidadãos americanos e o Poder Judiciário deve aceitar a responsabilidade de proteger os dados de sua má utilização e concluiu que a minimização é a abordagem mais importante ao se tratar dos riscos à privacidade associados aos bancos de dados públicos.

Os danos à privacidade dos indivíduos causados pelo uso indevido de seus dados pessoais que circulam na Internet foram os propulsores éticos para a edição de leis de proteção de dados por todo o globo, como visto no primeiro capítulo desta pesquisa. Por sua vez, os Estados Unidos, que ainda relutam em adotar uma legislação federal, está na contramão de diversos de seus estados nacionais que já editaram leis de proteção de dados pessoais, sendo a mais proeminente delas a CCPA – California Consumer Privacy Act²²⁷. Nota-se, contudo, que, diferentemente da maioria das nações, inclusive do Brasil, que adotou um modelo de proteção geral de proteção de dados, aplicável a todos os segmentos, as leis adotadas pelos estados americanos, como a CCPA, que protege os dados de consumidores, continuam setORIZADAS.

Assim, a LGPD contribui fortemente para a rediscussão de conflitos entre os direitos fundamentais à intimidade, à informação e à publicidade dos atos públicos, bem como da dicotomia: interesse individual e supremacia do interesse coletivo.

Como foi visto no capítulo anterior, a LGPD, à qual se submete, também o Poder Judiciário, vai de encontro com a limitação constitucional à publicidade dos atos processuais exercida pelo princípio da dignidade humana.

Recapitulando-se, a autodeterminação informativa, intrinsicamente conectada com o conceito de autonomia e que quer dizer o direito exercido pelo próprio indivíduo de controle sobre suas informações pessoais, evoluiu para o direito de proteção aos dados pessoais. O Estado, por sua vez, de tutelar e garantir a efetividade desse direito, considerado como fundamental em diversas

²²⁷ STATE OF CALIFORNIA. Civil Code. **California consumer privacy act of 2018**. [1798.100 - 1798.199] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.) Disponível em: <http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>_Acesso em: 17/08/2020.

nações e objeto da Proposta de Emenda à Constituição nº 17, de 22 de maio de 2019²²⁸, para que assim seja reconhecido no Brasil.

Entretanto, independentemente de a proteção aos dados pessoais vir a ser expressamente enumerada na CRFB como um direito fundamental, essencialmente vinculado à intimidade e ao princípio da dignidade da pessoa humana, ambos já garantidos constitucionalmente, e, diante do risco em potencial associado à subjetividade das pessoas e, também ao controle e abuso de poder de mercado no âmbito do Informacionalismo, o fato é que o tratamento dos dados pessoais passará a ser regulamentado pelas regras previstas na LGPD, o que, por certo, trará uma maior uniformização no entendimento jurisprudencial sobre a matéria.

É necessário compreender, com base nas disposições legais constantes de todos os instrumentos normativos que disciplinam este tema, que a publicidade, constitucionalmente garantida e regulamentada por leis ordinárias e resoluções do CNJ, é **do ato processual em si** e não das informações pessoais das partes do processo.

A propósito, o art. 17 da LGPD determina que toda pessoa natural tem assegurada a titularidade de seus dados pessoais. Isto significa dizer que os dados pessoais dos litigantes e terceiros envolvidos em processo judicial não são disponíveis, sendo-lhes assegurada, ademais, autodeterminação informativa, nos moldes do inciso II, do art. 2º da LGPD.

Não é razoável permitir que o exercício do direito garantido de acesso à Justiça possa trazer prejuízos concretos aos litigantes por terem seus dados pessoais expostos publicamente, inclusive para quem sequer tem interesse legítimo em saber se determinada pessoa é parte em processos judiciais. Essa proteção encontra-se disposta, inclusive, no art. 21 da LGPD, o qual dispõe que

²²⁸ A PEC nº 17 de 2019 propõe que inciso XII do art. 5º da CRFB passe a vigor com a seguinte redação “XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

os dados pessoais referentes ao exercício regular de direitos pelo Titular não podem ser utilizados em seu prejuízo.

Como já visto, danos concretos são vivenciados diariamente por indivíduos que têm suas informações pessoais e de foro íntimo expostas na Internet, sejam eles danos ao crédito, ao trabalho, como também podem se tornar vítimas de fraudes decorrentes do furto de dados ou até mesmo da própria identidade, que trazem enormes prejuízos às vítimas.

Pode-se observar uma clara violação da intimidade e privacidade dos jurisdicionados que têm, em muitos casos, sua vida invadida, em questão de segundos, por qualquer pessoa que tenha acesso ao site do Tribunal violando estes direitos assegurados pela Constituição Federal e, agora, também pela LGPD.

Um bom norteador ao Poder Judiciário nas adequações práticas que precisará realizar para estar *compliant* com a LGPD é o conjunto de regras conhecido como Carta de Heredia.

Em julho de 2003, o Instituto de *Investigación para la Justicia Argentina*, com o apoio da Corte Suprema de Justiça da Costa Rica, e patrocínio da *International Development Research Centre* do Canadá, reuniu em Heredia, na Costa Rica, representantes de diversos países da América Latina para discutir o tema “Sistema Judicial e Internet”, com a finalidade de analisar as vantagens e dificuldades dos *sites* dos poderes judiciais na rede, os programas de transparência e a proteção dos dados pessoais.

Conforme informam GREGÓRIO e PAIVA²²⁹, participaram daquele evento diversos magistrados de Cortes Superiores de vários países da América do Sul e Central, e foram desenvolvidas diversas teses e exposições que culminaram na formulação da Carta de Heredia, que estabelece as regras

²²⁹ GREGÓRIO, Carlos; PAIVA, Mário. **Proteção de dados pessoais no âmbito judicial** (2005). Disponível em: <https://www.jornaljurid.com.br/doutrina/civil/protecao-de-dados-pessoais-no-ambito-judiciala-stylemso-footnote-idftn1-href_ftn1-name_ftnref1-titlespan-classmsofootnotereferencespana>. Acesso em: 13/03/2020.

mínimas a serem adotadas pelos órgãos responsáveis pela difusão de informação judicial na Internet, a seguir transcritas:

Regra 1. A finalidade da difusão em Internet das sentenças, e despachos judiciais será: (a) O conhecimento da informação jurisprudencial e a garantia da igualdade diante da lei; (b) Para procurar alcançar a transparência da administração da justiça.

Regra 2. A finalidade da difusão em Internet da informação processual será garantir o imediato acesso das partes, ou dos que tenham interesse legítimo na causa, a seus andamentos, citações ou notificações.

Regra 3. Será reconhecido ao interessado o direito de opor-se, mediante petição prévia e sem gastos, em qualquer momento e por razões legítimas próprias de sua situação particular, a que os dados que lhe sejam concernentes sejam objeto de difusão, salvo quando a legislação nacional disponha de modo diverso. Em caso de decidir-se, de ofício ou a requerimento da parte, que dados de pessoas físicas ou jurídicas estejam ilegitimamente sendo difundidos, deverá ser efetuada a exclusão ou retificação correspondente.

Regra 4. Em cada caso os motores de busca se ajustarão ao alcance e finalidades com que se difunde a informação judicial.

Regra 5. Prevalecem os direitos de privacidade e intimidade, quando tratados dados pessoais que se refiram a crianças, adolescentes (menores) ou incapazes; ou assuntos familiares; ou que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a participação em sindicatos; assim como o tratamento dos dados relativos à saúde ou à sexualidade; ou vítimas de violência sexual ou doméstica; ou quando se trate de dados sensíveis ou de publicação restrita segundo cada legislação nacional aplicável ou tenham sido considerados na jurisprudência emanada dos órgãos encarregados da tutela jurisdicional dos direitos fundamentais. Neste caso, se considera conveniente que os dados pessoais das partes, coadjuvantes, aderentes, terceiros e testemunhas intervenientes sejam suprimidos, anonimizados ou inicializados, salvo se o interessado expressamente o solicite e seja pertinente de acordo com a legislação.

Regra 6. Prevalecem a transparência e o direito de acesso à informação pública quando a pessoa concernente tenha alcançado, voluntariamente, o caráter de pública e o processo esteja relacionado com as razões de sua notoriedade. Sem embargo, consideram-se excluídas as questões de família ou aquelas em que exista uma proteção legal específica. Nestes casos, poderão manter-se os nomes das partes na difusão da informação judicial, mas se evitarão os domicílios ou outros dados identificatórios.

Regra 7. Em todos os demais casos se buscará um equilíbrio que garanta ambos os direitos. Este equilíbrio poderá instrumentalizar-se: (a) nas bases de dados de sentenças, utilizando motores de busca capazes de ignorar nomes e dados pessoais; (b) nas bases de dados de informação processual, utilizando como critério de busca e identificação o número único do caso.

Regra 8. O tratamento dos dados relativos a infrações, condenações penais ou medidas de segurança somente poderá efetuar-se sob controle da autoridade pública. Somente poderá ser realizado um registro completo de condenações penais sob o controle dos poderes públicos.

Regra 9. Os juízes, quando redijam suas sentenças, despachos e atos, farão seus melhores esforços para evitar mencionar fatos inócuos ou relativos a terceiros, buscarão somente mencionar os fatos ou dados pessoais estritamente necessários para os fundamentos de sua decisão, tratando de não invadir a esfera íntima das pessoas mencionadas. Excetua-se da regra anterior a possibilidade de consignar alguns dados necessários para fins meramente estatísticos, sempre que sejam respeitadas as regras sobre privacidade contidas nesta declaração. Igualmente se recomenda evitar os detalhes que possam prejudicar a pessoas jurídicas (morais) ou dar excessivos detalhes sobre os *modi operandi* que possam incentivar alguns delitos. Esta regra se aplica, no pertinente, aos editais judiciais.

Regra 10. Na celebração de convênios com editoriais jurídicos deverão ser observadas as regras precedentes.

As Regras de Heredia, ainda que criadas no ano de 2003, contêm disposições relevantes no tocante à proteção de dados no processo judicial e sua aplicabilidade no momento atual não deve ser desconsiderada.

Pelo exposto, identifica-se que a busca livre realizada nos *sites* de tribunais, apesar de garantir publicidade e o acesso à informação, acaba, também, trazendo sérios prejuízos à intimidade e privacidade daqueles que procuram as cortes judiciais. Por isso a necessidade da adequação dos motores de busca vedando em alguns casos os tipos de busca que trazem prejuízo à intimidade e privacidade do cidadão e, em outros, resguardando o anonimato dos litigantes.

Entende-se, portanto, que os processos judiciais que versem sobre dados pessoais sensíveis deverão correr em segredo de justiça. Já os dados pessoais, sejam eles sensíveis ou não, deverão ser restringidos e passar por alguma forma de anonimização em publicações.

Anteriormente à edição da LGPD, o CNJ já havia consolidado seu entendimento de que a publicidade dos atos processuais não autoriza o acesso irrestrito por terceiros a todo o conteúdo dos processos eletrônicos, tendo como fundamentos a Lei do Processo Eletrônico (Lei 11.419/1996) e as Resoluções do CNJ 121/2010 e 185/2013, que regulamentaram o acesso aos processos eletrônicos, conforme se observa em decisão²³⁰ proferida pela Conselheira Daldice Santana, na qual esclarece que o processo é público, mas alguns documentos contêm dados pessoais que não estão incluídos nos dados básicos do processo e que, somente esses, seriam disponíveis para consulta irrestrita. De acordo com a Conselheira, há níveis distintos de perfil de acesso ao processo em razão da inexistência de interesse público na divulgação de dados que revelam a vida privada das pessoas e destaca o seguinte:

Para a realização de busca por precedentes judiciais, assim como para fins de pesquisa acadêmica ou para mero acompanhamento das atividades desenvolvidas pelo Poder Judiciário, é suficiente a consulta ao inteiro teor das decisões, mesmo porque todas elas trazem consigo o relatório narrativo acerca das alegações das partes e dos atos processuais praticados até o deslinde do feito.

A referida decisão fundamentou-se, ainda, na Resolução 215/2015 que regulamenta a Lei de Acesso à Informação (Lei 12.527/2011) no âmbito do Poder Judiciário e que ressalva o acesso de dados referentes à intimidade das partes, por dizerem respeito à esfera privada, destacando-se artigo 8º, § 1º; artigo 9º[3], caput e § 2º; artigo 25, § 5º, inciso III, e artigo 32, inciso I.

O que se verifica, porém, é que, muito embora haja a restrição de acesso somente aos dados básicos do processo com a finalidade de resguardar a intimidade e a privacidade das partes do processo, fato é que as decisões judiciais disponíveis para acesso irrestrito, notadamente os acórdãos publicados, contêm toda a sorte de dados pessoais.

²³⁰ BRASIL. **Conselho Nacional de Justiça**. RECURSO ADMINISTRATIVO NO PEDIDO DE PROVIDÊNCIAS 0005957-84.2015.2.00.0000, Disponível em: <<https://www.cnj.jus.br/Infojuris12/Jurisprudencia.seam.jsessionid=10E06D0D34D48B1AF111DD78A300FD16?jurisprudenciaIdJuris=48192&indiceListaJurisprudencia=24&firstResult=5450&tipoPesquisa=BANCO>> Acesso em: 15/11/2019.

Outro ponto a se destacar é que, para que um cidadão que não seja parte do processo tenha acesso aos dados básicos do processo, deverá efetuar consulta no *site* do tribunal correspondente e comprovar tratar-se de uma pessoa natural através de tecnologia de verificação, onde ficarão registrados os acessos efetuados, o que é muito mais seguro e restrito do que a disseminação das informações por meio de buscadores da Internet.

Vale discorrer sobre o que dispõe a Lei de Acesso à Informação, que regulamentou o princípio da publicidade e a transparência dos órgãos públicos. Segundo prevê o art. 8º da LAI, os órgãos públicos devem promover a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral.

Ao mesmo tempo, o art. 6º, III, disciplinou a obrigação dos órgãos e entidades do poder público de proteger a informação sigilosa e a informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. Já em seu art. 31, determinou que o tratamento das informações pessoais deve respeitar a intimidade, a vida privada, honra e imagem das pessoas, e que tais informações pessoais terão acesso restrito a agentes públicos, sendo possível sua divulgação ou acesso por terceiros, somente por meio de previsão legal ou consentimento expresso dos titulares, o que vai de encontro com o que dispõe a LGPD.

Considerando a obrigação legal de disponibilidade de acesso aos bancos de dados públicos, o art. 31, §2º, da LAI, dispõe sobre a responsabilização de quem usar indevidamente as informações pessoais obtidas, bem como estabelece a dispensa de consentimento quando as informações forem necessárias à realização de estatísticas e pesquisas científicas de interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem. É neste ponto, em especial, que *legaltechs* e demais empresas de tecnologia se apoiam para advogar pela restrição mínima de acesso, já que os dados pessoais de magistrados e, muitas vezes das próprias partes, são indispensáveis para o desenvolvimento de sistemas de jurimetria,

cuja fontes de alimentação de suas informações estatísticas são os dados obtidos a partir das bases de dados dos diversos órgãos do Poder Judiciário.

Na concepção de SARLET e MOLINARO²³¹, o fenômeno *informação* “*objeto da regulação pelo Direito, se tenciona nas ações de informar, informar-se e ser informado*”. O direito de acesso à informação, por sua vez, deve observar, necessariamente, a proteção dos direitos da personalidade, limitando, dessa forma, o acesso e difusão da informação, “fundada na paridade de armas entre cidadãos e cidadãos e entre cidadãos e o Estado, objetivando a concreção do direito à autodeterminação informativa”.

Os direitos fundamentais do indivíduo constituem, portanto, limites intransponíveis à atuação do Estado. No que se refere ao acesso às informações de processos judiciais, considerando que a LGPD veio, por sua vez, tutelar e regulamentar o direito à proteção de dados, a leitura normativa indica a necessidade premente de impedir tais acessos por meio do nome das partes, sem que aquele que deseja obter a informação tenha efetuado prévio cadastramento e demonstre manifesto interesse.

Diante de tudo quanto foi exposto até o momento, entende-se, após análise dos textos normativos ora percorridos, que o princípio da publicidade pode ser garantido em sua concepção e finalidade e ainda preservar a intimidade e a vida privada, por meio da **harmonização dos princípios**, conforme lição de CANOTILHO:

Harmonizar princípios equivale a uma contemporização ou transacção entre princípios de forma a assegurar, nesse concreto, a aplicação coexistente dos princípios em conflito. A ponderação reconduz-se, no fundo, à criação de uma hierarquia axiológica móvel entre princípios conflitantes.²³²

Para tanto, a solução mais acertada seria o Brasil adotar, como já se faz de forma sistematizada na Europa, a pseudonimização de dados pessoais,

²³¹ SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. **O direito à informação na ordem constitucional brasileira: breves apontamentos**. In: Acesso à informação como direito fundamental e dever estatal. Coordenadores: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla; RUARO, Regina Linden. Porto Alegre: Livraria do Advogado, 2016. p. 16

²³² CANOTILHO, J. J. **Direito constitucional e teoria da constituição**. p. 1.241

como o uso de acrônimos, por exemplo, de forma que os dados pessoais não constem de publicações eletrônicas, cujas bases de dados podem ser acessadas por sistemas de tecnologia de *Big Data* que realizam a análise quantitativa e qualitativa das informações armazenadas.

A Assembleia Nacional da França, em 23 de março de 2019, promulgou a lei 2019-222 que, dentre outras disposições, regulamentou o acesso aos dados judiciais, impondo medidas rígidas, que foram, e continuam sendo, duramente criticadas²³³.

Em seu art. 33, que declarou expressamente a intenção de conciliar as decisões da justiça com o direito à privacidade, definiu-se os critérios de acesso e disponibilização de dados eletrônicos sobre processos, incluindo tópicos como os custos do acesso, a forma de disponibilização, anonimização e reuso de dados na construção de modelos preditivos.

Uma das disposições determina que todos os acórdãos dos tribunais judiciais da França sejam disponibilizados em formato eletrônico e estabelece restrições e diretrizes para a anonimização de parte das informações incluídas nos acórdãos e dispõe que os nomes próprios e os sobrenomes das pessoas físicas mencionadas nos acórdãos, sejam elas partes ou terceiros envolvidos, devem ser ocultados antes de sua publicação. E vai além, a lei passa a possibilitar que, quando a divulgação possa prejudicar a segurança ou infringir a privacidade das pessoas, sejam ocultados, além dos nomes das partes, demais elementos que possam identificar, não somente elas, mas também os terceiros, os magistrados e os membros da serventia.

²³³ Em artigo publicado no editorial jurídico Migalhas, os autores afirmam que tanto a anonimização como a proibição de reuso dos dados pessoais, notadamente dos magistrados, estão sendo criticadas pela comunidade em geral, especialmente pelos pesquisadores empíricos e participantes do mercado de *legaltechs*, em razão da limitação imposta pela lei francesa de acesso a dados considerados de interesse público e de grande relevância para o estudo do funcionamento da justiça, especialmente voltados para a área de jurimetria. NUNES, Marcelo Guedes; CORRÊA, Fernando; TRECENTI, Julio. *A lei francesa de acesso a dados judiciais: algumas reflexões* (2019). Disponível em: <<https://www.migalhas.com.br/depeso/304441/a-lei-francesa-de-acesso-a-dados-judiciarios-algumas-reflexoes#:~:text=A%20premissa%20da%20qual%20a,%C3%A0%20intimidade%20das%20pessoas%20envolvidas.>>> Acesso em: 28/07/2020.

3.2 O COMPARTILHAMENTO DE DADOS PROCESSUAIS PELOS ÓRGÃOS DO PODER JUDICIÁRIO COM PESSOAS JURÍDICAS DE DIREITO PRIVADO

Enquanto na iniciativa privada há uma intenção clara do legislador de proteger o consumidor em sua subjetividade, livre arbítrio e livre desenvolvimento de sua personalidade frente à utilização pelas empresas dos seus dados pessoais como insumos de suas atividades econômicas, o Poder Público, ainda que não tenha, *ab initio*, por fim obter vantagem econômica, também necessita de dados como insumos para a elaboração de suas políticas públicas e para a consecução de seus objetivos constitucionais e sociais, como visto no capítulo anterior.

No que concerne o Poder Judiciário, a garantia de efetividade e celeridade da prestação jurisdicional, constitucionalmente prevista, impulsiona a busca por inovações tecnológicas que desafoguem a Justiça brasileira, a qual, em vista da louvável garantia de amplo acesso à Justiça, precisa contornar os efeitos adversos causados pela hiperjudicialização.

Considerando a enorme quantidade de processos em trâmite, aliada à alteração de paradigma introduzida pelo *Big Data*, é razoável (e esperado) que o Poder Judiciário se valha dos benefícios da tecnologia, tais como a Inteligência Artificial, amplamente utilizada na iniciativa privada, para desenvolver aplicações que possam efetivamente melhorar a entrega dos serviços aos jurisdicionados e facilitar a atividade dos servidores.

O CNJ, inclusive, já se pronunciou a respeito do interesse de empresas privadas nos bancos de dados processuais mantidos pelos Tribunais para fins de oferecimento de serviços ao Poder Judiciário, enfatizando a urgência de uma norma que regule o acesso de empresas privadas a tais informações²³⁴:

[...] a principal urgência normativa é regular o acesso aos sistemas dos Tribunais por parte de pessoas jurídicas, ante notícias de que empresas procuram os Tribunais para oferecimento de serviços mediante acesso à respectiva base de dados dos processos judiciais. Ressaltou, também, que antes de se deliberar sobre questões de compras pelas áreas de TI dos Tribunais, é necessário verificar e acompanhar o que já foi feito nesse sentido.

²³⁴ Disponível em: <<https://www.cnj.jus.br/o-cnj/estrutura-organizacional/comissoes/comissao-permanente-de-tecnologia-da-informacao-e-infraestrutura>>. Acesso em: 15/03/2020.

Denota-se que a problemática de acesso aos dados mantidos pelo Poder Judiciário, seja por iniciativa de seus próprios órgãos ou em razão do acesso conferido em decorrência da publicidade dos atos processuais, é latente e amplificada pelos avanços tecnológicos. Neste sentido, passa-se a investigar de que forma a LGPD poderá auxiliar ou, ao menos, direcionar as ações do Poder Judiciário no que se refere ao compartilhamento de informações constantes de seus bancos de dados.

3.2.1 Compartilhamento de dados para fins de desenvolvimento de sistemas de tecnologia da informação e Inteligência Artificial

Em publicação do CNJ intitulada “Inteligência Artificial no Poder Judiciário”, que avalia a utilização da Inteligência Artificial, são feitas as seguintes reflexões: “Qual o papel do Poder Judiciário em um mundo em constante mutação? Como a inovação tecnológica pode ser apropriada por essas estruturas tradicionais para melhorar a qualidade da prestação jurisdicional?”, e continua afirmando que China, Reino Unido, Singapura, Japão, Finlândia, Índia, Dinamarca, Canadá e Estados Unidos incorporaram, com sucesso, tecnologia ao processo para facilitar o acesso dos cidadãos ao Poder Judiciário²³⁵.

Ademais, além da situação de litigância única no cenário brasileiro, a Era Digital, formada por uma Sociedade complexa e massificada, também apresenta a multiplicação de demandas de massa, consubstanciadas em processos sobre o mesmo tema tramitando em diversas comarcas distintas. Assim, conforme apontou o CNJ, “é essencial o desenvolvimento de ferramentas que garantam estabilidade, uniformidade, previsibilidade, coerência e integridade à jurisprudência dos tribunais”, afirmando, também que “[u]m mundo digital exige uma Justiça digital: célere, dinâmica e também digitalmente conectada”²³⁶.

No mesmo documento, destacou-se a necessidade de oferecer uma resposta adequada aos que buscam os serviços de justiça e o papel central do CNJ na inovação do Poder Judiciário, como por exemplo, através da

²³⁵ CONSELHO NACIONAL DE JUSTIÇA. **Inteligência artificial na justiça**. Coordenação: José Antônio Dias Toffoli; Bráulio Gabriel Gusmão. Brasília: CNJ, 2019. p. 7

²³⁶ CONSELHO NACIONAL DE JUSTIÇA. **Inteligência artificial na justiça**. p. 8

automatização de atividades repetitivas e de apoio à decisão, por meio do desenvolvimento colaborativo de modelos de Inteligência Artificial que sejam, também, capazes de realizar previsões sobre decisões, sugerindo ao usuário qual a melhor opção aplicável a cada caso²³⁷.

A título apenas de registro, faz-se aqui uma ressalva de que não se evidenciou menção à proteção a dados pessoais no documento preparado pelo CNJ, que aponta as diversas tecnologias que estão sendo desenvolvidas por Tribunais brasileiros e pelo próprio CNJ, inclusive para fins de reconhecimento facial.

À respeito das tecnologias de reconhecimento facial, a IBM anunciou, em 08 de junho de 2020, em meio às manifestações que seguiram o assassinato de George Floyd, que irá abandonar a pesquisa, o desenvolvimento e o fornecimento deste tipo de tecnologia e de softwares de análises de rostos, devido à sua discordância com os usos atuais dessas aplicações, que incluem a vigilância em massa, a criação de perfil racial, violações de liberdade e direitos humanos básicos, e reforçaram a necessidade de se iniciar um diálogo em nível nacional para avaliar *se e de que forma* tecnologias de reconhecimento facial devem ser empregadas por autoridades policiais e agências de segurança²³⁸.

Ademais, verificou-se que estudos anteriormente realizados a respeito de algoritmos treinados com bancos de imagens e a partir de ordens humanas, acabam tornando-se enviesados com o tempo, o que pode levar a "falsos positivos" e incriminação de pessoas sem evidência. No mesmo passo da IBM, a Microsoft recomenda que governos regulamentem o uso de reconhecimento facial, enquanto o CEO da Google, Sundar Pichai, pediu no início de 2020 que governos da União Europeia restringissem o poder do setor. A Amazon, por outro lado, investe bastante no setor e tem sistemas até capazes de reconhecer medo. No Brasil, houve casos de utilização bem sucedida dessas

²³⁷ CONSELHO NACIONAL DE JUSTIÇA. *Inteligência artificial na justiça*. p. 14

²³⁸ THE VERGE. **IBM will no longer offer, develop, or research facial recognition technology**. Disponível em: <<https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software>>. Acesso em: 08/06/2020.

ferramentas durante o Carnaval, mas ela também já levou a polícia a cometer erros e deter inocentes²³⁹.

Os exemplos citados acima demonstram a preocupação da sociedade civil com a vigilância exercida pelo Estado por meio das tecnologias que se utilizam de dados pessoais sensíveis dos cidadãos.

Em artigo intitulado *Let's talk ethics: privacy and data protection framework for a learning analytics toolbox*, os autores sustentam que, para encontrar o equilíbrio entre as pesquisas de aprendizagem analítica por meio de sistemas e a privacidade do indivíduo, o projeto em questão deve endereçar todas as questões envolvendo a proteção de dados e estar em conformidade com as leis e diretivas nacionais e internacionais, nas quais a proteção dados recebem status de direito fundamental e destacam que as aplicações desenvolvidas devem assegurar o tratamento ético dos dados pessoais.

MORAIS DA ROSA²⁴⁰ assevera que a complexidade da sistemática necessária à compreensão de um fenômeno jurídico, consubstanciada na seleção das regras e princípios jurídicos aplicáveis ao caso, que vão desde a Constituição da República até às *soft laws*, passando-se pela jurisprudência dos diversos tribunais brasileiros, e sua estruturação com a capacidade cognitiva dos agentes jurídicos envolvidos, é uma árdua tarefa. E afirma²⁴¹:

[...] é perceptível a necessidade em tornar visível a transformação digital no Direito, compondo o ambiente forense com fontes de informação adequada e estruturadas, capazes de aprender a auxiliar no processo de decisão. Posto que olvidar-se ou desconhecer uma “portaria”, por exemplo, pode levar a um resultado desastroso. O papel da tecnologia, provida de Inteligência Artificial, mostra-se como disruptivo. O velho modelo

²³⁹ TECMUNDO. **IBM abandona biometria facial por discordar de usos da tecnologia.** Disponível em: <<https://www.tecmundo.com.br/software/153970-ibm-abandona-biometria-facial-discordar-usos-tecnologia.htm>>. Acesso em: 09 de junho de 2020.

²⁴⁰ MORAIS DA ROSA, Alexandre. **A questão digital: o impacto da inteligência artificial no Direito.** Revista de Direito da Faculdade Guanambi, Guanambi, v. 6, n. 02, e259, jul./dez. 2019. Disponível em: <http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/259>. Acesso em: 20/06/2020. p. 4

²⁴¹ MORAIS DA ROSA, Alexandre. **A questão digital: o impacto da inteligência artificial no Direito.** Revista de Direito da Faculdade Guanambi, Guanambi, v. 6, n. 02, e259, jul./dez. 2019. Disponível em: <http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/259>. Acesso em: 20/06/2020. p. 4

de decisão calcado nas capacidades individuais demanda a conjugação de mecanismos tecnológicos capazes de ampliar o horizonte de credibilidade, volume, dentre outros critérios, transformando o *Big Data* em um auxiliar importante.

No contexto internacional, vale destacar a experiência do Poder Judiciário chinês, no sentido de contribuir com informações acerca da realidade mundial para que se possa analisar de maneira crítica as possibilidades e necessidades brasileiras.

Em 2014, o Judiciário da China iniciou uma reforma do seu sistema judicial. Segundo CUI²⁴², um dos cientistas jurídicos envolvidos no projeto, destacou que ciência e tecnologia são meios importantes de alcançar a modernização judicial e que combinar ciência moderna e tecnologia, tal como Inteligência Artificial, com a criatividade judicial proporciona uma grande oportunidade de resolver problemas judiciais.

Em 2019, a terceira versão do sistema denominado “Shanghai Intelligent Assistive Case-Handling System for Criminal Cases” possibilita que todas as fases do processo nos casos criminais sejam realizadas online: desde a denúncia, passando pela investigação, mandados de prisão, revisão, persecução, audiência de julgamento, conversão de regime, até a concessão de liberdade condicional, o que, segundo CUI²⁴³, representou um grande avanço na aplicação da tecnologia de Inteligência Artificial no campo judicial. De acordo com autor, o presidente da China Xi Jinping afirmou que o país que controlar a Inteligência Artificial irá direcionar o futuro.

CUI reconhece, contudo, que a Inteligência Artificial é uma faca de dois gumes:

AI is an integration of technical and social attributes. On the one hand, AI promotes the transformation of the economy and society. It has been made a national strategy and becomes new core competitiveness. On the other hand, AI may bring risks and challenges. Once out of control, serious damages will be caused. The advantages of AI should not be exaggerated, nor the use of AI

²⁴² CUI, Yadong. **Artificial Intelligence and Judicial Modernization**. Springer: Singapura, 2020. eBook. English Edition. p. vi

²⁴³ CUI, Yadong. **Artificial Intelligence and Judicial Modernization**. p. vi

be prohibited. It is viable that we seek advantages and avoid disadvantages, maximizing the benefit of AI.

Atualmente, a aplicação de Inteligência Artificial no sistema judicial da China é aplicada nos seguintes aspectos: 1) apoio no processamento e criação de documentos; 2) apoio na transcrição de audiências; 3) apoio na condução de casos, inclusive na verificação de provas e predição de resultados, fornecendo referência para a decisão a ser tomada pelo juiz; e 4) apoio na prestação de serviços judiciais, através aconselhamento jurídico ao público por meio de robôs.

Segundo CUI²⁴⁴, é muito mais confiável, padronizado e efetivo deixar o sistema, ao invés de pessoas com livre arbítrio, controlar os procedimentos dos casos criminais de acordo com as normas vigentes.

Vale consignar o posicionamento de CUI²⁴⁵:

In the era of AI, we should actively apply AI to improve social governance. We should make full use of the technological advantages of AI to accurately perceive, predict and prompt the important situation of social security, timely grasp group cognition and psychological changes, and make decisions to response actively, so as to improve social governance through the use of AI, enhance the efficiency of public services at different levels, and maintain social harmony and stability. Thus, the social governance will be raised to a new level.¹ In particular, in order to meet the urgent needs of comprehensive social management, new crime investigation and anti-terrorism, we should develop intelligent security and police products integrating multiple detection and sensing technologies, video image information analysis and recognition technology and biometric recognition technology, and establish an intelligent monitoring platform. We should strengthen the intelligent transformation and upgrading of security equipment in key public areas and support communities or cities with appropriate conditions to develop public security regional demonstration based on AI. And we can do more. Through the in-depth application of AI in the field of social governance and public security, the modernization of social governance system and governance capacity will be realized.

Em que pese os enormes benefícios decorrentes da utilização de Inteligência Artificial, fato é que ainda existe um enorme vazio a ser preenchido

²⁴⁴ CUI, Yadong. **Artificial Intelligence and Judicial Modernization**. p. 136

²⁴⁵ CUI, Yadong. **Artificial Intelligence and Judicial Modernization**. p. 187

entre o desenvolvimento e utilização de Inteligência Artificial e as pesquisas relacionadas à segurança dessa tecnologia.

Sabe-se, que o insumo que alimenta a Inteligência Artificial são dados. Através da análise de dados e das tecnologias de *machine learning*, a Inteligência Artificial desenvolvida “aprende” a reconhecer padrões. E é aqui que se identifica um dos problemas apontados no uso de Inteligência Artificial pelo Poder Judiciário em relação ao tratamento de dados processuais: a possibilidade de discriminação.

Um dos princípios basilares da LGPD é a não discriminação. Portanto, ao compartilhar dados processuais com empresas de tecnologia, é fundamental que Poder Judiciário suprima dados pessoais, especialmente os dados pessoais sensíveis por ausência de autorização legal para o referido tratamento, uma vez que, diante do contexto atual de evolução tecnológica dos sistemas de informação e dos possíveis riscos ao livre desenvolvimento da personalidade que podem vir a acarretar, estes devem ser considerados irrelevantes para o desenvolvimento de Inteligência Artificial, que deve ser, assim como a Justiça, imparcial.

Neste ponto, vale destacar o posicionamento de LEVY²⁴⁶, filósofo da informação e estudioso no campo da Inteligência Artificial. Ao discorrer sobre a disponibilidade de dados e o poder de cálculo das novas tecnologias, o filósofo argumenta que, na era do ciberespaço, quase todos os signos culturais são criados, gravados e interconectados em uma rede digital que se expande a cada dia e que inclui computadores, smartphones, aparelhos eletrônicos móveis, assim como coisas e máquinas em que se encontram embutidos chips de identificação e de conexão. Em termos de localização, os novos sistemas de realidade aumentada fornecem acesso em tempo real a informações relevantes associadas a lugares e situações, que facilitam, como nunca, encontrar pessoas e serviços de acordo com suas localizações geográficas. Em termos de deslocalização, o armazenamento de dados e aplicações em “nuvens” permitem que sejam

²⁴⁶ LÉVY, Pierre. **The semantic sphere 1**: computation, cognition and information economy. ISTE Ltda: Londres, 2011. Ebook. p. 182

acessados de qualquer ponto da *network* e afirma que a sociedade está progredindo para uma situação de computação ubíqua, na qual capacidades de memória, cálculo e comunicação sem fio são praticamente ilimitadas e completamente integradas ao ambiente.

Todos os documentos estão virtualmente interconectados, em regra formando um único hipertexto fluido, lido e escrito por um imenso número de leitores e escritores de diversas línguas, culturas e etnias. De acordo com LEVY²⁴⁷, um *software* nada mais é do que um tipo de escrita adaptado ao mundo dos computadores conectados em rede e capaz de agir por conta própria, interagir com outros *softwares*, criar combinações, ligar máquinas e ativar robôs. Entretanto, em que pese defender as pesquisas e os avanços proporcionados pela tecnologia, a ubiquidade dos dados, a unidade de suas codificações binárias, o entrelaçamento de seus hipertextos e a calculabilidade e rastreabilidade das informações fazem emergir uma nova situação epistemológica, haja vista seus efeitos em relação à ética e à proteção da privacidade, razão pela qual LEVY entende que, como um princípio moral provisório, ou seja, até que se tenha um efetivo conhecimento do poder advindo do entrelaçamento de informações e da autonomia de *softwares*, as ciências humanas não devem utilizar dados pessoais capazes de identificar indivíduos e processem somente as dimensões semânticas, axiológicas e quantitativas dos fluxos de dados.

As observações acima são ainda mais pertinentes se forem considerados a qualidade e o alcance das informações pessoais constantes dos processos judiciais. Deverá haver um equilíbrio entre a necessária inovação que precisa, de fato, ser abraçada pelo Poder Público na busca por eficiência e redução de custos de seus serviços, com a proteção dos riscos à intimidade e às liberdades individuais, mormente relacionados à discriminação, que ainda não podem ser previstos diante da crescente evolução das tecnologias.

A LGPD, apesar de, em um primeiro momento, ter sido recepcionada como um entrave à inovação, após uma análise mais detida, é

²⁴⁷ LEVY, Pierre. **The semantic sphere 1**: computation, cognition and information economy. p. 129

possível aferir que, na verdade, o que ela fez foi estabelecer regras para situações que não são mais passíveis de retorno ao *status quo*, como as inovações tecnológicas advindas da Inteligência Artificial, a exemplo da China e diversos outros países que já fazem uso deste tipo de tecnologia em seus processos judiciais.

Ademais, o tratamento de dados pessoais deve estar fundado em pelo menos uma das hipóteses constantes do art. 7º da LGPD. Como verificado anteriormente, a autorização de tratamento dos dados pessoais recebidos pelo Poder Judiciário no âmbito do processo judicial está disciplinada no inciso VI do referido artigo e, segundo o que dispõe o art. 6º, I, as atividades de tratamento de dados pessoais deverão ser realizadas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

A ANPD terá papel fundamental na definição e identificação das bases legais de tratamento, como demonstra a experiência da *Information Commissioner's Office*²⁴⁸, a agência de proteção de dados do Reino Unido que, no dia 23 de julho de 2020, publicou os primeiros relatórios a partir de seu *Sandbox Regulatório*²⁴⁹.

O objetivo do *Sandbox Regulatório* da ICO foi demonstrar que a proteção de dados pode ser aliada a soluções inovadoras do mundo real, garantindo *compliance* com as regulações existentes. De acordo com a ICO, ao aplicar a legislação em situações novas e emergentes, é possível construir um entendimento que está sendo utilizado para informar as diretrizes e a abordagem regulatória do órgão.

²⁴⁸ ICO. Information Commissioner's Office. *First reports published from the Regulatory Sandbox* (2020). Disponível em: <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/first-reports-published-from-the-regulatory-sandbox/>>. Acesso em: 28/07/2020.

²⁴⁹ *Sandbox Regulatório* é a terminologia utilizada pelas empresas de tecnologia, especialmente da indústria financeira, para se referir a um mecanismo cujo objetivo é o desenvolvimento de um ambiente regulatório que consiga acompanhar as rápidas transformações advindas das inovações e não sirvam de “entrave” ao desenvolvimento da inovação.

Entre os dez produtos e serviços que utilizam dados pessoais de forma inovadora e que estão sendo avaliados, estão os projetos da organização não governamental do setor educacional “Jisc” e do Aeroporto Heathrow, objeto do relatório acima mencionado.

No caso da Jisc, a ONG desenvolveu um Código de Prática com universidades que desejam investigar a utilização de dados relacionados às atividades dos alunos para melhorar os serviços de apoio ao estudante, inclusive relacionados à saúde mental e bem estar. Juntamente com a ICO, foram desenvolvidas duas ferramentas-chave: uma Matriz de Compatibilidade da Finalidade²⁵⁰, através da qual as universidades serão capazes de analisar se os dados que pretendem utilizar são compatíveis com a finalidade original para a qual foram coletados (princípio da adequação); e um modelo padrão de DPIA, com as diretrizes para universidades e medidas de mitigação de riscos pré-definidas.

No que diz respeito ao Heathrow Airport, participou do *Sandbox* o programa de automação de viagem do passageiro, cujo objetivo é utilizar dados biométricos, como o reconhecimento facial, que seria oferecido nos serviços de check-in, despacho de bagagem e portões de embarques, para oferecer uma experiência de viagem sem interrupções aos passageiros, uma vez que não precisariam mais apresentar diferentes documentos, tais como passaporte e cartão de embarque, em diferentes etapas da viagem. Durante o *Sandbox* foram avaliados os seguintes problemas: a complexidade envolvendo a definição do Controlador dos dados e as bases legais para o tratamento. O Heathrow Airport e a ICO concordaram que o consentimento explícito seria a única base para tratamento, e que, devido à complexidade em se obter o referido consentimento, o Heathrow comunicou à ICO que iria adiar os planos para novas avaliações de seus processos.

O que se observa da análise desses dois exemplos em cotejo com as bases legais definidas no art. 7º da LGPD, considerando que os dados

²⁵⁰ *Purpose Compatibility Matrix*

dados pessoais constantes em processos judiciais são coletados e recepcionados pelo Poder Judiciário em decorrência da finalidade descrita no inciso VI, ou seja, para o exercício regular de direitos em processo judicial, denota-se que o compartilhamento de tais dados pessoais com pessoas jurídicas de direito privado somente seria possível após a obtenção do consentimento explícito do titular dos dados para a operação de tratamento desejada, o que, assim como no caso do Heathrow Airport, é de tamanha complexidade e inviabilidade que impossibilita o tratamento sob essa base legal.

Dentre as alternativas oferecidas pelo legislador, o tratamento de dados pessoais, inclusive o seu compartilhamento, pode ser realizado quando necessário para atender aos interesses legítimos do Controlador, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de dos dados pessoais, conforme prevê o inciso IX do art. 7º da LGPD.

O tratamento fundamentado no legítimo interesse do Controlador somente poderá ser realizado para finalidades legítimas, consideradas a partir de situações concretas que incluem, mas não se limitam, ao apoio e promoção de atividades do controlador e à proteção do exercício regular dos direitos do titular ou à prestação de serviços que o beneficiem.

Neste caso, os órgãos do Poder Judiciário, na figura de Controladores dos dados pessoais que serão compartilhados, deverão adotar medidas para garantir a transparência do tratamento de dados, além de a ANPD poder solicitar o relatório de impacto à proteção de dados pessoais, o DPIA.

Ademais, o legislador suprimiu a possibilidade de tratamento de dados pessoais sensíveis fundamentado no legítimo interesse do Controlador. Dada a natureza dos processos judiciais, notadamente aqueles que tramitam em segredo de justiça, identifica-se, neste ponto, um complicador no que se refere ao compartilhamento de base de dados de processos judiciais que tragam em seu bojo dados pessoais sensíveis.

Da análise conjunta dos dispositivos supra, é possível a interpretação de que o compartilhamento de informações pessoais dos litigantes e

demais partes envolvidas em processos judiciais com entidades privadas para fins de desenvolvimento de tecnologia carece de base legal de tratamento expressa, recaindo na possibilidade de caracterização de legítimo interesse, previsto no art. 7º, IX, da LGPD, ressalvado o compartilhamento de dados pessoais sensíveis.

Há, ainda, a possibilidade de anonimização dos dados pessoais constantes das bases de dados de processos judiciais por meio de tecnologia específica. Nestes casos, conforme prerrogativa do art. 12 da LGPD, os dados anonimizados não serão considerados dados pessoais e, portanto, não se sujeitam aos preceitos da Lei, salvo se puderem ser revertidos.

Vale, contudo, destacar o contraponto feito por MACCAN²⁵¹ ao afirmar que não é fácil “desidentificar”, como Google e Netflix descobriram quando disponibilizaram dados anônimos de seus consumidores para pesquisa e todos os indivíduos anonimizados puderam ser identificados posteriormente através do uso de informações cruzadas. Por isso é importante que se adotem medidas efetivas de anonimização.

Em relação ao processo de anonimização, a ANPD poderá dispor sobre padrões e técnicas utilizados e realizar verificações acerca de sua segurança, nos termos do §3º do art. 12 da LGPD

Em sendo assim, da mesma forma como deverá ocorrer com a publicação de atos processuais, os dados pessoais das partes deverão ser suprimidos no caso de compartilhamento com terceiros.

Do que se verifica, é primordial que a ANDP seja devidamente constituída para que defina as diretrizes necessárias aos pontos omissos e ambíguos identificados na Lei.

²⁵¹ MACCANN, Duncan. **Power and accountability in the digital economy**. Data and big tech companies have more and more power. As the digital economy develops, we need to put people and society at the centre. Disponível em: <<https://neweconomics.org/2019/10/power-and-accountability-in-the-digital-economy>>. Acesso em: 15/10/2019.

3.2.2 A transferência internacional de dados e a cloud computing

Tal como a circulação de mercadorias foi um elemento primordial para o desenvolvimento global após a Revolução Industrial, hoje o fluxo de dados é essencial para a nova etapa de desenvolvimento econômico e social²⁵².

A transferência internacional de dados, instituto que não é novo e já vem sendo operacionalizado desde os primórdios das transações internacionais e tem sido potencializado pelo fenômeno da globalização, certamente continuará a aumentar.

Desde a adoção das diretrizes para o processamento de dados pessoais pela OECD, em 1980, como visto no primeiro capítulo desta pesquisa, a proteção da privacidade e das liberdades individuais não é, por seu turno, o único objetivo de tais diretrizes. A OECD objetiva, também, albergar o fluxo transfronteiriço de dados pessoais de forma a prevenir disparidades entre normas nacionais que possam servir de empecilho ao livre fluxo de dados pessoais para além das fronteiras nacionais²⁵³.

A compreensão das regras da OCDE para o fluxo transfronteiriço de dados é de grande valia, uma vez que os EUA, país que adota um sistema de proteção à privacidade e dados pessoais de forma setORIZADA, segue as diretrizes da OECD, que são menos rígidas que aquelas estabelecidas pelo GDPR.

De forma simples e direta, a OCDE define o fluxo transfronteiriço de dados como sendo os “movimentos dos dados pessoais além das fronteiras nacionais”²⁵⁴.

²⁵² GUTIERREZ, Andriei. **Capítulo IX – Da autoridade nacional de proteção de dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**. in MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. LGPD: Lei Geral de Proteção de Dados. p. 401

²⁵³ FUSTER. Gloria González. **The emergence of personal data protection as a fundamental right of the EU**. Brussel: Springer, 2014. p. 81

²⁵⁴ “*Transborder flows of personal data*” means movements of personal data across national borders. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD guidelines on the protection of privacy and transborder flows of personal data**. Disponível em: < https://www.oecd.org/sti/economy/oecd_privacy_framework.pdf>. Acesso em: 15/04/2020.

Na quarta parte das referidas diretrizes, estão estabelecidos os princípios básicos aplicáveis em âmbito internacional, quais sejam: o livre fluxo de dados e restrições legítimas e define as seguintes regras:

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing²⁵⁵.

A União Europeia, por meio do GDPR, estabelece que, via de regra, a transferência internacional de dados é proibida, a menos que atendidas as condições previstas em lei e só podem ser realizadas a jurisdições que mantenham um nível adequado de proteção de dados pessoais ou quando o exportador dos dados tenha implementado mecanismo legítimo de transferência de dados.

A LGPD disciplina as regras para a transferência internacional de dados pessoais em seu capítulo V e descreve as hipóteses permitidas, de forma exaustiva, em seu art. 33, abaixo transcrito na íntegra:

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

²⁵⁵ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD guidelines on the protection of privacy and transborder flows of personal data**. Disponível em: < https://www.oecd.org/sti/economy/oecd_privacy_framework.pdf>. Acesso em: 15/04/2020.

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Da leitura do *caput*, é possível inferir que o legislador pretendeu restringir as hipóteses em que é permitida a transferência internacional de dados pessoais, sendo a sua possibilidade a exceção à regra.

Para melhor compreensão da norma, faz-se necessário entender o que configura uma atividade de transferência internacional sob a ótica da proteção de dados.

Primeiramente, é importante frisar que, além das transferências de dados decorrentes de contratos e acordos de cooperação internacional, incorrem em transferência internacional de dados os órgãos e entidades que utilizam serviços de TI online, serviços em nuvem, serviços de acesso remoto e demais serviços e operações correlatas e, portanto, deverão implantar mecanismos legais para a transferência de dados.

Por outro lado, com base no melhor entendimento europeu sobre o tema, haja vista que a LGPD ainda não entrou em vigor e, portanto, há a carência de situações nacionais suficientes para se identificar um padrão, é importante entender que um simples acesso à aplicação de Internet não deve ser considerado uma transferência internacional de dados, sob pena de, segundo CHAVES²⁵⁶, “banalizar a aplicação do conceito e transformar o regime jurídico especial da transferência internacional em geral, o que poderia culminar, inclusive, em uma desarmonia com as bases legais do art. 7º da LGPD”.

Referenciando, ainda mais uma vez, o *Information Commissioner's Office* do Reino Unido, não se deve confundir *transferência* de dados com *trânsito* de dados.²⁵⁷

Assim, nas situações em que ocorrer, do ponto de vista técnico-jurídico, transferência internacional de dados, deverá ser observado ao menos um dos requisitos disciplinados nos incisos do art. 33 da LGPD, quais sejam: (i) a transferência somente é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD, cuja avaliação pode ser requisitada à ANPD pelo interessado; (ii) quando o controlador dos dados oferecer e comprovar garantias dos cumprimentos das premissas da LGPD na forma de cláusulas contratuais, normas corporativas globais, bem como por selos, certificados e normas de conduta; (iii) para fins de

²⁵⁶ CHAVES, Luis Fernando Prado. **Capítulo V: da transferência internacional de dados**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019

²⁵⁷ INFORMATION COMMISSIONER'S OFFICE. **Guide to the general data protection regulation (GDPR)**. Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>>. Acesso em: 30/07/2020.

cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, segundo os instrumentos jurídicos previstos para tais finalidades; (iv) quando necessária para proteger a vida ou a incolumidade física do titular ou de terceiro; (v) quando autorizado pela ANPD; (vi) se necessária para cumprimento de compromisso assumido em acordo de cooperação internacional; (vii) para execução de política pública ou atribuição legal do serviço público; (viii) quando o titular tiver fornecido consentimento específico para a transferência; (viii) para o cumprimento de obrigação legal do controlador; (ix) para a execução de contratos a pedido do titular; ou (x) para o exercício regular de direitos em processo judicial.

Já o art. 34 da LGPD dispõe que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela ANPD, que deverá levar em consideração os requisitos dispostos na referida Lei.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

A ANPD deverá, portanto, analisar o nível de adequação de países estrangeiros, com base nos critérios definidos pelo artigo supra referido. CHAVES²⁵⁸ pontua que uma preocupação inerente ao dispositivo legal em

²⁵⁸ CHAVES, Luis Fernando Prado. **Capítulo V: da transferência internacional de dados**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados.

comento diz respeito ao tempo em que a ANPD tomará para decidir o nível de adequação de cada país, ainda mais se for levado em conta que a autoridade em questão sequer foi estruturada, e destaca que, na experiência europeia, um dos fatores alvo de críticas é o tempo que se leva para tomar a decisão de adequação, o que vem impactando as relações comerciais entre os países.

O caso mais emblemático envolvendo o uso de computação em nuvem pelo Poder Judiciário, brevemente mencionado no primeiro capítulo desta pesquisa, refere-se à suspensão pelo CNJ do processo de contratação da Microsoft pelo Tribunal de Justiça de São Paulo para a “criação de estratégia de longo prazo na área digital e tecnológica, incluindo o desenvolvimento de um novo sistema de tramitação processual”, no valor estimado de R\$ 1 bilhão e 320 milhões. O TJSP justificou a escolha do serviço em nuvem da Microsoft por dois motivos: redução de custo com infraestrutura de *data center* e potencialização da incorporação de novas tecnologias e serviços disponíveis em nuvem.

A decisão de suspensão do contrato foi proferida pelo Conselheiro Relator Márcio Schiefler Fontes, juiz do Tribunal de Justiça de Santa Catarina e presidente da Comissão de Tecnologia da Informação e Infraestrutura, nos autos do procedimento de Acompanhamento de Cumprimento de Decisão 0000681-09.2014.2.00.0000, que havia concedido ao Tribunal de Justiça de São Paulo.

Em seu voto, o Conselheiro faz ponderações pertinentes sobre as ressalvas do CNJ.

Considerando a abrangência dos assuntos abordados, oportuno destacar alguns pontos da decisão: (i) a caracterização da Microsoft como empresa transnacional; (ii) a necessidade de se ter a tecnologia o serviço de processamento de banco de dados em nuvem privada à disposição do Judiciário, em compatibilidade com o PJe; (iii) preocupações com a inovação tecnológica em análise, especificamente quanto à segurança e sigilo das informações; (iv) adoção de quaisquer tecnologias pelo Judiciário não pode caminhar sem que seja

permeada por constante cautela, notadamente quando se está diante de guarda e acesso a dados judiciais; (v) as preocupações com escândalos de vazamentos de dados em grande escala ocorridos nos últimos anos; (vi) invasões de privacidade praticadas, sem exceção, sobre bases de dados mantidas pelas conhecidas empresas transnacionais de tecnologia; (vii) nível de interesse que as informações que constam dos processos judiciais em trâmite no país podem despertar, como contratos, detalhes sobre a vida pessoal, dados patrimoniais, políticas de Estado, preferências individuais ou coletivas, enfim, uma miríade de informações que integra muitos milhões de processos em curso ou arquivados; (viii) a existência de Ação Civil Pública proposta pelo Ministério Público Federal contra a Microsoft Informática Ltda. e a União que objetiva verificar violações ao direito de privacidade/intimidade praticadas pela empresa Microsoft, por intermédio do Sistema Operacional Windows 10;

Da decisão, vale destacar o seguinte trecho:

É dever do Estado, ao impor o monopólio legítimo da força, sendo o Poder Judiciário uma das suas expressões, garantir aos usuários – cidadãos, empresas, entes públicos etc. – segurança no tratamento das informações que obrigatoriamente recaem sob a custódia dos Tribunais.

Ante o contexto referido, permanecem não só válidas, mas sobretudo atuais, as preocupações com segurança, que são inerentes à contratação de um sistema eletrônico para lidar com tão valioso repositório de informações.

Após descrever situações ocorridas em relação a vazamento de dados pessoais reportados no Brasil e no mundo, envolvendo empresas como Facebook, Cambridge Analytica, Google, T-Mobile e British Airways, para nomear algumas, o Relator destaca que referidas invasões de privacidade são praticadas, sem exceção, sobre bases de dados mantidas pelas conhecidas empresas transnacionais de tecnologia e faz a ressalva de que não há como desconsiderar o nível de interesse que as informações que constam dos processos judiciais em trâmite no país podem despertar, tais como “[c]ontratos, detalhes sobre a vida pessoal, dados patrimoniais, políticas de Estado, preferências individuais ou coletivas, enfim, uma miríade de informações que integra muitos milhões de processos em curso ou arquivados”.

A insegurança jurídica mais premente, contudo, refere-se ao fato de os dados estarem armazenados em jurisdições sujeitas a regramentos distintos, como expõe o Conselheiro na decisão do CNJ que suspendeu a contratação da Microsoft pelo Tribunal de Justiça de São Paulo, cujo excerto da decisão se colaciona a seguir:

É dizer: potencialmente falando, empresa estrangeira, em solo estrangeiro, manterá guarda e acesso a dados judiciais do Brasil, onde a intensa judicialização reúne, nos bancos de dados dos Tribunais, uma infinidade de informações sobre a vida, a economia e a sociedade brasileira, o que, ressalvadas as cautelas certamente previstas, pode vir a colocar em risco a segurança e os interesses nacionais do Brasil, num momento em que há graves disputas internacionais justamente acerca dessa matéria.

Em que pese riscos apontados, o Relator, ressaltou que o serviço de processamento de banco de dados em nuvem privada já foi, inclusive, objeto de recente contratação realizada pelo STF, fato que confirma a contemporaneidade da matéria e a necessidade de se ter esse tipo de tecnologia à disposição do Judiciário.

Em artigo²⁵⁹ publicado em 26 de março de 2019, no jornal eletrônico JOTA, a Vice-Presidente Jurídica e de Assuntos Corporativos da Microsoft Brasil, muito provavelmente impulsionada pela suspensão do contrato firmado com o TJSP, faz algumas ponderações sobre a contratação dos serviços de nuvem e sua correlação com a proteção de dados no setor público:

Uma questão importante é a necessidade premente de manter as informações do cidadão a salvo de ameaças cibernéticas, um problema dos nossos

tempos. Nesse sentido, plataformas de computação em nuvem se mostram muito mais capazes de detectar, proteger e combater o crime virtual.

Apesar de tantos exemplos bem-sucedidos em muitos países, a adoção de serviços de nuvem pelo setor público no Brasil,

²⁵⁹ DEL BEBBIO, Alessandra. **Nuvem e proteção de dados no setor público**. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/nuvem-e-protecao-de-dados-no-setor-publico-26032019>> Acesso em: 20/04/2020.

providos por empresas privadas, ainda é uma novidade e, portanto, é natural que suscite dúvidas, especialmente no campo da privacidade e segurança de dados.

Entendemos a privacidade dos dados pessoais como um direito humano fundamental. Nossos clientes são os proprietários de seus dados, que estão protegidos, inclusive pelas mais modernas técnicas de criptografia. Privilegiando a transparência, asseguramos a nossos clientes visibilidade, acesso e controle de seus dados.

A Microsoft, por exemplo, foi uma das primeiras apoiadoras do GDPR na Europa e optamos por adotar como padrão seus rigorosos parâmetros de privacidade e proteção para todos os clientes no mundo. Aqui no Brasil, também nos preparamos para a Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em 2020.

Muito se discute sobre as perspectivas de transformação digital que tecnologias emergentes, como inteligência artificial e internet das coisas, podem propiciar. Nesse norte, considerando a enorme capacidade computacional da nuvem, essas tecnologias vêm gerando ganhos de eficiência, inovação e economia nos setores público e privado.

O rápido e crescente avanço das aplicações de tecnologia (com foco na segurança da informação e recursos financeiros para a constante atualização tecnológica e regulatória) disponíveis pelas grandes empresas de tecnologia, que são de caráter transnacional, comparado com o cenário nacional, o que acaba prejudicando a manutenção dos dados no Brasil. Apesar de que uma das exigências em contrato possa ser a garantia de que não haverá transferência internacional de dados e os mesmos ficarão armazenados no Brasil.

No contexto da União Europeia, em um ambiente de Internet, a proteção dos direitos dos cidadãos europeus se estende a países e empresas terceiros mesmo que o cidadão não esteja fisicamente em outro país. Os direitos devem ser protegidos, inclusive, quando a transferência de seus dados pessoais a países terceiros, muitas vezes sem que o titular dos dados tenha conhecimento dessa operação, uma vez que governos e empresas europeus utilizam

provedores de serviços de armazenamento em nuvem de fora da União Europeia²⁶⁰.

Da mesma forma, há a necessidade de proteção dos dados quando terceiros em países de fora da União (empresas ou autoridades governamentais) têm acesso a dados armazenados na Europa. Um exemplo dessa situação é a transferência de dados pessoais de dentro da União Europeia para os Estados Unidos em decorrência dos objetivos do *Terrorist Finance Tracking Program*. Segundo este acordo celebrado entre a União Europeia e os Estados Unidos, a *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) como o provedor designado fornece determinados dados financeiros de residentes da EU ao Departamento de Tesouro dos Estados Unidos²⁶¹.

A aplicabilidade da proteção, apesar de bastante abrangente, não significa, necessariamente, que os indivíduos têm direito à proteção contra todos os riscos da Internet. Uma proteção efetiva contra todos os riscos, ou seja, uma abordagem risco zero, seria muito difícil de atingir. Ademais, direitos fundamentais coincidem, e muitas vezes, chocam-se com outros direitos fundamentais e interesses públicos. *Trade-offs*, portanto, precisam ser feitas, como no caso acima exemplificado, em que se verifica o trade-off entre privacidade e segurança²⁶².

Há de se destacar, também, a transferência de dados entre Cortes, com base no transjudicialismo. Ao tratar deste fenômeno, SLAUGHTER²⁶³ assevera que a causa mais óbvia da crescente comunicação transjudicial é o aumento da internacionalização de todas as transações anteriormente restritas às fronteiras nacionais, devido tanto a tendências históricas, quanto pelas possibilidades tecnológicas. À medida que os sujeitos da adjudicação doméstica tomam proporções cada vez mais internacionais, os tribunais serão forçados a

²⁶⁰ É por essa razão que a Directive 95/46/EC contém um capítulo tratando a respeito da transferência de dados pessoais a países de fora da União.

²⁶¹ HIJMANS, Hielke. **The european union as guardian of internet privacy**: the story of the art. 16 TFEU. Law, Governance and Technology Series. Springer Nature, 2016. p. 35

²⁶² HIJMANS, Hielke. **The european union as guardian of internet privacy**: the story of the art. 16 TFEU. p. 35

²⁶³ SLAUGHTER, Anne-Marie. **A typology of transjudicial communication**. University of Richmond Law Review. 29 U. Rich. L. Rev. 99 (1994). Available at: <http://scholarship.richmond.edu/lawreview/vol29/iss1/6>. p. 129

entrar em contato com outros sistemas jurídicos e, por conseguinte, com outros tribunais, e trocar dados e informações entre si.

Cumpre, também, destacar o posicionamento adotado pelo estudo destinado às cortes europeias no que tange à aplicabilidade do GDPR quanto ao controle de adequação dos países destinatários de dados concernente ao fluxo transfronteiriço de dados judiciais:

The personal data processed as part of the proceeding are communicated to the parties or other stakeholders in the dispute. Courts as public bodies are subject to national legislation concerning free access to information. Such disclosure may be either routine (e.g. publication of court decisions online) or per request. Data can be further disclosed to courts from other countries based on requests within the cross-border judicial cooperation. These countries may include also third countries outside the Member States. In case of all transmissions, the rights and freedoms of the data subject must be observed through compliance with the principles of personal data protection as well as with specific obligation in case of transmissions with additional potential for risk (e.g. adequacy of the level of protection pursuant to Article 44 GDPR by transmissions to third countries)²⁶⁴.

Ao contrário, porém, do que concluiu o estudo europeu, de que mesmo nos casos de cooperação judiciária internacional os princípios de proteção de dados e as especificidades previstas no GDPR em caso de risco potencial na transferência internacional de dados, o inciso III, do art. 33, da LGPD, expressamente garante que serviços de inteligência internacional, investigações e atividades de cooperação jurídica internacionais não serão inviabilizados pelas regras e restrições de transferência de dados.

Há, ainda, outro risco descrito na literatura acerca do armazenamento em nuvem, que é a chamada fragmentação da Internet, no sentido da segurança dos dados armazenados em um país que acaba se fragmentando.

Diversos autores discorrem sobre a “balcanização” ou fragmentação da Internet, o que significa dizer que a Internet seria separada em frações

²⁶⁴ INFORM Introduction of the data protection reform to the judicial system. **WP2: data protection regulatory review & training material elaboration** – review report on GDPR aimed at court staff. Masaryk University, 2018. p. 30

regionais, e que isso é tido como uma ameaça à Internet. “EU cloud”, à “BRICS Internet”, ou à “halal Internet”, são exemplos da fragmentação mencionada. Modelos de fragmentação variam desde restrições impostas pela legislação interna de um país e que leva ao bloqueio de determinados *websites*, como aqueles contendo pornografia infantil, o que ocorre em muitas jurisdições, a contratos de licenciamento contendo limitações regionais concernentes à difusão de conteúdos específicos na Internet, até o bloqueio de grandes partes da Internet em algumas jurisdições. Assim, a fragmentação possibilitaria a censura da informação por determinados governos, vantagem econômicas advindas da fragmentação, monitoramento de usuários, trazendo consequências negativas para a privacidade e segurança e impactos à soberania nacional²⁶⁵.

3.3 A (IN)SUJEIÇÃO DO PODER JUDICIÁRIO À AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS E OUTRAS (IN)CERTEZAS

A Constituição é a ordem jurídica fundamental da coletividade: determina os princípios diretivos, segundo os quais devem se formar a unidade política e as tarefas estatais a serem exercidas e regula os procedimentos de pacificação de conflitos na sociedade²⁶⁶.

O princípio da separação de poderes é ancorado na acepção de discricionariedade: um poder está proibido de invadir a discricionariedade dos outros. Este o ponto de equilíbrio, a linha fronteira.

A teoria da separação dos Poderes alicerça-se em três postulados fundamentais: i) a diferenciação de **estruturas organizacionais estatais**, em que cada uma das estruturas possui uma esfera de autonomia, não se subordinando à outra; ii) a diferenciação entre as **funções estatais**, identificadas como a legislação, a jurisdição e a administração – a separação funcional de Poderes; e iii) a atribuição de um tipo diverso de função à cada estrutura organizacional, ou Poder, assim o Poder Judiciário é investido na competência jurisdicional, o Poder

²⁶⁵ HIJMANS, Hielke. **The european union as guardian of internet privacy**: the story of the art. 16 TFEU. Law, Governance and Technology Series. Springer Nature, 2016. p. 90

²⁶⁶ NERY JUNIOR, Nelson. **Princípios do processo na constituição federal**. p. 50

Legislativo na competência legislativa ou legiferante e o Poder Executivo na competência administrativa ou executiva²⁶⁷.

3.3.1 O Poder Judiciário

O Poder Judiciário é um dos três poderes expressamente reconhecidos pelo art. 2º da CRFB e a ele foi atribuída a tarefa de dizer o Direito e de julgar, como sua competência jurisdicional.

Conforme lecionam STRECK e MORAIS²⁶⁸, duas significações decorrem da palavra “poder”, uma que representa os órgãos estatais, quais sejam, os Poderes Executivo, Legislativo e Judiciário, e outra que representa as funções desempenhadas, em seu sentido funcional, ou seja, as atividades executiva, legislativa e judiciária, sendo certo, contudo, que cada órgão não exerce exclusivamente uma única função. A função típica é aquela correspondente órgão e a função atípica, aquela exercida pelo órgão em caráter extravagante. A função atípica do judiciário, realizada para aperfeiçoar a sua atuação final, principal ou essencial, cujas atividades encontram-se previstas nos arts. 96 e 99 da CRFB, que dispõem, respectivamente, sobre as garantias da autonomia orgânico-administrativa e da autonomia administrativa e financeira dos órgãos jurisdicionais.

Dessa forma, a **função jurisdicional** do Poder Judiciário é aquela para a qual foi concebido e estruturado. A máxima segundo a qual é vedada a justiça privada tem como imperativo a destinação dos conflitos sociais ao Estado. De acordo com TAVARES²⁶⁹, da função típica do Poder Judiciário, ou seja a jurisdicional, depreendem-se duas ideias básicas: 1) o Estado não pode se negar a apreciar e decidir o conflito social; e 2) nenhum conflito social poderá ser excluído da apreciação dos órgãos estatais competentes.

²⁶⁷ JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. 2. ed. rev. e atual. São Paulo, Saraiva: 2006p. 23

²⁶⁸ STRECK, Lenio Luiz; BOLZAN DE MORAIS, Jose Luis. **Comentários à Constituição do Brasil**. Coordenação: J.J. Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. 2. ed. São Paulo, Saraiva Jur, 2008. Ebook. p. 325

²⁶⁹ TAVARES, André Ramos. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2020. 18. ed. p. 1191

Ademais, o Judiciário, portanto, assim como os demais Poderes, além de sua função típica, jurisdicional, exerce, como **funções atípicas**, atividades administrativas e normativas.

No âmbito da função administrativa, é relevante registrar que a EC 45/2004 acrescentou o inciso I-A ao art. 92, criando, como órgão do Poder Judiciário, o “Conselho Nacional de Justiça”.

Independência do Poder Judiciário e controle externo

A CRFB, em seu artigo 60, §4º, III²⁷⁰, instituiu a separação dos Poderes e a protegeu como cláusula pétrea²⁷¹.

Por meio do princípio da proteção judicial efetiva, previsto no art. 5º, XXXV, da CRFB, segundo o qual “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”, do princípio do juiz natural, delineado no art. 5º, XXXVII e LIII, da CRFB e do princípio do devido processo legal, descrito no art. 5º, LV, a CRFB consagra o livre acesso ao Judiciário. Segundo SARLET e BRANDÃO, tais princípios têm influência decisiva no processo organizatório da Justiça.

São, ainda, essenciais à garantia de um Judiciário imparcial e independente as diversas prerrogativas da magistratura, descritas nos artigos 93 e 95 da Constituição Federal, e a expressa garantia de autonomia administrativa e financeira.

Segundo MORAES²⁷², “a chave do poder do judiciário se acha no conceito de independência”.

²⁷⁰ Art. 60. A Constituição poderá ser emendada mediante proposta:

[...]

§ 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:

[...]

III – a separação dos Poderes;

²⁷¹ Segundo SARLET e BRANDÃO, o *princípio da separação de poderes* tem como premissa um certo pessimismo antropológico: segundo a máxima de Lord Acton, “todo o poder corrompe”, de maneira que a concentração de todo o poder político efetivo num só órgão colocaria em risco as liberdades individuais, ante o risco do seu exercício abusivo. Portanto, o fracionamento das funções estatais em órgãos distintos e independentes tem como telos a preservação da liberdade.

²⁷² MORAES, Alexandre de. **Direito constitucional**. 32. ed. rev. e atual. até a EC nº 91, de 18 de fevereiro de 2016 – São Paulo: Atlas, 2016. p. 790

Em relação à independência do Poder Judiciário, especialmente no que concerne à sua eventual sujeição à Autoridade Nacional de Proteção de Dados, faz-se importante analisar a possibilidade de controle externo sobre suas atividades.

Conforme leciona MORAES²⁷³, há que se estudar conjuntamente o teor do art. 2º²⁷⁴ e do art. 60, §4º, III²⁷⁵, da Constituição Federal, uma vez que a junção de ambos os dispositivos demonstra que o legislador constituinte, ao proclamar a existência de poderes da República, independentes e harmônicos entre si, acompanhada de um detalhado sistema de freios e contrapesos (*checks and balances*), consistente em controles recíprocos, teve como finalidade evitar o arbítrio e garantir a liberdade individual do cidadão. Ambas as previsões vieram acompanhadas pelo manto da imutabilidade, pretendendo o legislador constituinte evitar o futuro desequilíbrio entre os detentores das funções estatais.

Assim, é necessário lembrar, dentro dessa ideia de reciprocidade de controles, que a fiscalização contábil, financeira, orçamentária, operacional e patrimonial das unidades administrativas do Poder Judiciário deverá ser realizada pelo Poder Legislativo, através do próprio Congresso Nacional, com o auxílio do Tribunal de Contas da União, no âmbito nacional.

Não obstante a impossibilidade constitucional de criação de um órgão de controle externo, a Emenda Constitucional nº 45/04 instituiu o Conselho Nacional de Justiça, dentro da estrutura do próprio Poder Judiciário, a quem compete o controle da atuação administrativa e financeira e o controle do cumprimento dos deveres funcionais dos juízes.

Por sua vez, MORAES²⁷⁶ conclui que, independentemente do posicionamento político sobre a conveniência ou não da criação e existência

²⁷³ MORAES, Alexandre de. **Direito constitucional**. p. 805

²⁷⁴ Art. 2º São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário.

²⁷⁵ Art. 60. A Constituição poderá ser emendada mediante proposta:

[...]

§ 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:

[...]

III - a separação dos Poderes;

²⁷⁶ MORAES, Alexandre de. **Direito constitucional**. p. 822

desse órgão de controle central do Poder Judiciário, três importantes pontos caracterizadores do Conselho Nacional de Justiça afastam a possibilidade de declaração de sua inconstitucionalidade, por interferência na Separação de Poderes, quais sejam: ser órgão integrante do Poder Judiciário, sua composição apresentar maioria absoluta de membros do Poder Judiciário e possibilidade de controle de suas decisões pelo órgão de cúpula do Poder Judiciário. Afirma, também, que, como bem salientou o Supremo Tribunal Federal, “a composição híbrida do CNJ não compromete a independência interna e externa do Judiciário, porquanto não julga causa alguma, nem dispõe de atribuição, de nenhuma competência, cujo exercício interfira no desempenho da função típica do Judiciário, a jurisdicional”.

A compreensão das atividades inerentes ao CNJ é de extrema importância para analisar a abrangência e o escopo da Agência Nacional de Proteção de Dados, cuja relação com o Poder Judiciário passará a ser ventilada.

3.3.2 A Autoridade Nacional de Proteção de Dados – ANPD

O cientista político, sociólogo e atuante há mais de 15 anos em conselhos consultivos de empresas de tecnologia, Andrei Gutierrez, narra que a sanção presidencial da LGPD, em 14 de agosto de 2018, foi recepcionada como uma grande vitória, após ter defendido, juntamente com uma ampla coalização de mais de 80 entidades, liderada pela Associação Brasileira das Empresas de Tecnologia e da Comunicação, perante o Presidente da República que a sanção desta Lei tratava-se de um grande pacto social de importância histórica e social de pacificação de uma sociedade dividida e pavimentação do desenvolvimento tecnológico do país.

Uma sociedade na qual os dados assumem importância crescente precisa de regras claras e mais transparência sobre a maneira como esses dados são coletados, armazenados, tratados, compartilhados e até descartados. Regras, quando equilibradas, trazem previsibilidade para os setores produtivos e confiança para os cidadãos e consumidores. E, a despeito de críticas pontuais que possa receber, a LGPD traz essa confiança e previsibilidade,

permitindo que a transformação digital brasileira avance de maneira sustentável²⁷⁷.

Considerando a relevância e alcance da LGPD, impende ressaltar que, tão importante quanto o assunto que ela regulamenta, é a maneira institucional pela qual se fará ser observada e cumprida.

A Lei nº 13.853, de 2019, que alterou disposições da LGPD, criou, por meio da inclusão do art. 55-A, a Autoridade Nacional de Proteção de Dados como um órgão da administração pública federal, integrante da Presidência da República²⁷⁸. Contudo, sua natureza jurídica poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República²⁷⁹.

Do que se observa do texto normativo, depreende-se que a ANPD passará a exercer atuação regulatória. Conforme ensina JUSTEN FILHO, a regulação econômico-social é um dos tipos de atividade estatal, que se traduz no desempenho tanto de função administrativa como legislativa, jurisdicional e de controle. Ademais, em que pese a regulação dirigir-se a disciplinar principalmente a conduta dos particulares, não se exclui a submissão dos sujeitos públicos à regulação, o que advém da forte autonomia e de competência dessas entidades administrativas para vincular a própria Administração direta²⁸⁰.

Passa-se, agora, a analisar se o Poder Judiciário, tendo em vista sua independência institucional, deverá se sujeitar aos ditames fiscalizatórios e sancionatórios da ANPD.

²⁷⁷ GUTIERREZ, Andriei. **Capítulo IX – Da autoridade nacional de proteção de dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**. n MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. LGPD: Lei Geral de Proteção de Dados. p. 392-393.

²⁷⁸ Por meio da Lei nº 13.844, de 18 de junho de 2019, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, o art. 2º, VI, dispõe que Autoridade Nacional de Proteção de Dados Pessoais integra a Presidência da República.

²⁷⁹ Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

²⁸⁰ JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. p. 456-457

Diferentemente do Regulamento Geral sobre a Proteção de Dados da União Europeia, que definiu, explicitamente, o seu âmbito de aplicação em se tratando das atividades exercidas pelo Poder Judiciário, a LGPD não cuidou de tratar sobre essa premissa. Vale transcrever o Considerando (20)²⁸¹, do GDPR, a seguir:

(20) Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. **A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização os membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento dos dados.** (Grifos nossos)

Considerando a tendência nacional em se seguir os parâmetros estabelecidos pela diretiva europeia, parece adequado concluir pela necessidade de *compliance* do Poder Judiciário com os termos da LGPD quando estiver no exercício de suas funções atípicas e administrativas, excetuando-se, portanto, a competência da ANPD como órgão fiscalizador das atividades de tratamento de dados decorrentes da função típica do Judiciário.

Ademais, o art. 103-B, §4º, da CRFB estabelece que compete ao Conselho Nacional de Justiça o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, cabendo-lhe, dentre outras atribuições: (i) zelar pela autonomia do Poder Judiciário e pelo cumprimento do Estatuto da Magistratura; (ii) zelar pela observância do art. 37 e apreciar, de ofício ou mediante provocação, a legalidade dos atos administrativos

²⁸¹ Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>>. Acesso em: 01/03/2020.

praticados por membros ou órgãos do Poder Judiciário; e (iii) receber e conhecer das reclamações contra membros ou órgãos do Poder Judiciário, inclusive contra seus serviços auxiliares, serventias e órgãos prestadores de serviços notariais e de registro que atuem por delegação do poder público ou oficializados.

O CNJ, inclusive, já manifestou em decisões que sua competência não se limita ao controle interno do Poder Judiciário; alcança também a relevante função de formular e supervisionar políticas de âmbito nacional, inclusive no que se refere à tecnologia da informação, que deve ocorrer sem negligenciar princípios e garantias constitucionais, assim como reclama indispensáveis preocupações com a segurança de dados.

Em análise à competência que a CRFB conferiu ao CNJ, identifica-se um conflito com o disposto na LGPD. Da mesma forma como foi estabelecido no GDPR, entende-se que o Poder Judiciário, quando no exercício de sua função jurisdicional, não se submete à ANPD.

Um exemplo é o caso do Poder Judiciário inglês, que mantém *Privacy Notice* (Aviso de Privacidade)²⁸² em seu sítio eletrônico com informações relacionadas aos dados pessoais de indivíduos e que, embora o *Data Protection Act 2018* (legislação similar ao GDPR em vigência no Reino Unido) conceda aos titulares de dados direitos relacionados a suas informações pessoais, tais como o direito a solicitar uma cópia das informações mantidas pela organização que realizou o tratamento dos dados, tais direitos não se aplicam aos casos em que os dados pessoais são processados pelo Poder Judiciário no exercício de suas funções jurisdicionais.

O aviso vai além e informa ao usuário que, caso deseje obter acesso às informações processadas pelo Judiciário no exercício de suas funções jurisdicionais, o mesmo poderá requerê-las de acordo com a legislação pertinente. No Brasil, um exemplo seria através da ação de habeas data.

²⁸² COURTS AND TRIBUNALS JUDICIARY. **Judiciary and Data Protection: Privacy Notice.** Disponível em <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice/> Acesso em 20/04/2020.

Conclui informando que o *Information Commissioner* não tem autoridade supervisora sobre os atos do Judiciário quando no exercício de sua função jurisdicional e informa os dados do setor responsável do próprio tribunal encarregado da Proteção de Dados Judiciais.

Seguindo a mesma linha, o Poder Judiciário da Irlanda informa expressamente que, embora a *Data Protection Commission* – a autoridade de proteção de dados irlandesa seja, em regra, responsável por supervisionar, monitorar e garantir a aplicação da lei de proteção de dados na Irlanda, as funções da referida autoridade não se estendem à supervisão dos atos e processos dos Tribunais quando atuarem nos moldes de sua competência jurisdicional. Para esses casos, o Poder Judiciário irlandês indica um Juiz responsável por supervisionar o tratamento de destes dados²⁸³.

Considerando, portanto, a garantia de independência do Poder Judiciário, o que impede fiscalização de seus órgãos pela ANPD, quando estes atuarem nos limites de sua competência jurisdicional, juntamente com a sensibilidade e alto teor técnico e especializado do conteúdo da LGPD, entende-se que CNJ deve assumir as funções fiscalizatória e normativa para garantir que os Tribunais observem os preceitos de proteção de dados pessoais previstos na referida Lei quando o tratamento de dados pessoais realizado pelos Tribunais seja decorrente de sua função típica.

Por outro lado, o papel fiscalizatório e sancionador da ANPD em relação ao tratamento de dados pessoais realizados fora do âmbito de sua função jurisdicional, o melhor entendimento, valendo-se do que dispõe o texto legislativo, é de que deverá ser observado pelos órgãos do Poder Judiciário.

3.3.3 A figura do Encarregado: deverá o Poder Judiciário nomear um DPO?

Conforme prescreve o inciso III, do art. 23, combinado com o art. 39, ambos da LGPD, as pessoas jurídicas de direito público referidas na LAI, em que

²⁸³ THE COURTS SERVICE OF IRELAND. **Processing of personal data by or on behalf of courts acting in a judicial capacity.** Disponível em <<https://www.courts.ie/courts-data-protection-notice>>. Acesso em: 17/07/2020.

se incluem os órgãos do Poder Judiciário, deverão indicar um encarregado (que passará a ser denominado DPO, em referência à terminologia internacionalmente reconhecida do *Data Protection Officer*) quando realizarem operações de tratamento de dados pessoais na condição de Controladores e representa uma função crucial na conformidade das práticas previstas na Lei Geral Proteção de Dados.

Da análise do texto legal, conclui-se que os órgãos do Poder Judiciário deverão constituir um DPO, cujas atribuições, previstas no art. 41 da LGPD, são as seguintes:

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

[...]

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Verifica-se que, tanto na Europa quanto no Brasil, cabe ao DPO receber do Controlador todas as informações que possam identificar atividade de tratamento de dados, entender todo o ciclo de vida dos dados pessoais, desde a coleta, passando pela recepção, armazenamento, até a exclusão, e dar todas as instruções necessárias para que as atividades de tratamento estejam em conformidade com as premissas estabelecidas na LGPD.

No que se refere ao Poder Judiciário, entende-se que a mesma ressalva contida no *Recital 20* do GDPR quanto à competência da ANPD sobre as atividades decorrentes da competência jurisdicional dos tribunais, deverá ser aplicada ao DPO, ou seja, o melhor entendimento é de que seja nomeado algum

membro do próprio Tribunal em questão, que fará a interlocução com o CNJ no sentido de garantir a conformidade de suas atividades com os ditames da LGPD.

De outro modo, as atividades administrativas desenvolvidas pelos órgãos do Poder Judiciário deverão ser supervisionadas pelo DPO constituído nos termos do art. 41 da LGPD, o qual deve atuar com independência e não ter ingerência sobre as atividades do Controlador, devendo apenas orientar as atividades de tratamento de dados dentro de seu escopo de atuação para que sejam realizadas em estrita observância aos termos da LGPD e fazendo, por sua vez, a interlocução com a ANPD.

CONSIDERAÇÕES FINAIS

As distopias sobre o futuro descritas em romances como 1984, Admirável Mundo Novo e Fahrenheit 451 tratam, de maneira singularmente distinta, a respeito dos impactos da evolução tecnológica sobre a privacidade, diante de sua troca por valores como a segurança, a ordem e a estabilidade social. Esse *trade-off* é possibilitado pelas novas tecnologias de vigilância e de *condicionamento* comportamental.

Em uma interpretação pessoal da autora deste trabalho do romance de Aldous Huxley, Admirável Mundo Novo, o ápice dos efeitos da perda da privacidade ocorre quando o personagem identificado como “Selvagem”, que, capaz de suportar todas as dificuldades inerentes ao convívio social, tais como o sentimento de exclusão, ausência de afetividade e o coração partido pela idealização do amor, sucumbiu diante da exposição daquilo que, para ele, era um ato sagrado de purificação, existente somente entre ele e o Criador. Quando as cenas de seu autoflagelo, gravadas às escondidas, foram transmitidas aos demais moradores da Cidade, e o Selvagem teve consciência dessa exposição, a dor e a humilhação da invasão de sua vida privada e seus segredos mais íntimos, foram insuportáveis e a ele não restou mais nada, a não ser tirar sua própria vida.

A cena acima descrita faz questionar se a humanidade está disposta a abrir mão de todos os contornos de sua privacidade em troca de valores como a segurança e a estabilidade social. A privacidade é, hoje, um valor em mutação que deixará de ser “fundamental” às futuras gerações? A humanidade está disposta a abrir mão da privacidade e dos contornos de sua vida íntima em troca de segurança e estabilidade social, permitindo a ingerência arbitrária em sua autodeterminação? Os movimentos regulatórios em torno da proteção de dados e da privacidade ao redor do mundo sugerem que, por ora, ainda não.

As legislações de proteção de dados que estão sendo editadas e hoje já integram o sistema jurídico-legal de mais de 120 países fazem parte de um esforço global para manter e restaurar os valores intrínsecos à vida privada diante

do novo paradigma da Sociedade da Informação. Além, é claro, de nivelar o campo de jogo mercadológico que hoje é dominado pelos grandes detentores das novas tecnologias de processamento de dados, no âmbito da *Data Economy*.

No que se refere aos resultados específicos da pesquisa pretendida com este trabalho, qual seja, o de analisar os reflexos da LGPD no tratamento de dados processuais pelo Poder Judiciário e sua contextualização no âmbito da Sociedade da Informação, chegou-se às conclusões a seguir descritas.

Em relação à primeira hipótese levantada (letra **a** da introdução), concernente à contribuição da evolução tecnológica que caracteriza a Sociedade da Informação para a necessidade de criação de regulação específica para salvaguardar o direito à proteção de dados pessoais, foi possível identificar a sua confirmação.

Verificou-se que as novas tecnologias disruptivas que permitiram a extração de informações relevantes em meio a uma quantidade avassaladora de dados, especialmente o trinômio *Big Data*, *Cloud Computing* e Inteligência Artificial, fomentaram a criação de um nicho econômico bilionário, caracterizado como *Data Economy*, em que os dados passaram a ser os insumos mais valiosos do mercado, sendo para a Sociedade da Informação, no conceito abrangente de Manuel Castells, o que o petróleo significou para a Sociedade Industrial, tendo sido estabelecido um novo paradigma social, econômico e tecnológico.

Foi possível identificar, também, que a Europa já tem uma cultura de proteção de dados consolidada, sendo que quase a totalidade de seus estados-membros já possuíam leis de proteção de dados pessoais em vigor. A função precípua do GDPR foi uniformizar tais leis e, especialmente, estabelecer as regras para o tratamento de dados no âmbito internacional e fixar os limites e as premissas para a efetivação da transferência internacional de dados. O Brasil, por outro lado, tem como grande desafio criar uma cultura de proteção de dados, o que se dará por meio da aplicação da LGPD e das orientações que se espera sejam editadas pela Autoridade Nacional de Proteção de Dados, cuja constituição se aguarda com grande expectativa, uma vez que, a ANPD ainda não foi formada.

Ademais, constatou-se que a LGPD reproduziu dispositivos do GDPR, norma paradigmática que serviu de inspiração para a lei brasileira, oriunda de pressões exercidas pela sociedade civil e da necessidade de se manter as relações comerciais com a Europa. O bloco europeu exige a existência de legislação robusta prevendo a proteção de dados pessoais para o intercâmbio de dados pessoais, sob pena de grande impacto econômico.

Um destaque foi para a abrangência do conceito de dados pessoais, que não se limitam somente aos dados que identificam uma pessoa de pronto, como seus dados cadastrais, por exemplo, e englobam, também, dados identificáveis, como o CEP, o IP do computador, hábitos de compras, entre outros que, por meio do cruzamento de informações, é possível identificar um indivíduo.

Conforme premissas da LGPD, o tratamento dos dados pessoais deve ser regulamentado para que não sejam usados de forma a perseguir e discriminar cidadãos, tampouco para a manipulação por meio da propaganda direcionada, de modo a não ferir a autonomia individual.

Com relação à segunda hipótese ventilada, de que a entrada em vigor da LGPD ensejará mudanças na publicidade dos atos processuais, no acesso aos processos judiciais e no acesso às bases de dados dos tribunais para a incorporação de novos avanços tecnológicos ao Sistema de Justiça (letra **b** da introdução), também foi possível constatar a sua confirmação.

Realizado o cotejo analítico dos textos normativos atualmente vigentes com os dispositivos da LGPD, concluiu-se que os tribunais deverão restringir a coleta e a disponibilização de dados pessoais ao mínimo necessário para realização de suas finalidades, para executar suas funções e atender obrigações legais, de forma proporcional e não excessiva em relação às finalidades do tratamento.

Em relação à interseção entre a LAI, que regulamentou a publicidade e transparência das informações dos órgãos públicos e a LGPD, que regulamentou a privacidade dos dados pessoais dos indivíduos, e que pese o aparente conflito entre os bens regulados, o entendimento que parece mais

adequado para garantia de conformidade com ambas as leis é a de que é possível garantir transparência ao mesmo tempo em que se garante a proteção dos dados pessoais, não havendo a necessidade de sopesar os princípios constitucionais da publicidade e da privacidade, mas sim, de harmoniza-los, no conceito operacionado por Canotilho.

A transparência deve, neste contexto, permear a atuação do Poder Judiciário, adequando os sistemas de informação e procedimentos de forma a evitar o acesso fraudulento a informações pessoais que estejam em suas bases de dados, ou seja, deverão ser adotadas medidas técnicas e administrativas de proteção de acessos não autorizados e de prevenção de incidentes com os dados, sejam eles acidentais (como um e-mail direcionado ao destinatário errado) ou ilícita (como a invasão dos sistemas), de forma a evitar a destruição, perda, alteração, comunicação ou difusão de dados pessoais.

Quanto à publicação de acórdão com dados pessoais, o entendimento adotado nesta pesquisa foi o de que, muito provavelmente, deverá ser adotado o procedimento já realizado pelos tribunais europeus, que é a supressão e até a anonimização de dados pessoais. O presente trabalho apresentou as regras de Heredia como possíveis sugestões de procedimentos a serem adotados para a proteção de dados pessoais publicados pelos tribunais nos meios eletrônicos, no processo judicial eletrônico. Destacou-se que a publicidade prevista constitucionalmente é dos atos processuais e não de todas as informações constantes do processo. Os dados pessoais tratados no âmbito do processo judicial são indisponíveis e, como tal, estão sujeitos a regramentos específicos para o seu compartilhamento e difusão.

Considerando, ainda, o princípio da não discriminação, a agregação de novas tecnologias ao cotidiano do Poder Judiciário, o que pode trazer inúmeros benefícios, benefícios estes que já podem ser identificados por meio da utilização pelo STF do sistema VITOR, deve se pautar, além dos demais princípios previstos na LGPD, na não discriminação, com destaque, neste ponto, às tecnologias de Inteligência Artificial.

Outro aspecto relevante da LGPD são os regramentos para que sejam realizadas transferências internacionais de dados pessoais. Os destaques, para o Poder Judiciário, são o armazenamento de dados em nuvem e a transferência de dados decorrentes dos processos que se conceituou, nesta pesquisa, de transjudicialização, notadamente em relação à cooperação jurídica internacional.

Quanto ao *cloud computing*, os tribunais deverão garantir que, caso os servidores receptores de dados estejam localizados em outros países, a transferência seja realizada somente a países que atendam as premissas da LGPD, após análise e autorização da LGPD. O melhor entendimento, contudo, até que se tenha um melhor alcance dos riscos, é de que o Poder Judiciário evite a utilização de programas abertos que estejam situados em outros países, pelo risco excessivo de acessos indevidos, além da fragmentação da rede, que pode ocasionar a perda de dados.

Assim, constituiu-se obrigação do Poder Judiciário garantir a segurança no acesso aos dados, de modo a evitar que haja captação indevida, prejuízos morais decorrentes do cruzamento de informações, utilização diversa da finalidade da que foram disponibilizados, garantido, ainda, a responsabilização pelo uso indevido.

Já no que se refere à terceira e última hipótese formulada, qual seja, se o Poder Judiciário, na qualidade de detentor de expressivo banco de dados pessoais decorrentes de processos judiciais, deverá observar e se sujeitar aos ditames da LGPD, haja vista as peculiaridades constitucionais e institucionais da atividade jurisdicional (letra **c** da introdução), foi possível a sua confirmação parcial.

O fato de a ANPD ainda não estar constituída e de que diversos pontos da LGPD dependem de normativa posterior pelo referido órgão para se chegar a uma conclusão mais assertiva, a presente pesquisa se baseou na realidade europeia, pelas semelhanças existentes entre a lei de proteção de dados brasileira e o GDPR e pelo sistema jurídico fundamentalmente de *Civil Law*.

Chegou-se ao entendimento de que o Poder Judiciário deverá observar os ditames da LGPD ao tratar dados pessoais, salvo quando o tratamento decorrer do exercício de sua função típica jurisdicional, consubstanciada na aplicação do Direito.

Quanto à figura do Encarregado (DPO), viu-se que, segundo o que dispõe a LGPD, o Poder Judiciário deverá efetuar tal nomeação. Ao DPO compete orientar o Controlador, normalmente identificado na figura do Presidente do Tribunal, que poderá, ou não, adotar as recomendações formuladas, devendo, contudo, observar suas limitações institucionais e legais, como a lei de responsabilidade fiscal, por exemplo.

Conforme se observou, eventual vazamento de dados, acidental ou ilícito, deve ser reportado à ANPD, que poderá adotar uma das sanções aplicáveis ao Poder Público, sendo a mais grave delas a publicização do incidente, o que pode levar à desmoralização da instituição. Como afirma GIDDENS, em uma multiplicidade de sistema abstratos, a confiança é uma parte necessária da vida cotidiana da atualidade, quer isto seja ou não conscientemente reconhecido pelos indivíduos em questão.

Os Tribunais deverão elaborar relatórios de impacto para detalhar os dados que deverão constar de acórdãos publicados, os planos de vazamentos de dados e as bases de legitimação de tratamento, conforme preceitos estabelecidos pela LGPD, restando, claro, por sua vez, que a ANPD não tem qualquer ingerência sobre as funções típicas do Poder Judiciário.

Ainda restam incertezas sobre como se dará a interlocução entre o Poder Judiciário e a ANPD. Os movimentos observados até o momento indicam que o CNJ ocupará um lugar central e atuará como o ente uniformizador do entendimento sobre a aplicação da LGPD dentro dos diversos órgãos do Poder Judiciário, notadamente em relação aos *reports* de incidentes, introdução de novas tecnologias e sanções previstas.

Da análise da LGPD foi possível extrair, também, o conceito de *Accountability*, que não significa somente a responsabilização, mas também a

prestação de contas e o controle das atividades que o órgão desempenha e ao qual está sujeito o Poder Judiciário.

Assim, para conferir maior segurança à interpretação da LGPD pelos tribunais ao reverem seus procedimentos de tratamento de dados pessoais e a elaboração de relatório de impacto, a expectativa é de que o CNJ seja o órgão que edite as normativas padronizadoras do controle de acesso aos dados processuais no âmbito dos órgãos do Poder Judiciário.

A conclusão geral, portanto, foi de que os dados pessoais não são disponíveis e são de titularidade exclusiva dos cidadãos a quem eles se referem. Correlacionando a LAI e a publicidade dos atos jurídicos, viu-se que o ato em si é público, mas os dados pessoais, não, especialmente no contexto tecnológico da Sociedade atual, em que o uso da informação dá ensejo à vigilância, a práticas discriminatórias de mercado, à manipulação dos hábitos por meio da propaganda direcionada, ao roubo de identidade e fraudes realizadas com os dados obtidos por meio de bancos de dados públicos, como o do Poder Judiciário, por exemplo, deixando o cidadão sem saída, e às escuras, seguindo o modelo operacional do Panóptico, desenhado por Jeremy Bentham.

Outrossim, verificou-se que é fundamental garantir *compliance* com a LGPD no tratamento e gestão dos dados pessoais, no sentido de que as leis devem ser interpretadas de acordo com o contexto social em que estão inseridas e que o legislador, ao editar as regras de publicidade de informações processuais no passado, não poderia imaginar a revolução tecnológica atual e os danos que o cruzamento de informações podem causar aos cidadãos, ferindo diretamente o princípio basilar da CRFB: a dignidade humana.

Diante do exposto, a regulamentação da proteção de dados, que parecer ter chegado atrasada ao atual estágio de disponibilização e compartilhamento de dados existente, pode servir para reestabelecer as regras do jogo em um ecossistema tecnológico que, a cada dia, fragiliza o direito à privacidade dos indivíduos frente à constante evolução de suas aplicações.

Para finalizar, cumpre destacar a observação feita pela advogada e DPO Andrea Willemin, atuante junto à Comissão formada pelo Tribunal de Justiça de Santa Catarina de adequação à LGPD, para quem “sem a proteção de dados, seremos somente números em um sistema computacional. Precisaremos usar uma capa de invisibilidade para sair às ruas em razão da vigilância ostensiva, que detém o condão de causar danos à nossa esfera pessoal”²⁸⁴.

²⁸⁴ Palestra realizada no Tribunal de Justiça de Minas Gerais em 12 de março de 2020. A Figura do DPO na Lei Europeia GDPR e na LGPD e suas Atribuições no Poder Judiciário. Disponível em: < <https://www.youtube.com/watch?v=UINmHGPv9qc>>. Acesso em 20/06/2020.

REFERÊNCIA DAS FONTES CITADAS

AGRA, Walber de Moura. **Curso de direito constitucional**. 9. Ed. Belo Horizonte: Fórum, 2018.

ASHLEY, Kevin D. **Artificial intelligence and legal analytics**: new tools for law practice in the digital age. Cambridge University Press, 2017

ÁVILA, Humberto. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Malheiros, 2005.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: a construção de um conceito jurídico à luz da jurisprudência mundial. Tradução: Humberto Laport de Mello. Belo Horizonte: Fórum, 2014.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2010. 2ª Ed.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 21 ed. São Paulo: Saraiva, 2000.

BECK, Ulrich; GIDDENS, Anthony Giddens; LASH, Scott. **Modernização Reflexiva**: política, tradição e estética na ordem social moderna. Tradução: Magda Lopes; revisão técnica de Cibele Saliba Rizek. 2 ed. São Paulo: Unesp. 2012. Título Original: Reflexive Modernization.

BENACCHIO, Marcelo; MACIEL, Renata Mota. **A LGPD sob a perspectiva da regulação do poder econômico**. In: Comentários à Lei Geral de Proteção de Dados. Coordenadora: LIMA, Cíntia Rosa Pereira. São Paulo: Almedina, 2020. Versão Kindle.

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

BOBBIO, Norberto. **A era dos direitos**. Tradução: Carlos Nelson Coutinho. Título original: L'età dei Diritti. Rio de Janeiro: Elsevier, 2004.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF. Diário Oficial da União, Distrito Federal, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 8 dez. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, Brasília, DF, 15/08/2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>. Acesso em: 12/12/2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da República Federativa do Brasil, Brasília, DF, 24/04/2014. Disponível em <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/30054611/do1-2014-04-24-lei-n-12-965-de-23-de-abril-de-2014-30054600>. Acesso em: 12/12/2019.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm>. Acesso em: 02/03/2020.

BRASIL, **Supremo Tribunal Federal**. Ação Penal n. 307-3/DF. Relator: Min. Ilmar Galvão. Brasília, 1994. Diário da Justiça, Brasília, 13 dez. 1994.

BRASIL, **Supremo Tribunal Federal**. Recurso Extraordinário n, 418.416/SC. Relator: Min. Sepúlveda Pertence, por maioria, Brasília, 2006. Diário da Justiça, Brasília, 10 mai. 2006.

BRASIL E SILVA, Vívian. **A necessidade de relativização do princípio da publicidade no processo eletrônico como garantia da dignidade da pessoa humana**. Disponível em <<http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3653.pdf>> Acesso em 01 jun. 2020.

CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra, Portugal: Edições Almedina, 2003.

CANOTILHO, José Joaquim Gomes. **Estudos sobre Direitos Fundamentais**. 2ª Ed. Coimbra Editora, 2008.

CASTELLS, Manuel. **A sociedade em rede: a era da informação**. Vol. I. 15ª impressão. 6 ed. Tradução Roneide Venancio Majer. São Paulo: Paz e Terra. 2012. Título Original: Rise of the Network Society: The Information Age. Original escrito em 1942

CINTRA, Antonio Carlos de Araújo, GRINOVER, Ada Pellegrini, DINAMARCO, Cândido Rangel. **Teoria Geral do Processo**. 21. ed. São Paulo: Malheiros, 2004.

COELHO, Alexandre Zavaglia Pereira; SILVEIRA, Vladimir Oliveira. **O processo de inovação tecnológica e elementos da sustentabilidade digital**. In: Direito, Inovação e Tecnologia. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015.

COLOMBO, Cristiano; FACHINI NETO, Eugêncio. **Mineração de dados e análise preditiva**: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para a sua adequada implementação à luz do ordenamento brasileiro. In: Revista de direito, governança e novas tecnologias. v. 3. n. 2. jul-dez 2017.

COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010.

CONSELHO NACIONAL DE JUSTIÇA. **Inteligência artificial na justiça**. Coordenação: José Antônio Dias Toffoli; Bráulio Gabriel Gusmão. Brasília: CNJ, 2019.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em números 2019**. Brasília: CNJ, 2019. Disponível em <https://www.cnj.jus.br/wp-content/uploads/conteudo/arquivo/2019/08/justica_em_numeros20190919.pdf> Acesso em 02 abr. 2020.

COURTS AND TRIBUNALS JUDICIARY. **Judiciary and Data Protection: Privacy Notice**. Disponível em <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice/> Acesso em 20/04/2020.

CRUZ, Paulo Márcio. **Política, poder, ideologia e estado contemporâneo**. 3 ed. Curitiba: Juruá, 2003. p. 35.

CUI, Yadong. **Artificial Intelligence and Judicial Modernization**. Springer: Singapura, 2020. eBook. English Edition.

DANTAS, Marcelo Buzaglo; OLIVIERO, Maurizio; CRUZ, Paulo Marcio. **Direito, transnacionalidade e sustentabilidade empática**. Revista do Direito, Santa Cruz do Sul, v. 2, n. 49, p. 29-45, set. 2016. ISSN 1982-9957. Disponível em: <https://online.unisc.br/seer/index.php/direito/article/view/7911/5122>. Acesso em: 27 out. 2019.

DEL BEBBIO, Alessandra. **Nuvem e proteção de dados no setor público**. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/nuvem-e-protecao-de-dados-no-setor-publico-26032019>>. Acesso em 20 abr. 2020.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 26. ed. São Paulo: Atlas, 2013.

DWORKIN, Ronald. **Uma questão de princípio**. São Paulo: Martins Fontes, 2000.

EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/>>. Acesso em: 18/08/2020

EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/>>. Acesso em: 18/08/2020

EPIC – Electronic Privacy Information Center. **Privacy and public records**. Disponível em: <<https://epic.org/privacy/publicrecords/frcpcom21506.html>>. Acesso em: 18/08/2020

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do Estado**. In: PIZOLIO, Reinaldo; GALVADÃO JÚNIOR, Jayr Viégas (Coord.). Sigilo fiscal e bancário. São Paulo: Quartier Latin, 2005.

FUSTER, Gloria González. The emergence of personal data protection as a fundamental right of the EU. Brussel: Springer, 2014.

FREITAS, Cinthia Obladen de Almendra Freitas. **O lado tecnológico da LGPD**. Disponível em <<https://www.jota.info/opiniao-e-analise/artigos/o-lado-tecnologico-da-lgpd-22032020>>. Acesso em 15 mai. 2020.

GIDDENS, Anthony. **A constituição da sociedade**. Tradução: Álvaro Cabral. 2. ed. São Paulo: Martins Fontes, 2003.

GREGÓRIO, Carlos; PAIVA, Mário. **Proteção de dados pessoais no âmbito judicial**. Disponível em <https://www.jornaljurid.com.br/doutrina/civil/protecao-de-dados-pessoais-no-ambito-judiciala-stylemso-footnote-idftn1-href_ftn1-name_ftnref1-titlespan-classmsofootnotereferencespana>. Acesso em 13 mar. 2020.

HARARI, Noah Yuval. **21 lessons for the 21st century**. London: Jonathan Cape, 2018. E-book.

HIJMANS, Hielke. **The european union as guardian of internet privacy: the story of the art. 16 TFEU**. Law, Governance and Technology Series. Springer Nature, 2016.

JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. 2. ed. rev. e atual. São Paulo, Saraiva: 2006

KANT, Immanuel. **A metafísica dos costumes**. 3ª ed. São Paulo: Edipro, 2017.

KEHDI, Andre; CORDANI, Dora Cavalcanti. **CNJ deve impedir processos em sites de busca**. Disponível em <https://www.conjur.com.br/2010-out-22/cnj-impedir-sites-busca-encontrerem-informacoes-processuais#_ftn1_7163>. Acesso em 05 mai. 2020.

KLOEPFER, Michael. **Neutralidade na rede no âmbito da Sociedade da Informação**. In: Direito, Inovação e Tecnologia. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015.

KUMAR, Sree; CHIK, Warren B.; NG, See-Kiong; TEO, Sin Gee. **The data economy**: implications from Singapore. New York: Routledge, 2019. (versão Kindle).

KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B. **The challenge of 'big data' for data protection**. International Data Privacy Law, Vol. 2, No. 2. Oxford University Press, 2012. Disponível em: <<https://academic.oup.com/idpl/article-abstract/2/2/47/755343>>. Acesso em: 24 out. 2019

LAFER, Celso. **A Reconstrução dos Direitos Humanos**: um diálogo com o pensamento de Hanna Arendt. São Paulo: Companhia das Letras, 1988.

LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001

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

LEONARDI, Marcel. **Marco Civil da Internet e Proteção de Dados Pessoais**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). Direito & Internet III: Marco civil da internet. São Paulo: Quartier Latin, 2015.

LÉVY, Pierre. **The semantic sphere 1**: computation, cognition and information economy. ISTE Ltda: Londres, 2011.

LIMA, Caio César Carvalho. **Capítulo II: Do tratamento de dados pessoais**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. LGPD: Lei Geral de Proteção de Dados. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019.

LOPES, Alan Moreira. Lei 12.965, de 23.04.2014 – estabelece princípio, garantias, direitos e deveres para o uso da internet no Brasil (marco civil da internet). In TEIXEIRA Tarcísio; LOPES, Alan Moreira. Direito das novas tecnologias. São Paulo: Revista dos Tribunais, 2015

MACCANN, Duncan. **Power and accountability in the digital economy**. Data and big tech companies have more and more power. As the digital economy develops, we need to put people and society at the centre. Disponível em <https://neweconomics.org/2019/10/power-and-accountability-in-the-digital-economy>. Acesso em 15 out. 2019

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019. Versão Kindle.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Novo código de processo civil comentado**. 3. ed. rev. ampl. São Paulo: Revista dos Tribunais, 2017.

MARQUES, Gil da Costa, CRESPO, Marcelo Xavier de Freitas. **Um panorama sobre a Sociedade da Informação: o *cloud computing* e alguns aspectos jurídicos no ambiente digital**. In: Direito, Inovação e Tecnologia. Coordenadores: Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**.

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

MORAES, Alexandre de. **Direito constitucional**. 32. ed. rev. e atual. até a EC nº 91, de 18 de fevereiro de 2016 – São Paulo: Atlas, 2016.

MORAIS DA ROSA, Alexandre. **A questão digital: o impacto da inteligência artificial no Direito**. Revista de Direito da Faculdade Guanambi, Guanambi, v. 6, n. 02, e259, jul./dez. 2019. Disponível em: <http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/259>. Acesso em 20 jun. 2020.

NERY JUNIOR, Nelson. **Princípios do processo na constituição federal**. 12 ed. rev. atual. ampl. São Paulo: Editora Revista dos Tribunais, 2016.

NEWMAN, Abraham L. **Protectors of privacy: regulating personal data in the global economy**. Ithaca: Cornell University Press, 2008.

NUNES, Marcelo Guedes; CORRÊA, Fernando; TRECENTI, Julio. **A lei francesa de acesso a dados judiciais: algumas reflexões** (2019). Disponível em <https://www.migalhas.com.br/depeso/304441/a-lei-francesa-de-acesso-a-dados-judiciarios-algumas-reflexoes#:~:text=A%20premissa%20da%20qual%20a,%C3%A0%20intimidade%20das%20pessoas%20envolvidas.>. Acesso em 28/07/2020.

PADILHA, Rodrigo. **Direito Constitucional**. 5ª Ed. Rev. Ampl. Rio de Janeiro: Forense, São Paulo: Método, 2018.

PARO, João Pedro. **A conformidade do poder judiciário à lei geral de proteção de dados**: como cada um dos Estados membros do bloco europeu está se adaptando aos novos parâmetros da diretiva? Disponível em <<https://www.jota.info/opiniao-e-analise/artigos/a-conformidade-do-poder-judiciario-a-lei-geral-de-protecao-de-dados-06062019>>. Acesso em 01 mar. 2020.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. Versão Kindle.

REMÉDIO, José Antonio; SILVA, Marcelo Rodrigues da. **O uso monopolista do Big Data por empresas de aplicativos**: políticas públicas um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e livre concorrência. Disponível em <<https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4966/3651>>. Acesso em 20 mar. 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e à privacidade. In: **Revista da Faculdade de Direito – UFPR**. . 53. 2011. Disponível em: <http://repositorio.pucrs.br/dspace/bitstream/10923/11558/2/o_direito_a_protecao_de_dados_pessoais_e_a_privacidade_r.pdf> Acesso em: 20 out. 2019.

SANTOS, Felipe Augusto dos; MORAES, Ana Paula Bagaiolo. **O direito concorrencial e a proteção ao consumidor na era do big data**. In: BAGNOLI, Vicente. Concorrência e Inovação: anais do congresso internacional para a promoção de debates acerca do direito da concorrência e inovação tecnológica diante da realidade e desafios da economia digital. São Paulo: Scortecci, 2018

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. **O direito à informação na ordem constitucional brasileira: breves apontamentos**. In: Acesso à informação como direito fundamental e dever estatal. Coordenadores: SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla; RUARO, Regina Linden. Porto Alegre: Livraria do Advogado, 2016.

SCHNEIER, Bruce. **Data and Goliath**: the hidden battles to collect your data and control your world. New York: W.W.Norton & Company, Inc., 2015.

SILVA, José Afonso. **Curso de direito constitucional positivo**. 13 ed. São Paulo: Malheiros, 1997.

SMOLLA, Rodney. **The life of the mind and a life of meaning**: reflections on Fahrenheit 451. Michigan Law Review, Vol. 107, No. 6, 2009. Survey of Books Related to the Law, pp. 895-912. Michigan Law Review Association, 2009.

STEINER, Christina M.; KICKMEIER-RUST, Michael D.; ALBERT, Dietrich. **Let's Talk Ethics**: Privacy and Data Protection Framework for a Learning Analytics Toolbox. Ethics and Privacy in Learning Analytics (#EP4LA). Poughkeepsie, United States, 2015.

STRECK, Lenio Luiz; BOLZAN DE MORAIS, Jose Luis. **Comentários à Constituição do Brasil**. Coordenação: J.J. Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. 2. ed. São Paulo, Saraiva Jur, 2008. Ebook.

Supremo Tribunal Federal. **Presidente do Supremo apresenta ferramentas de inteligência artificial em Londres**. Disponível em <<http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=422699>>. Acesso em 02 abr. 2020.

SLAUGHTER, Anne-Marie. **A typology of transjudicial communication**. University of Richmond Law Review. 29 U. Rich. L. Rev. 99 (1994). Available at: <http://scholarship.richmond.edu/lawreview/vol29/iss1/6>.

TASSO, Fernando Antonio. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice;. **LGPD: Lei Geral de Proteção de Dados**. Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019.

TAVARES, André Ramos. **Curso de direito constitucional**. 18. ed. São Paulo: Saraiva, 2020.

THE COURTS SERVICE OF IRELAND. **Processing of personal data by or on behalf of courts acting in a judicial capacity**. Disponível em <https://www.courts.ie/courts-data-protection-notice>. Acesso em 17/07/2020.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**: the data economy demands a new approach to antitrust rules. Disponível em <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>>. Acesso em 20 out. 2019

THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#preface>>. Acesso em 20 nov. 2019

THE VERGE. **IBM will no longer offer, develop, or research facial recognition technology.** Disponível em <<https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software>>. Acesso em 08 jun. 2020.

VANZOIF, Rony. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados.** Coordenadores: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019.

WALTERS, Robert; TRAKMAN, Leon; ZELLER, Bruno. **Data protection law: a comparative analysis of asia-pacific and european approaches.** Singapore: Springer, 2019. (eBook)

WARREN, Samuel; BRANDEIS, Louis D. **The right to privacy.** Foreword by Steven Alan Childress. New Orleans: Quid Pro Law Books, 2010. (Versão Kindle).

ZANON, Orlando Luiz Júnior. **Formas jurídicas.** Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), 8(3):303-317, setembro-dezembro 2016 – UNISINOS, p. 308

ZANON JUNIOR, Orlando Luiz. **Teoria Complexa do Direito.** 2 ed. Prismas: Curitiba, 2015.