PROGRAMA DE PÓS-GRADUAÇÃO
PROFISSIONAL EM DIREITO

ESCOLA NACIONAL DE FORMAÇÃO E APERFEIÇOAMENTO DE MAGISTRADOS

PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM DIREITO

ÁREA DE CONCENTRAÇÃO:
DIREITO E PODER JUDICIÁRIO/EFICIÊNCIA E SISTEMA DE JUSTIÇA

CURSO DE MESTRADO PROFISSIONAL

DANIELA BANDEIRA DE FREITAS

UMA PROPOSTA DE GOVERNANÇA DE DADOS PESSOAIS NO PODER JUDICIÁRIO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: ESTUDO DE CASO DO TRIBUNAL DE JUSTIÇA DE SÃO PAULO

TEXTO DE QUALIFICAÇÃO

BRASÍLIA/DF
2022

DANIELA BANDEIRA DE FREITAS

UMA PROPOSTA DE GOVERNANÇA DE DADOS PESSOAIS NO PODER JUDICIÁRIO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: ESTUDO DE CASO DO TRIBUNAL DE JUSTIÇA DE SÃO PAULO

Texto de qualificação, apresentado ao Programa de Pós-Graduação Profissional em Direito da Escola Nacional de Formação e Aperfeiçoamento de Magistrados, como requisito parcial para obtenção do título de Mestre (a) em Direito.

Área de concentração: Direito e Poder Judiciário. Eficiência e Sistema de Justiça.

Orientador: Professor Doutor Fabio Cesar dos Santos Oliveira.

BRASÍLIA/DF

2022

DANIELA BANDEIRA DE FREITAS

UMA PROPOSTA DE GOVERNANÇA DE DADOS PESSOAIS NO PODER JUDICIÁRIO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: ESTUDO DE CASO DO TRIBUNAL DE JUSTIÇA DE SÃO PAULO

Texto de qualificação, apresentado ao Programa de Pós-Graduação Profissional em Direito da Escola Nacional de Formação e Aperfeiçoamento de Magistrados, como requisito parcial para obtenção do título de Mestre (a) em Direito.

Área de concentração: Direito e Poder Judiciário. Eficiência e Sistema de Justiça.

Aprovado em:___/___/_____

BANCA EXAMINADORA

_____

Professor Doutor Fabio Cesar dos Santos Oliveira (orientador)

Escola Nacional de Formação e Aperfeiçoamento de Magistrados

_____

Professor Doutor Samuel Meira Brasil Junior (examinador)

Escola Nacional de Formação e Aperfeiçoamento de Magistrados

_____

Professora Doutora Luciane Amaral Corrêa Münch (examinadora)

Escola Nacional de Formação e Aperfeiçoamento de Magistrados

SUMÁRIO

1 INTRODUÇÃO

A preocupação com a proteção dos registros de dados pessoais e dados pessoais sensíveis[1], especialmente quanto ao armazenamento adequado, tratamento e circulação, em face de possíveis vazamentos ou utilização indevida e/ou ilícita, decorre de dois fatores preponderantes ao longo do século XX e que se intensificaram com o advento do século XXI. O primeiro relaciona-se com a progressão dos grandes bancos de dados públicos, na primeira metade do século XX, alicerçada em uma política totalitária, em especial na Europa, e na ideia de que o Estado deveria obter informações de seus cidadãos, em troca de bem-estar social e segurança[2]. E o segundo, sob uma perspectiva de mercado, que decorre da falta de transparência e regulação dos bancos de dados de grandes financeiras que passaram a colher informações pessoais, após a crise econômica de 1929, em especial nos Estados Unidos da América e após a Primeira Guerra Mundial, com objetivo de análise de perfil para fins de concessão de crédito e impulsionamento da economia.

Os bancos públicos de informações pessoais passaram a ser instituídos com o propósito de auxiliar a Administração Pública, nos países ocidentais, a concretizar os chamados direitos sociais ao longo da primeira metade do século XX. Enquanto tarefas constitucionais do Estado, a prestação de serviços sociais pela Administração Pública necessitava de registros de dados dos cidadãos[3] e o Estado progrediu de uma simples estrutura de dominação política para uma organização que passou a assumir funções de um "aparato prestacional".

O armazenamento de dados pelo Estado ganhou importância na gestão da Administração Pública do Estado social e decorreu, da mesma forma, da complexidade da civilização tecnológica, da urbanização crescente e, também, pelo

---

[1] A Lei Geral de Proteção de Dados Pessoais – LGPD – Lei nº 13.709/18 – considera dado sensível, segundo o artigo 5º, inciso II, aquele dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[2] No sentido de que "menos privacidade, mais segurança" é uma receita falsa, fundada na metáfora do homem de vidro, de matriz nazista. Cf. RODOTÀ, Stefano. A Vida na Sociedade da Vigilância. A Privacidade Hoje. Rio de Janeiro: Renovar, 2008. Págs. 08 a 10.

[3] No sentido de que após a Primeira Guerra Mundial, o alargamento das responsabilidades públicas poderia ter sido um pretexto para o crescimento dos modos de execução privada de tarefas públicas. Porém, não foi o que ocorreu. Das ruínas da Primeira Guerra, emergiu um poderoso Estado Administrativo que, pelos seus próprios meios, se propôs a cuidar da existência e do bem-estar dos seus cidadãos. Cf. GONÇALVES, Pedro. Entidades Privadas com Poderes Públicos. Coimbra: Almedina, 2005. Pág. 44.

fato de que a progressiva divisão de trabalho converteu o ser humano em um ser dependente de sistemas, prestações e serviços públicos[4].

A análise de perfil de dados pelas financeiras, especialmente voltadas a decisão quanto à concessão ou não de crédito, pós-crise econômica de 1929 nos Estados Unidos da América, expõe a preocupação com os registros de dados e repousa na ideia de uma necessária regulamentação por parte do Estado sobre os critérios e tipos de dados pessoais que deveriam motivar estas decisões. E, por outro lado, retrata, também, a preocupação com o volume de dados armazenados e tratados por organizações privadas para fins de circulação de moeda e crédito na economia, o que poderia representar riscos de segurança econômica e vazamento de dados pessoais.

Nesse sentido, a sociedade da informação, fruto da quarta revolução industrial[5] representa rápidas e significativas mudanças de ordem econômica, social, tecnológica e ambiental. As mudanças são decorrentes do fenômeno desenfreado da globalização, da valorização do capital intelectual, do advento da facilidade e eficiência das novas Tecnologias da Informação e Comunicação (TIC)[6] e dos desequilíbrios provocados pelo homem na natureza.

O desenvolvimento de uma sociedade baseada no uso da tecnologia, da inteligência artificial usada na construção e modelagem de sistemas e nos dados, registros de informação virtual, revela a crescente importância do controle individual dos dados e informações pessoais refletida nas legislações de proteção de dados pessoais e na jurisprudência sobre o tema.

---

[4] Neste sentido, cf. SANTAMARÍA PASTOR, Juan Alfonso. Principios de Derecho Administrativo General I. Madrid: Iustel, 2004. (Reimpressão, 2006), p. 55.

[5] Sobre a quarta revolução industrial, cf. SCHWAB, Klaus. A Quarta Revolução Industrial. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2019, p. 11 a 12.

[6] No sentido de que a Quarta Revolução industrial, que alguns autores enquadram o momento em que estamos vivendo e ao apontar para uma: "(...) sociedade baseada em máquinas computacionais, fragmentado em "bits e bytes", hipertextual, complexo, não linear. Redes sociais online, tecnologias "mobile", realidades mistas e híbridas, tecnologias de voz, vídeo imersivo, impressão 3D, inteligência artificial, internet das coisas, "chatbots" e robôs, são algumas das tecnologias e plataformas digitais que se apresentam para ampliar o nosso cenário. Somos testemunhas de mudanças profundas em todos os setores, marcadas pelo surgimento de novos modelos de negócios, pela descontinuidade dos operadores e pela reformulação da produção, do consumo, dos transportes e dos sistemas logísticos. Na sociedade, verifica-se uma mudança de paradigma em curso no modo como trabalhamos e nos comunicamos, bem como nas maneiras de nos expressarmos, nos informarmos e nos divertirmos. Igualmente, está em andamento a reformulação de governos e de nossas instituições. As novas maneiras de usarmos a tecnologia para promover a mudança de comportamentos e os sistemas de produção e consumo também formam um potencial de regeneração e preservação dos ambientes naturais." Cf. GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. São Paulo: Atlas, 2020 (4ª reimpr.), p. 15 a 17.

O capital intelectual está relacionado ao conhecimento. O conhecimento assume um papel dominante na economia, nas empresas e no trabalho e, torna-se, de fato, mais importante que a matéria-prima, ou até mesmo, que o recurso financeiro. Dessa forma, o conhecimento e a informação passam a ser considerados os produtos econômicos mais valiosos de uma organização.

Neste contexto, o sistema de justiça insere-se neste debate e na exigência normativa de adequação à nova lei de Proteção de Dados Pessoais – LGPD -, porque armazena um volume grande de dados pessoais de forma virtual, nos sistemas judiciais e administrativos de cada Tribunal e do próprio Conselho Nacional de Justiça. Se faz necessária, portanto, uma proposta de construção de uma governança de dados pessoais no âmbito de cada Tribunal, o que permitirá o exercício dos direitos previstos pela novel legislação pelos titulares de dados pessoais no Poder Judiciário e a gestão eficiente destes dados por cada Tribunal.

Por meio da governança de dados, os Tribunais definirão mecanismos de análise de processos e procedimentos que criam, abastecem ou produzem os dados, criando um sentido maior de eficiência, qualidade, transparência e proteção. A definição de governança[7] de dados abertos e de proteção de dados pessoais, bem como a governança das informações é ampla e plural. É um conceito em evolução, que envolve o cruzamento de diversas disciplinas, com foco central em qualidade de dados no sentido mais amplo. Passa pela busca de maturidade da organização na gerência desses recursos, melhoria na valoração e produção dos dados, monitoramento de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de conformidade (*compliance*), a eles associadas[8].

Os Tribunais inserem-se neste cenário e deverão definir, a partir de agora, objetivos organizacionais, rotinas e processos institucionalizados, que serão implementados dentro do equilíbrio fundamental entre tecnologia da informação e

---

[7] Owen Hughes demonstra os vários sentidos e definições técnicas e acadêmicas do conceito de "governance" ou governança e aponta que o conceito não se restringe quer ao setor público ou privado, mas perpassa os dois setores, com aplicação às corporações e organizações privadas e públicas. E que o conceito deve ser utilizado e enquadrado a depender do argumento e da hipótese em que ele será empregado. A partir desta preocupação ou premissa, analisa e aponta algumas definições básicas do conceito de governança ao longo de uma evolução histórica e, também, indica definições mais modernas do conceito a partir da análise das ideias e conclusões de alguns autores. In HUGHES, Owen. Does Governance Exist? In The New Public Governance. Emerging Perspectives on the Theory and Practice of Public Governance. Editado por Stephen P. Osborne. Londres, Nova York: Routledge, 2010, p. 87 a 104.

[8] BARBIERI, Carlos. Governança de Dados: prática, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2020, p. 52. Kindle.

outras áreas judiciais e administrativas, ao compreender que os dados não se restringem mais ao domínio da área tecnológica, mas são compreendidos como um ativo organizacional e um direito, enquanto dado pessoal, que deve ser protegido.

Os conceitos de eficiência, qualidade, transparência e proteção, atrelados ao ciclo de vida e linhagem dos dados, já são considerados em organizações privadas mais maduras. Como processo organizacional, a governança de dados estabelece políticas, padrões, processos, procedimentos e diretrizes corporativas, ao regular dados e atribuir papéis específicos para tratar esses elementos com responsabilidade e *accountability* (responsabilidade objetiva e direta). Os titulares dos dados pessoais, controladores e operadores terão que estabelecer diálogo direto com os arquitetos e gestores de dados no âmbito dos Tribunais.

A gestão pública, especialmente no âmbito do sistema de Justiça, tem suas complexidades e especificidades – convive com informações ampliadas, incertezas, redes e conexões multilaterais, relações interorganizacionais – que a distingue das organizações privadas, exigindo habilidades e conhecimentos específicos. Deve estar associada à melhoria da qualidade dos serviços prestados aos cidadãos, além da simples perspectiva econômica e financeira.

A economia informacional[9], resultante do incremento da tecnologia e da circulação de dados pessoais e corporativos no ambiente da rede mundial de computadores – internet –, acelerou o processo de troca de informações e permitiu que os dados/informações sobre pessoas e organizações passassem a ser um fim em si mesmo, com valor econômico de troca e, portanto, um ativo financeiro[10].

Este processo identificado como “monetização de dados”, ou seja, processo de atribuição de valor econômico/financeiro aos dados pessoais e

---

[9] O termo “economia informacional” é um termo equívoco e empregado em contextos diversos, inclusive na sociologia desde a década de 1970, fundado no contexto de uma economia da informação e no fortalecimento do terceiro setor do Estado. Cf. CASTELLS, Manuel. A Sociedade em Rede. Tradução de Alexandra Lemos e Rita Espanha. Sob a coordenação de José Manuel Paquete de Oliveira e Gustavo Leitão Cardoso. Lisboa: Fundação Calouste Gulbenkian, 2003. (A Era da Informação: economia, sociedade e cultura. V. 1). No sentido de que a expressão “sociedade da informação” “(...) não é um conceito técnico: é um *slogan*. Melhor se falaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar toda a mensagem como informação.” Cf. ASCENSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Rio de Janeiro: Forense, 2002, p. 71.

[10] A frase “*data is the new oil*” surgiu em 2006 dita por Clive Humby, matemático inglês, e desde então vem sendo utilizada frequentemente em publicações importantes para se referir à importância do dado e da informação na era do *big data*.

corporativos impulsionou as empresas a controlarem estas informações, como ativo e meio de capitalização e geração de receitas/faturamento.

Os avanços tecnológicos aumentaram consideravelmente a capacidade de armazenamento de informações pelos computadores, capazes de organizar e estruturar milhares de dados a custo cada vez mais baixo. E esta realidade, hoje, presente em todos os Tribunais, em razão do processo de informatização ou virtualização dos processos judiciais e administrativos e de todos os processos e rotinas, exige uma governança de proteção destes dados pessoais arquivados e registrados em sua grande maioria em meio digital e eletrônico, em razão da crescente preocupação legislativa de proteção dos dados pessoais, expressão do direito fundamental à autodeterminação informativa[11].

Segundo dados oficiais do relatório "Justiça em Números", publicado pelo Conselho Nacional de Justiça (CNJ) em 2021[12], o Poder Judiciário finalizou o ano de 2020 com 75,4 (setenta e cinco vírgula quatro) milhões de processos em tramitação.

O relatório traz a informação de que a política do Conselho Nacional de Justiça de incentivo à virtualização dos processos judiciais tem registrado enormes avanços quanto à informatização dos tribunais a cada ano. A Resolução nº 185/2013 do Conselho Nacional de Justiça que instituiu o Sistema do Processo Judicial Eletrônico (PJe) como sistema de processamento de informações e prática de atos processuais impactou, de forma significativa, o percentual de processos autuados eletronicamente que passou de 30,4% (trinta vírgula quatro por cento) em 2013 para 97,2% (noventa e sete vírgula dois cento) em 2020[13].

---

[11] Cf. LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. São Paulo: Almedida, 2020, p. 33 e seguintes. O Supremo Tribunal Federal, por sua vez e em decisão pelo pleno, teve a oportunidade de reconhecer a existência no ordenamento brasileiro do direito à autodeterminação informativa. O julgamento se deu em apreciação de medida cautelar no bojo da Ação Direta de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (ADI nº 6387 – MC/DF, Rel.(a) Min. Rosa Weber) contra a Medida Provisória nº 954/2020. Cf. https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em 30/12/2021. O Partido da Social Democracia (PSDB), o Partido Socialista Brasileiro (PSB), o Partido Socialismo e Liberdade (PSOL) e o Partido Comunista do Brasil (PCB), também, ajuizaram ações no mesmo sentido, para questionar a constitucionalidade da mesma Medida Provisória. (ADI 6388; 6389; 6390; 6393).

[12] Conselho Nacional de Justiça. Justiça em Números, 2021 (ano base 2020). Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/11/relatorio-justica-em-numeros2021-221121.pdf. Acesso em 15/12/2021.

[13] Destaca-se a Justiça Trabalhista, segmento com maior índice de virtualização dos processos, com 100% (cem por cento) dos casos novos eletrônicos no Tribunal Superior do Trabalho e 98,9% (noventa e oito vírgula nove por cento) nos Tribunais Regionais do Trabalho, sendo 96,8% (noventa e seis vírgula oito por cento) no 2º grau e 100% (cem por cento) no 1º grau e com índices muito semelhantes em todos os Tribunais Regionais do Trabalho, mostrando a existência de um trabalho coordenado e uniforme nesse segmento. Na Justiça Eleitoral, o PJe passou a ser adotado em 2017 apenas em alguns

Entretanto, embora a instituição de uma governança de proteção de dados pessoais no âmbito do sistema de Justiça represente uma evolução com impactos positivos na gestão pública do Poder Judiciário, por outro lado, ainda há desafios a serem enfrentados.

A implementação de uma governança de proteção de dados pessoais pode provocar mudanças radicais nos paradigmas que interferem em valores e princípios, tais como a autonomia e a independência decisórias do Poder Judiciário quanto à implementação das regras de *compliance* impostas pela própria Lei de Proteção de Dados Pessoais e pelas normativas do Conselho Nacional de Justiça – Recomendação nº 73/2020 e Resolução CNJ nº 363/21. Outras questões podem ser levantadas, como por exemplo: i) a dicotomia entre proteção de dados pessoais e o princípio da publicidade, como regra processual constitucional, em face da construção de uma política de sigilo; ii) a dificuldade de configuração do órgão do encarregado de dados no âmbito dos Tribunais, figura central da legislação de proteção de dados pessoais; iii) e as questões relacionadas a estruturação do modelo e formato dos comitês gestores de proteção de dados pessoais.

A Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018 - passou a permitir maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito ou norma expressa que legitime a coleta e uso dos dados e obriga às organizações públicas ou privadas a ofertar processos e rotinas aos usuários com vistas a visualizar, corrigir e excluir seus dados pessoais.

A solução destas questões passa por uma necessária governança de proteção de dados pessoais, voltada aos Tribunais e ao Conselho Nacional de Justiça, com vistas a garantir o suporte necessário aos Tribunais quanto à necessária adequação às regras de *compliance*, rotinas e processos de trabalho de forma a garantir maior eficiência no cumprimento da nova legislação.

Há, ainda, uma importante barreira a ser transposta, que é a natureza heterogênea dos formatos de dados utilizados por cada Tribunal, bem como a

---

poucos tribunais. Esse segmento possui o menor percentual de casos novos eletrônicos, tendo somente três tribunais apresentado mais de 30% (trinta por cento) dos processos ingressados de forma eletrônica. Na Justiça Federal, 94,3% (noventa e quatro vírgula três por cento), e na Justiça Estadual, 88,3% (oitenta e oito vírgula três por cento). Outros onze tribunais se destacam positivamente por terem alcançado 100% (cem por cento) de processos eletrônicos nos dois graus de jurisdição: TJAC, TJAL, TJAM, TJMS, TJPR, TJSE, TJTO, TRF4, TJMRS, STM, TRT10, TRT11, TRT13, TRT16, TRT18, TRT24, TRT7, TRT9. Conselho Nacional de Justiça. Justiça em Números, 2021 (ano base 2020). Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/11/relatorio-justica-em-numeros2021-221121.pdf. Acesso em 15/12/2021.

atribuição diferenciadas de classes de processos e movimentos processuais, o que acaba por gerar uma baixa qualidade dos dados e uma dificuldade de estruturação (bases de dados não estruturadas). Trata-se de uma barreira técnica, tanto para os provedores quanto para os consumidores de dados, e impede a sociedade de perceber a transparência, confiabilidade e a eficiência concreta dos dados[14], especialmente os dados pessoais inseridos em cada processo judicial eletrônico.

Os dados, na atualidade, representam ativo importante e hoje são protegidos pela legislação de proteção de dados pessoais, eis que segundo uma análise preditiva e analítica (ciência de dados) é possível alcançar resultados positivos e significativos de gestão nas organizações públicas e privadas, contudo, sem descuidar da proteção necessária aos dados pessoais e sensíveis.

Por isso, a padronização, a definição dos processos e procedimentos, além das medidas, estrutura de dados e definição de pessoas e políticas internas de cada Tribunal, compõem a arquitetura de uma necessária governança de dados que apresenta, como um de seus escopos, a proteção de dados individuais e sensíveis, na forma da legislação de proteção de dados. A governança de dados em sentido amplo descreve os processos utilizados e necessários para planejar, especificar, habilitar, criar, adquirir, manter, usar, arquivar, recuperar, controlar e eliminar dados e que pode atuar na infraestrutura necessária de uma nova visão de proteção dos dados pessoais. A governança de dados pode ajudar aos Tribunais a criar uma missão, alcançar transparência, aumentar a confiança no uso dos dados organizacionais, estabelecer responsabilidades, manter o escopo, o foco e definir metas.

Com o advento da Lei Geral de Proteção de Dados (Lei nº 13.079/2018) em complementação ao marco civil da internet (Lei nº 12.965/2014), completa-se o arcabouço de proteção dos direitos fundamentais da personalidade no que diz respeito à circulação de dados, com claros fundamentos no respeito à autodeterminação informativa[15], liberdade de expressão, informação, comunicação de opinião, inviolabilidade da intimidade, da honra e imagem. O âmbito de aplicabilidade da lei refere-se às operações de tratamento de dados realizadas pelas pessoas

---

[14] Cf. ATTARD, Judie. ORLANDI, Fabrizio. SCERRI, Simon. AUER, Sörenl. A Systematic Review of Open Government Data Initiatives. In Government Information Quarterly. V. 32. Ed. 4. 2015, p.399 a 418, 2015. Disponível em:https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: 12 de julho de 2021.

[15] Quanto à evolução do direito à privacidade até o reconhecimento do direito à autodeterminação informativa. Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020. 2ª Edição, p. 29 e seguintes.

naturais ou jurídicas, independentemente do meio (virtual ou físico), do país de sua sede ou dos países onde se localizam os dados, observadas as condicionantes estipuladas nos artigos 3º e 4º da Lei Geral de Proteção de Dados.

A proposta de uma governança de dados à luz da Lei Geral de Proteção de Dados terá como ponto de partida o estudo de caso do Tribunal de Justiça de São Paulo. O tema central do estudo é a governança de dados pessoais. A pesquisa utiliza-se do método de estudo de caso do Tribunal de Justiça de São Paulo.

O que se busca demonstrar é "como e de que forma" o maior Tribunal do país construiu uma arquitetura de governança de proteção de dados pessoais. E a importância deste estudo e desta pesquisa é o legado, enquanto estudo acadêmico/profissional sobre o tema, que servirá de ponto de partida para outros Tribunais, no processo de implementação desta governança e na eventual avaliação e correção em projetos já concluídos ou em fase implantação.

A atribuição da missão de implementar uma governança de dados à luz da Lei de Proteção de Dados Pessoais em um Tribunal da dimensão e porte do Tribunal de Justiça do Estado de São Paulo, tal como qualquer outro projeto que lida com sua característica mais evidente, o porte e magnitude, é tarefa que inspira cuidado e criteriosa análise no caminho a ser trilhado, pois proporcional ao seu tamanho, são as consequências quantitativa e qualitativamente decorrentes de uma decisão administrativa equivocada, dada a questão de escala, comum a todos os órgãos públicos de grande porte.

Diante do exposto, o problema de pesquisa pode ser assim definido: "como e de que forma" se desenvolveu o processo de implementação de uma governança de proteção de dados pessoais no âmbito do Tribunal de Justiça de São Paulo? A pesquisa pretende identificar os pontos positivos e negativos neste processo de implementação da governança de proteção de dados pessoais no Tribunal de Justiça de São Paulo à Luz da Lei Geral de Proteção de Dados, da Recomendação CNJ nº 73/20 e da Resolução CNJ nº 363/21.

A implantação e adequação de uma governança de proteção de dados pessoais de acordo com a Lei de Proteção de Dados Pessoais nos Tribunais encontra fundamento jurídico nas disposições normativas inseridas nos artigos 23 a 30 e 46 a 51 que determinam a aplicação desta legislação às entidades e pessoas jurídicas integrantes do conceito de Poder Público e, desta forma, às pessoas jurídicas de

direito público, integrantes do conceito de Administração Pública, e impõem boas práticas de governança e gestão de risco.

O objetivo geral da pesquisa é apresentar um estudo de caso do Tribunal de Justiça de São Paulo e identificar as dificuldades e pontos positivos no processo de conformação (*compliance*) e implementação de uma governança de proteção de dados pessoais à luz dos princípios, exigências administrativas e formas de gestão eficiente de proteção dos dados pessoais previstos pela Lei nº 13.709 de 14 de agosto de 2018 – LGPD -, pela Recomendação CNJ nº 73/20 e pela Resolução CNJ nº 363/21.

Os objetivos específicos, por sua vez, podem ser definidos da seguinte forma:

i) Em caráter introdutório, pretende-se propor um estudo do contexto histórico e do arcabouço legislativo da proteção e governança de dados pessoais, especificamente com base na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18) -, na recomendação CNJ nº 73/20 e na Resolução CNJ nº 363/21, além do Marco Civil da Internet (Lei nº 12.965/2014), Lei de Acesso à Informação (Lei nº 12.527/2011) e outras legislações afins;

ii) Na segunda parte, pretende-se apresentar uma análise do estudo de caso do Tribunal de Justiça de São Paulo, quanto ao processo de implementação de uma governança de proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18) -, a recomendação CNJ nº 73/20 e a Resolução CNJ nº 363/21, na tentativa de se apontar as dificuldades e soluções encontradas no âmbito do modelo de padronização normativa proposto pelo Governo Federal e pelo Conselho Nacional de Justiça. A pesquisa pretende realizar uma análise avaliativa, descritiva e dedutiva das dificuldades e pontos positivos da implementação de uma governança de proteção de dados pessoais no âmbito do Poder Judiciário, a partir do estudo de caso do Tribunal de Justiça de São Paulo. E propor algumas soluções, como forma de garantir o fiel cumprimento (conformidade/*compliance*) das disposições normativas quanto à matéria, especialmente no que diz respeito ao tratamento e a gestão de

> dados pessoais e sensíveis extraídos e armazenados nos processos judiciais e administrativos.

Além da normativa legal – Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 -, a Recomendação nº 73 de 20/08/2020 do Conselho Nacional de Justiça impôs, inicialmente, aos Tribunais a adoção de medidas preparatórias e ações iniciais de forma padronizada em todo país, com vistas à adequação e à conformidade de governança das disposições contidas na legislação de proteção de dados, valendo mencionar: i) elaborar um plano de ação que contemple a organização e comunicação dos dados pessoais e sensíveis, os direitos do titular, a gestão do consentimento, a retenção de dados e cópia de segurança, adequação dos contratos, um plano de resposta a incidentes de segurança com dados pessoais; ii) disponibilizar, nos sítios eletrônicos de cada Tribunal, de forma ostensiva e de fácil acesso aos usuários, informações básicas sobre a aplicação da LGPD, incluindo os requisitos para o tratamento legítimo de dados, as obrigações do encarregado e do controlador e os direitos dos titulares; além de disponibilizar formulário para exercício de direitos dos titulares de dados pessoais; iii) disponibilizar, também, no sítio eletrônico, a política de privacidade e os registros de tratamento de dados; e iv) constituir um grupo de trabalho para a implantação da LGPD.

E a Resolução nº 363 de 12/01/21 editada pelo Conselho Nacional de Justiça estabeleceu, em uma fase seguinte, as medidas necessárias ao processo de adequação de governança institucional de dados pessoais de forma padronizada e de acordo com a Lei Geral de Proteção de Dados a serem adotadas pelos tribunais, com exceção do Supremo Tribunal Federal. Destaca-se: i) criação de um Comitê Gestor de Proteção de Dados Pessoais (CGPD), com caráter multidisciplinar, responsável pelo processo de implementação da LGPD; ii) capacitação dos membros integrantes dos Tribunais em gestão de governança de dados pessoais; iii) formação de grupo de trabalho técnico em auxílio ao Comitê Gestor; iv) criação de um site próprio com informações sobre a implementação da governança de dados pessoais; v) disponibilização neste site de formulário próprio de requerimentos dos titulares de dados pessoais tratados pelos Tribunais e definição de fluxo de tramitação administrativa de apreciação destes requerimentos; vi) definição da pessoa do encarregado de dados (*data officer protection*), na forma do artigo 5º, inciso VIII da LGPD; vii) estabelecimento de política de cookies no portal institucional de cada

Tribunal, política de privacidade e de tratamento de dados pessoais e política de incidente de risco e vazamento de dados; e viii) realização de mapeamento de dados e avaliação das vulnerabilidades no tratamento de dados pessoais, com a elaboração de um plano de ação de implantação da governança de dados pessoais a ser entregue ao Conselho Nacional de Justiça e à Autoridade Nacional de Proteção de Dados Pessoais – ANPD.

As medidas previstas pela Resolução CNJ nº 363 de 18 de janeiro de 2021, acima descritas, compõem uma arquitetura de governança de dados pessoais inserida no contexto maior de governança de dados. A capacitação dos membros de cada Tribunal, bem como o mapeamento dos dados pessoais, a avaliação de riscos e, por fim, a elaboração de um plano de ação representam as medidas mais importantes no âmbito do processo de implantação.

Destaque-se que a gestão eficiente exige a proteção dos dados e informações pessoais. A recente legislação trouxe um desafio às instituições públicas e privadas que deve ser absorvido pelo Poder Judiciário como meta (macro desafio) a ser alcançada de eficiência, transparência, credibilidade, acessibilidade e segurança na gestão dos dados pessoais administrados, armazenados, compartilhados e transferidos, por meio dos processos judiciais e administrativos.

A hipótese de pesquisa, portanto: “como e de que forma” o Tribunal de Justiça do Estado de São Paulo construiu uma arquitetura de governança de proteção de dados pessoais”; – exige uma investigação que passa pela observação dos processos, extração de informações por meio de entrevistas realizadas - que serão realizadas com os magistrados e servidores - , decisões administrativas, documentos e registros que servirão de suporte concreto ao estudo de caso como método escolhido.

A pesquisa apresenta-se em caráter descritivo e dedutivo, sem prejuízo da formulação de críticas e propostas construtivas que poderão servir de auxílio aos demais Tribunais na construção da governança de proteção de dados pessoais.

A dissertação apresentará um capítulo sobre metodologia, no qual serão descritos os tipos de pesquisa, fontes de dados, instrumentos de coleta, amostra, como será realizada a análise dos dados, quais os locais de pesquisa, quais os sujeitos e personagens que farão parte da pesquisa, e por último, quais as limitações da pesquisa.

Em seguida, seguirá o capítulo de apresentação da pesquisa bibliográfica de caráter introdutório sobre o tema, no qual se pretende abordar o panorama histórico do direito fundamental à proteção de dados pessoais, a perspectiva da governança de proteção de dados pessoais no Poder Judiciário brasileiro e a necessária construção desta governança, a regulação da governança de proteção de dados pessoais e a importância do marco inicial do processo de implantação desta governança, tendo como ponto de partida os Tribunais de Justiça de Santa Catarina e São Paulo.

O conteúdo deste capítulo é apresentar um contexto histórico da relevância do tema sobre a proteção de dados e sua evolução enquanto direito e direito fundamental na legislação e na jurisprudência do Brasil e de alguns países, em especial na Alemanha e nos Estados Unidos da América. E, ainda, demonstrar que a efetividade deste direito fundamental exige a concretização de sua dimensão objetiva, com a construção de uma governança de proteção de dados pessoais, exigência esta que abrange o sistema de justiça e demanda dos Tribunais um "fazer" positivo de construção de uma arquitetura organizacional e de rotinas de fluxos de trabalho que garantam a proteção do direito à autodeterminação informativa em face dos inúmeros registros, dados e *logs* inseridos nos sistemas de dados do Poder Judiciário.

E o capítulo quatro apresentará a descrição dedutiva e avaliativa da pesquisa do estudo de caso do Tribunal de Justiça de São Paulo, dividida em três partes: 1) fase preparatória, na qual serão apresentados como ocorreu o processo de formação e capacitação sobre o tema da proteção de dados pessoais no âmbito do Tribunal de Justiça do Estado de São Paulo; 2) fase executória, na qual serão apresentadas informações e dados sobre como a administração do Tribunal pensou e de que forma concretizou os requisitos necessários à construção da governança de proteção de dados pessoais: i) quais medidas e decisões administrativas foram tomadas com o objetivo de obter o engajamento necessário de servidores, colaboradores e magistrados; e ii) de que forma foi tomada a decisão de executar o plano de implementação – gerência do projeto – pela própria administração do Tribunal; quais as questões que levaram a esta decisão e quais os impactos; e 3) etapas de implementação, tópico em que serão trazidas informações sobre a arquitetura e formato do Comitê Gestor de Proteção de Dados Pessoais; sobre a construção do plano de trabalho do projeto de implementação; sobre as ações de transparência utilizadas pelo Tribunal de Justiça de São Paulo; sobre o projeto de registro e

mapeamento das atividades de tratamento; sobre a institucionalização das medidas de garantias dos direitos dos titulares de dados pessoais; sobre as medidas de revisão dos contratos, convênios e institutos congêneres; sobre a medidas de segurança da informação e ações de gerenciamento de riscos; e, por fim, sobre a instituição do órgão do encarregado no âmbito do Tribunal de Justiça do Estado de São Paulo.

2 METODOLOGIA

2.1Tipo de pesquisa e métodos

O interesse pela hipótese e tema da pesquisa iniciou-se com uma reflexão sobre uma pequena investigação realizada na internet, por meio da qual foi possível assistir a um vídeo no *Youtube* de palestra proferida pela Desembargadora do Tribunal de Justiça de Santa Catarina, Denise de Souza Luiz Francoski, em novembro de 2019, sobre o tema da proteção de dados pessoais, em especial, no contexto do Poder Judiciário[16].

O interesse foi despertado para o tema até então desconhecido no sistema de Justiça e a respeito do qual, foi identificada a necessidade de uma investigação e pesquisa com enfoque na construção e estruturação nos Tribunais de todo país de uma governança de proteção de dados pessoais, enquanto direito fundamental dos titulares, e quais seriam as dificuldades e necessidades básicas da construção desse processo.

O cenário de crescente informatização, digitalização e virtualização dos processos judiciais faz com que os Tribunais se apresentem de forma gradativa como grandes coletores e armazenadores de grande volume de dados pessoais inseridos e registrados nos sistemas de processamento eletrônico e que merecem proteção de forma adequada à luz da atual legislação de proteção de dados e das normativas do CNJ que tratam sobre o tema.

Os portais e sítios de consulta processual na rede mundial de computadores de cada Tribunal disponibilizam um enorme conjunto de dados processuais públicos que são tratados, registrados e armazenados por bancos de dados controlados pelo Poder Judiciário. E a atividade administrativa dos Tribunais, da mesma forma, registra, trata e armazena volume grande de dados pessoais, em contratos e instrumentos congêneres, registros da vida funcional de servidores, colaboradores, magistrados e desembargadores, como registros financeiros e outros dados inseridos na gestão do Poder Judiciário.

Para além do acesso individual aos dados dos processos judiciais eletrônicos, o acesso e o tratamento dos dados de processos judiciais são atividades que fazem parte de modelos de negócios de várias empresas denominadas *legaltechs* voltadas a fornecer serviços aos profissionais jurídicos, como escritórios de advocacia

[16] Disponível em https://www.youtube.com/watch?v=1Vk6bAlLB_o. Acesso em 12 de junho de 2021.

e pesquisas acadêmicas no âmbito do ensino jurídico. Tais empresas representam um mercado em ascensão e merecem atenção dos Tribunais pois podem implicar em violação de dados pessoais cuja responsabilidade de tratamento e armazenamento pertencem e são geridos pelo Poder Judiciário.

Outro ponto de extrema relevância diz respeito à estruturação de dados dos processos judiciais para fins de desenvolvimento tecnológico de sistemas, cada vez mais com uso de inteligência artificial. É preciso construir uma governança de proteção de dados pessoais, e que propicie a supervisão quanto à extração, estruturação e tratamento de dados pessoais voltados ao desenvolvimento de sistemas, sob pena de utilização de dados pessoais e/ou sensíveis de forma indevida, ilícita e discriminatória.

Por outro lado, os riscos de vazamento e/ou tratamentos ilícitos não autorizados de dados pessoais podem gerar para os Tribunais responsabilização administrativa e implicar, até mesmo, responsabilidade do Estado ou da União Federal. E, neste ponto, vislumbra-se a preocupação no que diz respeito aos pedidos de compartilhamento de dados pessoais e sensíveis armazenados no grande volume de processos judiciais, que são constantemente solicitados por órgãos públicos e/ou privados para fins de definição de políticas públicas, pesquisas acadêmicas ou outras finalidades.

Outro aspecto relevante é a questão da política de sigilo de dados, em especial dos dados pessoais, assunto que exige esforço de reflexão do Conselho Nacional de Justiça que instituiu um Comitê Consultivo de Dados Abertos e Proteção de Dados Pessoais e do qual sou membro integrante, na qualidade de Juíza representante dos Tribunais de grande porte. Este Comitê, dentre outras atribuições, objetiva propor soluções à luz de uma governança e adequação à legislação de dados abertos e de proteção de dados pessoais[17] no âmbito do sistema de Justiça.

A participação neste Comitê no Conselho Nacional de Justiça proporciona uma visão em perspectiva dos assuntos e questões relacionados ao tema e à hipótese de pesquisa, em especial no que diz respeito às dificuldades de implementação de uma governança de proteção de dados pessoais no âmbito de cada Tribunal. E, vem

[17] Cf. Portaria CNJ nº 41 de 03/02/2021 que designou os representantes do Comitê Consultivo de Dados Abertos e Proteção de Dados Pessoais, instituído pela resolução CNJ nº 334/2020. Portaria CNJ nº 41 de 03/02/2021, disponível em https://atos.cnj.jus.br/atos/detalhar/3718. Acesso em 01/12/2021. Resolução CNJ nº 334/2020. Disponível em https://atos.cnj.jus.br/atos/detalhar/3489. Acesso em 01/12/2021.

contribuindo não só para construção e coleta de informações relevantes da pesquisa de campo no âmbito do estudo de caso do Tribunal de Justiça do Estado de São Paulo, mas também, para a reunião dos registros de documentos relevantes, por meio de compartilhamento de informações com os demais membros do Comitê.

A pesquisa possui o objetivo de auxiliar os Tribunais na construção de uma governança de proteção de dados pessoais e de auxiliar na identificação das dificuldades de ordem prática na estruturação de rotinas de trabalho, constituição do comitê gestor de proteção de dados pessoais em cada Tribunal, nomeação do encarregado e de seu formato institucional, capacitação dos membros integrantes dos Tribunais em gestão de governança de dados pessoais, formação de grupo de trabalho técnico em auxílio ao Comitê Gestor, criação de um site próprio com informações sobre a implementação da governança de dados pessoais, disponibilização neste site de formulário próprio de requerimentos dos titulares de dados pessoais tratados pelos Tribunais e definição de fluxo de tramitação administrativa de apreciação destes requerimentos, estabelecimento de política de cookies no portal institucional de cada Tribunal, política de privacidade e de tratamento de dados pessoais e política de incidente de risco e vazamento de dados e realização de mapeamento de dados e avaliação das vulnerabilidades no tratamento de dados pessoais, com a elaboração de um plano de ação de implantação da governança de dados pessoais a ser entregue ao Conselho Nacional de Justiça e à Autoridade Nacional de Proteção de Dados Pessoais – ANPD.

A pesquisa tem um caráter teórico de desenvolvimento, por meio de busca de referencial sobre o tema de governança de proteção de dados pessoais, em especial no Poder Judiciário, com investigação científica em material bibliográfico e pesquisa na internet de sites de Tribunais e instituições integrantes do sistema de justiça nacional e internacional.

A pesquisa apresenta um caráter descritivo e explicativo, por meio de estudo de caso do Tribunal de Justiça de São Paulo. A escolha pelo Tribunal de São Paulo deve-se em primeiro lugar a exigência de isenção de pesquisa, eis que na qualidade de pesquisadora e Juíza coordenadora do comitê gestor de proteção de dados pessoais do Tribunal de Justiça do Estado do Rio de Janeiro, não gozaria da imparcialidade necessária para a investigação sobre o processo de construção da governança de proteção de dados pessoais no Tribunal de Justiça do Rio de Janeiro.

Por isso e em um primeiro momento, a escolha recaiu sobre o estudo do caso do Tribunal de Justiça do Estado de São Paulo.

Em segundo lugar, o Tribunal de Justiça do Estado de São Paulo, juntamente com o Tribunal de Justiça de Santa Catarina, foram os dois Tribunais pioneiros na construção de uma governança de proteção de dados pessoais, mesmo antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais e de uma regulação pelo Conselho Nacional de Justiça.

E a escolha entre os dois Tribunais de Justiça, pelo Tribunal de Justiça do Estado de São Paulo, deve-se ao fato de que o Tribunal de São Paulo é o maior Tribunal do país, com o maior número de magistrados, desembargadores, servidores e colaboradores, além de possui o maior acervo de processos judiciais. Trata-se de um Tribunal de grande porte, segundo a classificação do relatório Justiça em Números do Conselho Nacional de Justiça[18].

Estudar o caso de São Paulo, considerada a magnitude deste Tribunal, seja sob a perspectiva da administração do Tribunal, ou da atividade jurisdicional, revela a importância da pesquisa no cenário nacional. A pesquisa qualitativa, baseada em entrevistas estruturadas e/ou semiestruturadas, como método de coleta de informações sobre o processo de estruturação da governança de proteção de dados pessoais no âmbito do Tribunal de Justiça de São Paulo, por certo deixará, como legado ao sistema de justiça, um caminho de construção da governança, rotinas de trabalho e arquitetura de órgãos e pessoas que integraram e, hoje integram, o procedimento de adequação e conformação à Lei de Proteção de Dados Pessoais e às normativa do Conselho Nacional de Justiça que regulam a matéria.

---

[18] Os Tribunais que compõem o Poder Judiciário Nacional são classificados pelo Conselho Nacional de Justiça segundo seu porte, em cada esfera federativa e em cada ramo de justiça, com o objetivo de criar agrupamentos de forma a respeitar características distintas existentes no mesmo ramo de justiça. O escalonamento dos Tribunais em pequeno, médio e grande porte é feito pela utilização da técnica estatística multivariada denominada análise de componentes principais, sendo eles a despesa total da Justiça, casos novos, casos pendentes, total de magistrados e força de trabalho, chegando-se a um fator (escore). Em sua mais recente publicação, que tomou por base os números de 2020, o Relatório "Justiça em Números" do Conselho Nacional de Justiça atribuiu ao Tribunal de Justiça de São Paulo o escore de 4,318 pontos, sendo indiscutivelmente o Tribunal de maior porte dentre os Tribunais de Justiça. Comparativamente ao escore do segundo maior Tribunal de Justiça, o de São Paulo é 3,6 maior. Em relação ao menor dos de grande porte, representa 8,8 vezes sua grandeza. Grandeza esta que, como é importante ressaltar, não se espelha, necessariamente, em eficiência, bastando uma rápida leitura dos painéis comparativos do relatório para se identificar que os demais Tribunais de grande porte por vezes superam o Tribunal de Justiça de São Paulo. Portanto, o porte de um Tribunal é utilizado no presente estudo como método comparativo a permitir dimensionar o âmbito de incidência das ações de governança de seu órgão administrativo. Conferir relatório de Justiça em números: 2021/Conselho Nacional de Justiça – Brasília: CNJ, 2021. Disponível em https://www.cnj.jus.br/wp-content/uploads/2021/11/relatorio-justica-em-numeros2021-221121.pdf. Acesso em 15/12/2021.

Ao elaborar o projeto, o tema escolhido apresentava-se, inicialmente, como um tema genérico, assim definido: “Uma Proposta de Conformação da Lei Geral de Proteção de Dados no Âmbito do Poder Judiciário.” Entretanto, especialmente ao longo da pesquisa bibliográfica e sob o processo de orientação acadêmica, se fez necessária a escolha de uma metodologia de pesquisa, o que levou à escolha do estudo de caso de um determinado Tribunal e o consequente recorte voltado à pesquisa do processo de implementação de governança de proteção de dados pessoais.

O estudo de caso, portanto, passou a dar significado e motivo concreto ao projeto, eis que a partir da observação, coleta de informações e documentos, foi possível evidenciar as dificuldades, erros e acertos no processo de implementação da governança de proteção de dados pessoais em um determinado Tribunal.

Outro recorte importante, que proporcionou a fixação do tema e dos objetivos gerais e específicos da pesquisa, foi a definição da pesquisa sobre o processo de construção e estruturação de uma governança, que passa pela análise e identificação dos processos de trabalho, dos órgãos encarregados da proteção de dados previstos na legislação e nas normativas do Conselho Nacional de Justiça, quanto ao seu modelo e formato jurídicos, e quais as medidas necessárias que foram tomadas pelo Tribunal de Justiça de São Paulo, com vistas à adequação de uma arquitetura de governança de proteção de dados pessoais.

Desta forma, partiu-se de um tema genérico de pesquisa em que se pretendia investigar e estudar a adequação da Lei de Proteção de Dados Pessoais no âmbito do Poder Judiciário, em todos os seus aspectos, sem qualquer especificação, para uma delimitação da hipótese de pesquisa voltada a investigar como se desenvolveu o processo de construção de uma governança de proteção de dados pessoais no Tribunal de Justiça de São Paulo e, assim, pesquisar quais modelos de arquitetura orgânica, mecanismos decisórios, fases de implantação e medidas tomadas, como forma de auxiliar a promoção da necessária adequação normativa.

Uma vez que o tema central da pesquisa é a governança de proteção de dados pessoais, pretende-se utilizar um ensaio comparativo do corpo funcional entre órgãos de Justiça, tomando-se como parâmetro o número de magistrados 35,82% superior e administra quadro de servidores e auxiliares 58% maior que o de toda a Justiça Federal. Conclui-se que seus 2.650 magistrados e 67.512 servidores e auxiliares são titulares de dados pessoais cujo controle está centralizado num único

tribunal, o Tribunal de Justiça de São Paulo, enquanto os 1.951 magistrados e 42.639 servidores e auxiliares da Justiça Federal estão sob o controle de uma estrutura distribuída em cinco Tribunais Regionais Federais[19]. É justamente essa a dimensão do desafio que repousa sobre a administração da Corte Paulista que deve, de forma única e centralizada, exercer a governança dos dados pessoais de seu quadro de mais de 70.000 pessoas. Do ponto de vista dos usuários da Justiça Comum Paulista, seu acervo de 19.138.363 feitos em tramitação, correspondente a 24,82% de todo o movimento judiciário nacional, reúne dados pessoais de partes e atores processuais que representam uma população de quase 46 milhões de habitantes do Estado de São Paulo[20].

É justamente essa a dimensão do desafio que repousa sobre a administração da Corte Paulista que deve, de forma única e centralizada exercer a governança dos dados pessoais de seu quadro de mais de 70.000 pessoas.

Do ponto de vista dos usuários da Justiça Comum Paulista, seu acervo de 19.138.363 feitos em tramitação, correspondente a 24,82% de todo o movimento judiciário nacional, reúne dados pessoais de partes e atores processuais que representam uma população de quase 46 milhões de habitantes do Estado de São Paulo[21]. Os números e análises comparativas compilados possuem a específica finalidade de demonstrar o maior de todos os desafios na implementação de um programa de governança de dados numa instituição pública desse porte: o problema de escala.

Não bastasse o natural estranhamento que uma norma de proteção de dados suscitou em um país como o Brasil, que não possui tradição ou histórico normativo referencial a respeito do tema, planejar, implementar e gerenciar um programa de governança de dados em conformidade com a Lei Geral de Proteção de Dados em uma instituição pública do porte do Tribunal de Justiça de São Paulo tem na quantidade de pessoas e dados a serem gerenciados, o seu maior desafio. Sob a lente do tema governança corporativa, a análise de risco e impacto é fundamental em todo e qualquer projeto de implementação e guarda estreita relação com a

[19] Dados coletados em: BRASIL. Conselho Nacional de Justiça. Justiça em Números 2021. Brasília: CNJ, 2020. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/11/relatorio-justica-em-numeros2021-221121.pdf. Acesso em 15/12/2021.
[20] Disponível em: https://www.ibge.gov.br/cidades-e-estados/sp.html. Acesso em 14/07/2021.
[21] Dados extraídos do portal do IBGE. Cf. https://cidades.ibge.gov.br/brasil/sp/panorama. Acesso em 30/12/2021.

oportunidade de valorização e qualificação da atividade fim, mas, em contrapartida, com o risco da geração de danos colaterais aos direitos fundamentais das pessoas naturais usuárias do serviço público.

Os ganhos ou danos potenciais decorrentes da escala, ao se implementar norma, que busca garantir o adequado tratamento dos dados pessoais no âmbito do poder público são igualmente grandes. Isto se dá, predominantemente, em decorrência de duas características peculiares aos entes públicos de grande porte. A primeira delas consiste na dificuldade do estabelecimento de uma comunicação interna eficiente. Diferentemente de órgãos de grande porte, os entes públicos de pequeno ou médio porte, por sua própria dimensão, reúnem a possibilidade de estabelecer uma comunicação mais direta, assertiva e melhor gerenciável do ponto de vista do número de servidores alcançados e de sua dimensão territorial. A comunicação eficiente em organismos de grande porte sempre foi e continua sendo um desafio, a despeito da profusão de novas ferramentas tecnológicas como os comunicadores instantâneos, redes sociais institucionais, *wikis*, em acréscimo aos já conhecidos periódicos oficiais eletrônicos e mensagens eletrônicas. Consequentemente, a disseminação das políticas, normas e procedimentos em uma estrutura de grande porte altamente compartimentada, dificilmente alcança setores administrativos que, embora diminutos, tratam dados pessoais de seu público interno e externo.

O controle de conformidade, após a implantação do programa de governança de proteção de dados pessoais, é o segundo e mais crítico elemento de gerência em organismos de grande porte. Controlar e corrigir é especialmente difícil quando se lida com grande volume de transações e fluxos de dados pessoais no desempenho das atividades fim e meio de um determinado Tribunal.

Acrescente-se a essa equação um elevado número de pessoas envolvidas no processo de trabalho e a dificuldade de acesso e comunicação, seja em virtude da distância ou da repetição de erros em escala decorrentes de uma capacitação ineficaz. A dificuldade em interromper o ciclo gerador de atos caracterizados como tratamento irregular de dados pessoais e disseminar o procedimento correto causa, inexoravelmente, um volume de correções pendentes (*backlogs*) que onera ainda mais a já assoberbada equipe encarregada. O ideal seria que o procedimento paradigma chegasse tempestiva e eficientemente ao servidor que, em sua atividade,

procederia ao adequado tratamento de dados pessoais, de modo a gerar um mínimo de esforço de correção e ajuste antes mesmo de ocasionar dano ao titular.

O movimento judiciário nacional consiste na somatória de casos pendentes de todos os ramos da justiça em todos os níveis federativos e dos Tribunais Superiores, não estando incluído no cômputo, portanto, o Supremo Tribunal Federal.

Chega-se à conclusão de que, nos entes públicos de grande porte, é praticamente cerebrina a hipótese de haver de fato uma comunicação interna eficiente quanto às políticas, normas e procedimentos de proteção de dados e dispor de mecanismos de controle que evitem a concretização do dano em grande escala. Há que se recorrer a uma estratégia de implementação que se inicie com o tratamento do capital humano que sustenta toda e qualquer instituição pública ou privada. É nesse contexto que a criação de uma cultura interna de proteção de dados se mostra o investimento de melhor retorno em qualquer plano de implementação de um programa de governança de dados nos entes públicos de grande porte. Foi essa constatação que, no caso em estudo, foi a propulsora da implementação da Lei Geral de Proteção de Dados no Tribunal de Justiça de São Paulo.

O exercício do cargo de Juíza auxiliar da Presidência no Tribunal de Justiça do Estado do Rio de Janeiro e a proximidade com o Juiz auxiliar da Presidência do Tribunal de Justiça do Estado de São Paulo e responsável pelo processo de implementação da governança de proteção de dados pessoais Dr. Fernando Antonio Tasso, proporcionaram o início da pesquisa de campo, por meio da realização, até então, de 4 (quatro) entrevistas semiestruturadas, por meio da plataforma de videoconferência *Teams*, com alguns dos membros que integram o órgão encarregado, o gabinete de apoio e o Comitê Gestor de Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal de Justiça do Estado de São Paulo, todos instituídos pela Portaria da Presidência do Tribunal nº 9.912/2020[22].

O método de entrevistas semiestruturadas vem proporcionando um maior campo de liberdade de observação, deixando aos entrevistados uma maior autonomia para relatar suas experiências profissionais no contexto histórico e atual da construção de uma governança de proteção de dados pessoais no Tribunal de Justiça de São Paulo. A posição de fala de cada membro integrante do órgão do encarregado, do

[22]Disponível em https://www.tjsp.jus.br/Download/Portal/LGPD/Portaria_9912_20.pdf?637755147157389963. Acesso em 10/12/2021.

Comitê Gestor de Privacidade e Proteção de Dados Pessoais e do gabinete de apoio refletem a perspectiva, experiência e avaliação que cada profissional possui sobre a implantação e estruturação da governança de proteção de dados pessoais no Tribunal.

As observações e contribuições, que cada membro vem apresentando, serão valiosas no desenvolvimento da pesquisa e do estudo de caso, não só com o objetivo de identificação do atual estágio do projeto de implantação da governança, como também, para evidenciar eventuais dificuldades e pontos positivos que contribuirão de sobremaneira como legado para outros Tribunais do país.

2.2 Fontes de dados

Os dados coletados provêm, basicamente, de material bibliográfico sobre o tema da proteção de dados pessoais e governança de dados, documentos fornecidos pelo Tribunal de Justiça de São Paulo e, principalmente de informações coletadas durante as entrevistas semiestruturadas com os membros que compõem o Encarregado, o Comitê Gestor de privacidade e proteção de dados pessoais e o gabinete de apoio.

Valiosos dados estão sendo coletados, fruto da observação e registro de informações que advêm de todos os personagens envolvidos no processo de estruturação e construção de uma governança de proteção de dados pessoais no âmbito do Tribunal de Justiça de São Paulo.

Muitas informações coletadas não possuem registro formal em documentos, como por exemplo, o registro do plano de ação de implementação da governança de proteção de dados e o fluxo de trabalho dos requerimentos/solicitações dos titulares de dados. São informações que decorrem da experiência profissional de cada servidor, magistrado ou Desembargador, envolvidos no processo de construção, e representam dados importantes, e que irão contribuir para os objetivos da pesquisa.

Outra fonte importante são as normativas do Conselho Nacional de Justiça e as leis que tratam sobre a proteção de dados pessoais, em especial a própria Lei Geral de Proteção de Dados. A análise das disposições normativas referentes às regras de governança, como as que dispõe sobre a constituição de determinados órgãos de gestão e proteção no âmbito das organizações públicas e privadas, releva

o esforço do legislador e do Conselho Nacional de Justiça de efetivar o valor objetivo que decorre do direito fundamental à proteção de dados. A governança de dados e sua arquitetura são exigências objetivas de positivação e concretização deste direito.

Outra fonte, não menos importante, são dados de pesquisas e informações coletadas na rede mundial de computadores, em especial dados sobre a política e a implementação da governança de proteção de dados pessoais em Tribunais e cortes internacionais que servirão de modelo de boas práticas voltadas às proposições desta pesquisa, enquanto legado na construção de uma arquitetura de gestão de proteção de dados pessoais pelos Tribunais.

2.3 Instrumentos de coleta

O primeiro contato realizado com o Tribunal de Justiça de São Paulo ocorreu em novembro de 2020, por meio da plataforma *Teams* de videoconferência, em que foi possível, em entrevista realizada com o Juiz auxiliar da Presidência Dr. Fernando Antonio Tasso, coletar as primeiras impressões sobre o processo de implantação de uma governança de proteção de dados pessoais no Tribunal de Justiça de São Paulo.

Esta primeira aproximação propiciou a apresentação da pesquisa e seus objetivos no contexto do Mestrado Profissional da Escola Nacional de Formação e Aperfeiçoamento de Magistrados – ENFAM -, e permitiu o estabelecimento da metodologia de entrevistas e coleta de material, que se iniciou a partir do ano de 2021.

Como forma de tornar oficial a relação entre pesquisadora e o Tribunal de Justiça do Estado de São Paulo, foi encaminhado requerimento ao órgão do encarregado de proteção de dados pessoais no âmbito do Tribunal e dirigido à pessoa do Juiz coordenador, Dr. Fernando Antonio Tasso.

O requerimento foi submetido ao colegiado, ao órgão do Encarregado, e em resposta, por e-mail, o próprio Juiz coordenador informou que foi divulgado o escopo da pesquisa e sua relevância no âmbito deste órgão, no âmbito do Comitê Gestor de Privacidade e Proteção de dados pessoais e do gabinete de apoio, com a disponibilização dos nomes e dos endereços eletrônicos de todos os membros integrantes destes respectivos órgãos.

Foi encaminhado ofício ao órgão do encarregado de proteção de dados pessoais do Tribunal de Justiça do Estado de São Paulo em 10 de novembro de 2021, dirigido ao Juiz coordenador, Dr. Fernando Antonio Tasso, solicitando a divulgação da pesquisa no âmbito do Comitê Gestor de Proteção de Dados Pessoais do Tribunal de Justiça de São Paulo e a todos os membros que compõem o órgão do encarregado de proteção de dados pessoais, além de autorização para a realização de entrevistas com servidores, colaboradores, Juízes e Desembargadores que compõem o Comitê e o encarregado[23].

[23] Teor do ofício:

"OFÍCIO

Rio de Janeiro, 10 de novembro de 2021.

Exmo. Juiz Auxiliar da Presidência e membro do Encarregado de Proteção de Dados Pessoais no âmbito do Tribunal de Justiça do Estado de São Paulo, Dr. Fernando AntonioTasso,

Cumprimento V. Exa. e venho por meu deste e-mail/ofício, informar que sou aluna da primeira turma de Mestrado Profissional da Escola Nacional de Formação e Aperfeiçoamento de Magistrados (ENFAM) e que me encontro em fase de desenvolvimento de pesquisa empírica (estudo de caso) intitulada: "Uma Proposta de Governança de Dados no Poder Judiciário à Luz da Lei Geral de Proteção de Dados: estudo de caso do Tribunal de Justiça de São Paulo."

O objetivo geral do projeto é apresentar um estudo de caso do Tribunal de Justiça de São Paulo e identificar as dificuldades e pontos positivos no processo de conformação (*compliance*) e de implantação de uma governança de proteção de dados pessoais à luz dos princípios, exigências administrativas e formas de gestão eficiente dos dados pessoais previstos pela Lei nº 13.709 de 14 de agosto de 2018 – LGPD -, pela Recomendação CNJ nº 73/20 e pela Resolução CNJ nº 363/21.

O projeto de pesquisa exige a realização de entrevistas qualitativas semiestruturadas com os servidores, colaboradores, Juízes e Desembargadores que participaram da construção da arquitetura de governança de proteção dos dados pessoais e que, hoje, compõem os órgãos integrantes desta estrutura no âmbito do Tribunal de Justiça do Estado de São Paulo.

Certa de poder contar com os bons préstimos de V. Exa. na condução dos trabalhos de pesquisa, SOLICITO:

1) a divulgação da pesquisa no âmbito do Comitê Gestor de Proteção de Dados do TJ/SP e a todos os membros que compõem o Encarregado de Proteção de Dados Pessoais;

Na sequência, houve resposta do encarregado, por meio de e-mail, em 23 de novembro de 2021 e assinada pelo Juiz coordenador, Dr. Fernando Antonio Tasso, por meio da qual, informou que a solicitação da divulgação da pesquisa e da realização das entrevistas foi acolhida pelo órgão do encarregado de proteção de dados pessoais do Tribunal de Justiça do Estado de São Paulo. Ao ensejo, foram informados os nomes dos nomes e endereços eletrônicos de todos os membros integrantes deste órgão[24].

---

2) e autorização para realização das respectivas entrevistas com os servidores, colaboradores, Juízes e Desembargadores que compõem o Comitê Gestor de Proteção de Dados do TJ/SP e o Encarregado de Proteção de Dados Pessoais.

Aproveito a oportunidade e apresento votos de estima e consideração.

DANIELA BANDEIRA DE FREITAS
Juíza Auxiliar da Presidência
Tribunal de Justiça do Estado do Rio de Janeiro

Exmº. Senhor
Dr. FERNANDO ANTONIO TASSO
Juiz auxiliar da Presidência
Tribunal de Justiça do Estado de São Paulo"

[24] Teor da resposta:

"Prezada Dra. Daniela Bandeira de Freitas,

Tenho a honra de informá-la que o pedido veiculado no ofício abaixo foi acolhido pelo órgão Encarregado, em deliberação tomada na data de hoje.

Na oportunidade, foi divulgado o escopo de pesquisa e sua relevância para o engrandecimento da pesquisa na área.

Assim sendo, informo os nomes e e-mails dos integrantes dos órgãos de governança de proteção e dados.

Encarregado
Desembargador Antonio Carlos Alves Braga Júnior - antoniocjunior@tjsp.jus.br
Desembargador Cláudio Augusto Pedrassi - cpedrassi@tjsp.jus.br
Desembargador Miguel Angelo Brandi Júnior - mbrandi@tjsp.jus.br
Desembargador Rubens Rihl Pires Correa - rihl@tjsp.jus.br
Juiz Fernando Antonio Tasso (Coordenador) – ftasso@tjsp.jus.br

Gabinete de Apoio ao Encarregado
Edivaldo Antonio Sartor – esartor@tjsp.jus.br

Até o momento, foram realizadas 4 (quatro) entrevistas com o Juiz coordenador do Encarregado, Dr. Fernando Antonio Tasso. Por meio destas entrevistas semiestruturadas, realizadas no meses de novembro e dezembro de 2021, foi possível coletar informações e dados importantes para o desenvolvimento da pesquisa, baseadas em observações e deduções, especialmente sobre do modelo de construção da governança, rotinas de fluxos dos requerimentos de proteção de dados pessoais no Tribunal de Justiça de São Paulo e quais medidas e decisões administrativas foram tomadas com o objetivo de adequar o Tribunal às normativas da Lei Geral de Proteção de Dados Pessoais, da Recomendação CNJ nº 73/20 e da Resolução CNJ nº 363/21.

2.4 Amostra

A delimitação da amostra tem por base o próprio tema que se relaciona com o conceito de governança e se refere à construção de rotinas, fluxos e processos de trabalho, estruturação de órgãos no âmbito da administração dos Tribunais, capacitação dos servidores, colaboradores, magistrados e desembargadores e aspectos específicos relacionados à proteção de dados pessoais.

Portanto, a coleta de dados e informações, por meio de entrevistas e documentos, circunscreve-se aos órgãos e membros integrantes destes que compõem a estrutura estabelecida pelo Tribunal de Justiça de São Paulo de governança de proteção de dados pessoais.

2.5 Análise dos dados

O estudo realizará três tipos de pesquisa: bibliográfica, documental e estudo de caso.

Fábio Maçoli Cláudio Matos Ramos – fmacoli@tjsp.jus.br

Comitê Gestor de Privacidade e Proteção de Dados
Gustavo Santini Teodoro (Coordenador) – gteodoro@tjsp.jus.br

Cordialmente.”

A pesquisa bibliográfica utilizará procedimento exclusivamente teórico de forma a coletar e reunir o material necessário ao desenvolvimento deste referencial da dissertação. Este procedimento se propõe a coletar fontes primárias da pesquisa: leis, jurisprudência, livros, matérias de jornais e revistas, artigos bibliográficos, documentos públicos e/ou privados e sites retirados da internet (rede mundial de computadores); e de fontes secundárias: registros não oficiais de documentos públicos e/ou privados e outros documentos e referências que não possam ser enquadradas como fontes primárias.

O procedimento de levantamento de referencial teórico destina-se a atingir o primeiro objetivo específico: propor um estudo do contexto histórico e do arcabouço legislativo de proteção e governança de dados pessoais, especificamente com base na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), na recomendação CNJ nº 73/20 e na Resolução CNJ nº 363/21, além do Marco Civil da Internet (Lei nº 12.965/2014), Lei de Acesso à Informação (Lei nº 12.527/2011) e outras legislações afins.

O estudo de caso, baseado na experiência do Tribunal de Justiça de São Paulo, destina-se a atingir o segundo objetivo específico: apresentar a análise do processo de implementação de uma governança de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), a recomendação CNJ nº 73/20 e a Resolução CNJ nº 363/21, na tentativa de se apontar as dificuldades e soluções encontradas no âmbito do modelo de padronização normativa proposto pelo Governo Federal e pelo Conselho Nacional de Justiça. A pesquisa pretende realizar uma análise avaliativa e dedutiva das dificuldades de implantação da governança de proteção de dados pessoais no âmbito do Poder Judiciário, a partir do estudo de caso do Tribunal de Justiça de São Paulo. E propor algumas soluções, de forma a garantir o fiel cumprimento (conformidade) das disposições normativas quanto à matéria, especialmente no que diz respeito ao tratamento e a gestão de dados pessoais e sensíveis extraídos e armazenados nos milhões de processos judiciais e administrativos, não só aqueles em tramitação, como os já encerrados e arquivados.

As pesquisas, documental e estudo de caso, utilizarão os seguintes procedimentos: i) análise da documentação e de todas as fases do procedimento utilizado pelo Tribunal de Justiça de São Paulo, escolhido como paradigma de estudo; ii) análise dos “erros e acertos” do procedimento de implementação de uma

governança de proteção de dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais; e iii) a descrição das etapas, decisões e ações tomadas pelos órgãos do Tribunal escolhido como paradigma.

O estudo de caso dedutivo justifica-se como metodologia de pesquisa, em razão da hipótese e dos problemas apresentados e em razão de uma experiência concreta já construída e que pode ser servir como contribuição significativa nos processos de implementação da governança de proteção de dados pessoais em outros Tribunais no país.

2.6 Locais de pesquisa

Os locais de pesquisa restringem-se ao Tribunal de Justiça do Estado de São Paulo e, especificamente, aos órgãos e membros integrantes destes que compõem a estrutura estabelecida pelo Tribunal de Justiça de São Paulo de governança de proteção de dados pessoais.

2.7 Sujeitos/personagens

Os sujeitos da pesquisa são os membros integrantes dos órgãos que compõem a estrutura estabelecida pelo Tribunal de Justiça de São Paulo de governança de proteção de dados pessoais:

> "ENCARREGADO:
>
> Desembargador Antonio Carlos Alves Braga Júnior
> Desembargador Cláudio Augusto Pedrassi
> Desembargador Miguel Angelo Brandi Júnior
> Desembargador Rubens Rihl Pires Correa
> Juiz Fernando Antonio Tasso (Coordenador)
>
> GABINETE DE APOIO AO ENCARREGADO:
>
> Edivaldo Antonio Sartor
> Fábio Maçoli Cláudio Matos Ramos
>
> COMITÊ GESTOR DE PRIVACIDADE e PROTEÇÃO DE DADOS

Gustavo Santini Teodoro (Coordenador).”

Destaque-se que entrevistas semiestruturadas com outros servidores que fizeram parte do processo de mapeamento de dados pessoais e formação de capacitação para servidores, colaboradores e magistrados poderão ser utilizadas, com o objetivo de coletar informações sobre o procedimento, sob uma perspectiva passiva. Tais informações poderão ser relevantes na identificação dos pontos positivos e negativos do processo de implementação.

2.8 Limitações da pesquisa

No atual estágio do desenvolvimento da pesquisa, podem ser identificadas duas dificuldades.

A primeira é a distância, o que impõe a realização das entrevistas e coleta de documentos e informações por meio virtual: videoconferência, envio de arquivos por *e-mail* e coleta de documentos e informações diretamente no portal da Lei de Proteção de Dados, disponibilizado ao público por *link* de acesso pelo Tribunal de Justiça de São Paulo[25].

A ausência da presença física pode prejudicar a observação e avaliação de processos e procedimentos administrativos e interferir na análise da realidade, especialmente quanto às dificuldades encontradas pela administração do Tribunal de Justiça de São Paulo.

Outra dificuldade diz respeito à própria coleta de documentos. A administração do Tribunal de Justiça de São Paulo não realizou muitos registros do processo de implementação da Lei Geral de Proteção de Dados. São poucos os arquivos em documentos. Pretende-se buscar maiores informações, fontes e relatórios, com o objetivo de propiciar uma investigação mais aprofundada.

[25] Disponível em https://www.tjsp.jus.br/lgpd. Acesso em 30/12/2021.

3 A PERSPECTIVA DA GOVERNANÇA DE DADOS PESSOAIS NO PODER JUDICIÁRIO BRASILEIRO

3.1 O contexto histórico do direito à proteção dos dados pessoais

A história da proteção de dados pessoais coincide com a necessidade de compilação de dados pessoais pelo Estado, como instrumento de registro de dados para fins de prestação de direitos sociais. A construção de grandes bancos de dados públicos motivou uma preocupação inicial, no início do século XX, com a questão da privacidade, uma vez que o Estado estaria interferindo na ordem privada do cidadão, ao compilar e armazenar dados pessoais e individuais, com a possibilidade, inclusive, de compartilhamento com outras autoridades no âmbito da Administração Pública.

Em um primeiro momento, a ideia de privacidade, ou melhor, de direito à privacidade, desenvolve-se no contexto de emergência política da importância do indivíduo e do delineamento de uma esfera privada, intimamente ligada, em seus primórdios, à própria noção de propriedade, longe do alcance do Estado e em reação ao absolutismo[26]. E nesse contexto, Warren e Brandeis[27] oferecem uma articulação do direito à privacidade que aponta para a fundamentação desvinculada do direito à propriedade, ao definir o centro de racionalidade daquele direito no conceito de inviolabilidade da pessoa[28]. E, desta forma, o direito à privacidade ganha o contorno de um verdadeiro direito geral da personalidade[29].

Entretanto, o direito à privacidade, a partir da década de 1970[30], com o incremento do processamento de dados pessoais por meio digital, em razão do desenvolvimento da tecnologia e dos grandes bancos de dados públicos e, agora, de empresas privadas, tornou-se insuficiente enquanto pensado sob a simples

---

[26] Neste sentido, cf. WESTIN, Alan. Privacy and Freedom. New York: Atheneum, 1967, p. 369.

[27] No sentido de que o direito à privacidade ganha uma feição autônoma e decorre daquilo que os autores intitularam de "o direito de estar só": "*right to be alone*". Cf. WARREN, Samuel D. BRANDEIS, Louis D. Harvard Law Review. v. IV, nº 5, dec. 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em 03/12/2021.

[28] Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: revista dos Tribunais, 2020. 2ª Edição, p. 96.

[29] Cf. SCHWARTZ, Paul M. PEIFER, Karl-Nikolaus. Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept? California Law Review. vol. 98, p. 1925. 2010. UC Berkeley Public Law Research Paper nº. 1816885. Disponível em SSRN: https://ssrn.com/abstract=1816885. Acesso em 01/12/2021.

[30] No sentido de que era necessário que medidas fossem tomadas para assegurar a privacidade diante de uma nova interpretação deste direito frente ao incremento dos bancos de dados pessoais informatizados. Cf. WESTIN, Alan. Privacy and Freendom. New York: Atheneum, 1967, p. 351.

perspectiva da proteção do indivíduo, diante da necessária e atual proteção dos dados pessoais na sua dimensão de controle pelos seus respectivos titulares[31].

O aumento dos chamados registros digitais de informações e dados pessoais no âmbito da rede mundial de computadores e o incremento dos bancos de dados pessoais públicos e privados que permitem a entidades e organizações públicas e privadas tomarem decisões sobre cada indivíduo, baseada em seu perfil de dados, para fins de prestação de serviços públicos, decisões sobre políticas públicas e decisões para fins comerciais de venda de serviços e produtos no mundo corporativo, gerou a preocupação, na esfera jurídica, de se construir uma nova interpretação do direito à privacidade que pudesse ensejar o reconhecimento de um direito fundamental autônomo e implícito, extraído de uma interpretação da própria Constituição: o direito fundamental à proteção dos dados pessoais.

A nova realidade tecnológica e digital, diante da rapidez do desenvolvimento do *Big Data* e do *Data Analitics*, ferramentas que utilizam a inteligência artificial para armazenar, tratar e analisar dados pessoais, e que servem de auxílio na tomada de decisões estratégicas de cada organização, motivou o avanço da interpretação da Constituição pela jurisprudência dos Tribunais, especialmente no que respeita ao direito fundamental à privacidade, ao sigilo das informações e comunicações, e aos instrumentos constitucionais de acesso e retificação de dados pessoais[32].

Uma economia, cada vez mais crescente, baseada em dados e informações, revela importante ponto de partida para a compreensão da necessidade de proteção dos dados pessoais, enquanto direito fundamental a ser protegido pela Constituição. Este fenômeno apresenta repercussões nas esferas individuais de cada cidadão, eis que os dados ganharam importância, tornando-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia. Vistos como o novo petróleo, os dados são hoje insumos essenciais para as atividades econômicas e públicas, com reflexos essenciais na definição de políticas públicas e prestação de serviços pelo Estado[33].

---

[31] Cf. LEONARDI, Marcel. Tutela e Privacidade na Internet. São Paulo: Saraiva, 2012, p. 53.
[32] Cf. BENNET, Colin. Regulating Privacy. Data Protection and Public Policy in Europe and the United States. Ithaca and London: Cornell Univerty Press, 1992, p. 44.
[33] Cf. SRNICEK, Nick. Platform Capitalism. Cambridge: Polity Press, 2018, p. 39.

Diante deste contexto, não só a jurisprudência, como os legisladores, a partir da década de 1970, passaram a refletir a preocupação com um direito à proteção de dados pessoais[34], em sua dimensão subjetiva de proteção dos dados enquanto direito individualmente considerado e regulado pela ordem jurídica, e, da mesma forma, em sua dimensão objetiva, de garantia de estruturas, autoridades e instrumentos processuais que pudessem concretizar e positivar as disposições normativas de proteção dos dados pessoais. Este movimento jurídico reflete a preocupação da sociedade com a necessidade de se garantir proteção ao controle pessoal de cada indivíduo sobre suas próprias informações e dados pessoais, especialmente quanto à possibilidade dos direitos dele decorrentes, como direito de acesso, retificação e eliminação de dados pessoais.

A proteção de dados pessoais, no contexto financeiro e de concessão de crédito nos Estados Unidos da América, alimentou as preocupações com riscos de segurança, vazamento e monopólio exclusivo de informações pessoais por agentes econômicos privados, o que culminou com a edição de um conjunto de leis federais sobre privacidade de dados pessoais na década de 1970 que acabaram por influenciar algumas legislações brasileiras[35] quanto à matéria. O *Privacy Act* de 1974, por sua vez, é a primeira lei norte-americana que passou a reconhecer a existência de um *general right to privacy*[36]. Porém, mesmo até os dias atuais, sua eficácia é limitada, ao se aplicar, somente, a órgãos federais, sobre os dados pessoais armazenados e tratados[37].

A preocupação com a privacidade é mais antiga do que a rede mundial de computadores e do que se pode retirar do enredo da ficção distópica de George Orwell em 1984 que descreve a supressão da individualidade ou privacidade como método

---

[34] Sobre as primeiras leis que passaram a reconhecer o direito à proteção de dados pessoais. Cf. MONCAU, Luiz Fernando Marrey. Direito ao Esquecimento. São Paulo: Thomson Reuters Brasil, 2020. Pág. 128 a 132.

[35] No sentido de que em 1970, o *Fair Credit Reporting Act (FCRA)*, que posteriormente influenciou a legislação brasileira na matéria e estabeleceu obrigações de segredo e correção para dados financeiros de consumidores tratados por operadores de cadastros de crédito de consumo. Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2019. 2ª Ed, p. 239.

[36] Sobre o desenvolvimento do conceito de *general right do privacy* no direito norte-americano, cf. Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2019. 2ª Ed, p. 222 a 239.

[37] Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2019. 2ª Ed, p. 240.

de manutenção do poder. A preocupação com a privacidade[38], da qual decorre a proteção de dados pessoais, foi expressa por Samuel Warren e Louis Brandeis no célebre artigo *The* Right *to Privacy*, publicado na Harvard Law Review em 1890. Neste artigo, os autores questionam se haveria, no *common law*, um fundamento para a proteção à privacidade dos indivíduos, e qual seria sua natureza e extensão[39].

Ao longo do século XX, na Europa, na mesma linha das preocupações com a privacidade dos dados pessoais, especialmente quanto aos dados coletados pela Administração Pública, por meio de grandes bancos de dados públicos, as legislações avançaram no sentido de uma proteção e regulação cada vez mais intensas[40]. A primeira tentativa de elaborar um sistema de proteção de dados em país europeu foi a Lei de Proteção de Dados pessoais do *Lande* de Hesse em 1970 na então Alemanha Ocidental. Esta lei foi pioneira ao instituir o primeiro comissário para proteção de dados pessoais. E após outros estados alemães terem editado leis semelhantes, foi promulgada lei federal sobre a matéria em 1977[41].

Das várias leis editadas no cenário europeu, foi possível extrair um núcleo de princípios comuns que orientou iniciativas de normatização internacional. A Organização para Cooperação e Desenvolvimento Econômico (OCDE), em 1978, instituiu um grupo de especialistas para elaborar uma normativa modelo para o tráfego internacional de dados. Posteriormente, o Conselho da Europa, na mesma época, decidiu tratar da matéria de proteção de dados com uma convenção, considerada o primeiro passo para um sistema integrado europeu de proteção de dados pessoais, a convenção nº 108/1981, conhecida como Convenção de Strasbourg. Estas duas

---

[38] Sobre uma visão geral da privacidade e proteção de dados, cf. MONCAU, Luiz Fernando Marrey. Direito ao Esquecimento. São Paulo: Thomson Reuters Brasil, 2020, p. 112 e seguintes.

[39] Cf. WARREN, Samuel D. BRANDEIS, Louis D. Harvard Law Review. v. IV, nº 5, dec. 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em 03/12/2021. Os autores expõem que a quebra de um contrato e da confiança foi utilizada para solucionar muitos casos, porém a violação da vida privada nem sempre será atribuível a um contratante. Também o direito de propriedade, invocado para proteger os bens imateriais, não mais seria suficiente no mundo moderno e terminam por indicar que a proteção da vida privada repousa sobre o direito à privacidade que, por sua vez, é afeto ao direito mais amplo de personalidade. Embora o artigo seja usualmente considerado precursor do tema, os próprios autores dão notícia de sua ocupação pelo direito francês.

[40] No sentido de que a primeira lei nacional sobre proteção de dados pessoais foi a lei sueca sobre o controle de banco de dados de 1973. E que logo a seguir vieram leis em outros países europeus: na França, a Lei 78-17 de 06 de janeiro de 1978 que instituiu a CNIL – Commission Nationale de L'Informatique e des Libertés – como órgão encarregado de zelar pela aplicação da lei. E que outros países legislaram à época sobre esse tópico, como Dinamarca, Áustria, Noruega, Luxemburgo e Islândia. Cf. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2019. 2ª Ed, p. 191/192.

[41] Cf. SIMITIS, Spiros. Crisi Dell'informazioni Giuridica ed Elaborazione Elettronica dei Dati. Milano: Giuffrè, 1977, p. VIII.

normativas contribuíram para edição das Diretivas 95/46/CE e 2002/58/CE e para a formação do sistema europeu de proteção de dados que foi aprimorado com introdução do artigo 8º na Carta dos Direitos Fundamentais da União Europeia, que, por sua vez, reconheceu o direito à proteção de dados pessoais como direito fundamental. Recentemente, a edição, em 2016, do Regulamento Europeu de Proteção de Dados Pessoais – GDPR, que entrou em vigor em 25 de maio de 2018[42], passou a dispor, de forma mais precisa, este direito fundamental. O Regulamento Europeu expõe, em seu conteúdo, regras que concretizam as dimensões subjetivas e objetivas da proteção de dados no âmbito da União Europeia[43].

A tutela constitucional do direito à proteção de dados, por sua vez, está relacionada: i) à proteção da liberdade (liberdade em face da intervenção do Estado e liberdade de mercado) e da personalidade, como dignidade da pessoa humana[44]; ii) à segurança jurídica no que toca ao adequado armazenamento, compartilhamento e tratamento de dados pessoais; iii) à inovação, eis que os dados pessoais são o motor e o material necessários à construção de sistemas com uso de inteligência artificial[45]; iv) ao conceito de democracia, eis que os dados pessoais ganham importância em um cenário de análise de perfil político-eleitoral de cada cidadão, com uma possível perspectiva de análise de perfil eleitoral e possível influência no resultado de determinada eleição; e, ainda, no sentido de que o controle excessivo dados pessoais poderia propiciar um cenário de vigilância total e limitar de sobremaneira o exercício da liberdade individual; v) à livre comunicação que está intimamente ligada ao sigilo do fluxo de informações e o necessário equilíbrio com a liberdade de expressão; vi) e, por fim, ao valor igualdade que vincula o desenvolvimento de algoritmos para sistemas com uso de inteligência artificial e que exigem supervisão para que a escolha dos dados pessoais não provoquem discriminações não razoáveis ou ilegítimas.

---

[42] Cf. VENTURA, Leonardo Henrique de Carvalho. Considerações sobre a Nova Lei Geral de Proteção de Dados. Revista Síntese: Direito Administrativo, v. 13, n. 155, nov. 2018, p. 56-64.

[43] Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434#B-1. Acesso em 02/01/2021.

[44] No sentido de que nos Estados Unidos o centro de racionalidade do direito à privacidade possui fundamento no direito à liberdade em face do Estado e da liberdade de mercado e que na Europa continental, se desenvolveu a ideia de que a privacidade decorre da dignidade da pessoa humana, enquanto direito da personalidade. Cf. MONCAU, Luiz Fernando Marrey. Direito ao Esquecimento. São Paulo: Thomson Reuters Brasil, 2020, p. 118 e119.

[45] Cf. Resolução do Parlamento Europeu de 06 de outubro de 2021, sobre a inteligência artificial no direito penal e sua utilização pelas autoridades policiais e judiciárias em casos penais: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso em 02/01/2021.

A proteção de dados, portanto, vai muito além da proteção da privacidade, em uma perspectiva evolucionista do direito e envolve valores objetivos de proteção do sistema jurídico, tais como: controle, democracia, liberdade, personalidade e igualdade.

A evolução jurisprudencial apresenta um marco importante na decisão da corte constitucional alemã relacionada à proteção de dados – *Volkszählungsurteil* - sobre caso do censo demográfico, julgado pelo Tribunal Constitucional Federal em 15.12.1983. O caso versou sobre diversas reclamações constitucionais ajuizadas por grupos de cidadãos que impugnavam a lei federal de recenseamento alemã, editada em 1982, que havia sido aprovada por unanimidade tanto pelo Parlamento quanto pelo Conselho Federal. O texto legal previa que no ano de 1983 seria realizado um censo por parte de funcionários públicos e demais agentes encarregados, que não se limitaria apenas a fazer o levantamento do número de habitantes do país, mas também coletar uma série de outros dados pessoais dos cidadãos. Em sede liminar, o Tribunal Constitucional Federal suspendeu os efeitos da lei de recenseamento e acabou por julgar parcialmente procedentes as reclamações constitucionais. Em sua base, a realização do censo foi mantida, mas foi consideravelmente modificada, conforme as ordens do Tribunal, para que fosse procedida por meios que resguardassem a segurança dos dados dos cidadãos a serem entrevistados, como por exemplo, pela proibição de que alguns dados obtidos, como nome e endereço, fossem transferidos a outros órgãos de governo.

O contexto histórico da época, dentre outros fatores, era influenciado pela acentuada onda de protestos contra o censo e os temores dos cidadãos alemães com relação às previsões do livro 1984, de George Orwell, que chamava a atenção para os perigos do “Estado espião”. Havia, portanto, uma proximidade temporal entre o ano da realização do censo (1983) e o ano 1984, do título do livro de Orwell. Além disso, o desenvolvimento computacional da época situava-se em estágio inicial, no qual o armazenamento e o tratamento de dados se davam a partir de grandes computadores centralizados, pesados e volumosos, não havendo a disseminação e a descentralização da informação hoje presente com a Internet e com a acessibilidade a computadores pessoais, onde a grande maioria das pessoas é, além de usuário da informação, produtor da informação.

Esta decisão foi tão impactante e consistiu em um verdadeiro marco da proteção de dados, por ter fixado várias diretrizes desta disciplina que influenciaram legislações, doutrina e jurisprudência de diversos países.

O direito à autodeterminação informativa - *informationelle Selbstbestimmung -,* reconhecido nesta decisão como direito autônomo e implícito na Constituição alemã e como âncora constitucional da proteção de dados, integra o denominado direito geral da personalidade. O direito geral da personalidade vem sendo desenvolvido pelo Tribunal Constitucional Federal desde os anos 1950 e é derivado da combinação do Art. 1º, §1º (dignidade da pessoa) e Art. 2º, § 1º (liberdade) da Lei Fundamental, ou seja, a sua atuação em conjunto garante a cada indivíduo a possibilidade de desenvolver a sua própria personalidade.

A lei do censo alemã acaba declarada inconstitucional em apenas dois artigos, em especial aqueles que tratavam sobre o compartilhamento de dados entre entidades e autoridades públicas da Administração Pública. A Alemanha já possuía, nesta altura, uma lei federal de proteção de dados e alguns estados também possuíam leis estaduais. Porém, a lei federal alemã na época não vinculava o legislador infraconstitucional, eis que até a decisão da corte constitucional não havia o reconhecimento expresso na ordem jurídica alemã do direito à autodeterminação informativa. Desta forma, com a decisão do Tribunal Constitucional, passou a vincular o legislador, o executivo e o poder judiciário.

A corte alemã também decidiu que qualquer dado, mesmo que insignificante precisa de proteção, em razão da possibilidade de cruzamento e compartilhamento e em razão do possível potencial para gerar danos. Reconheceu, ainda, que a autodeterminação informativa encontra limites, enquanto direito, especialmente no que diz respeito à exigência de circulação e liberdade de expressão e informação. Os dados precisam fluir como ativo econômico e público e, por isso, o direito à proteção encontra limites em outros direitos fundamentais, tais como a liberdade de expressão e comunicação. A limitação deve estar fundada em lei ou ato normativo, que deve especificar a finalidade do tratamento. E este deve ser proporcional a finalidade almejada pelo ente, autoridade pública ou organização, em respeito aos princípios da finalidade e proporcionalidade.

Na Alemanha, inicialmente, se reconheceu, portanto, que a aplicação do direito à autodeterminação informativa seria oponível apenas ao Estado, em uma perspectiva de eficácia vertical deste direito fundamental. À medida que a tecnologia

avançou, percebeu-se que não só o Estado acarreta riscos à proteção de dados, mas também as empresas privadas que passaram a coletar e tratar dados com fins econômicos e comerciais. A corte alemã, então, passou a reconhecer, a eficácia horizontal do direito à autodeterminação informativa. Duas decisões jurisprudenciais representam o marco desta interpretação e aplicação: i) a primeira, de 1991, uma decisão sobre a celebração de contrato de aluguel por uma pessoa interditada que teria omitido esta condição jurídica. O locador pediu a rescisão do contrato, e a corte constitucional reconheceu o direito quanto à omissão da informação pelo locatário, sob o argumento de que ele não conseguiria celebrar nenhum contrato de aluguel e que não havia a obrigação de informar, em razão do risco de estigma; ii) e a segunda, refere-se a um contrato de seguro em que o segurado é obrigado a informar dados pessoais sem opção de escolha quanto aos dados a serem coletados. O segurado pleiteou que algumas informações não fossem prestadas à seguradora e argumentou que não tinha opção. A corte constitucional reconheceu a eficácia horizontal do direito à autodeterminação informativa, sob o argumento de que é preciso que sejam dadas alternativas ao segurado quanto ao fornecimento de dados[46].

Em 2008, em julgado do Tribunal Constitucional Federal, foi reconhecido mais um novo direito fundamental, em certa medida um desdobramento do direito fundamental à autodeterminação informativa: o denominado direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais, proclamado no contexto de uma reclamação constitucional ajuizada contra dispositivos da lei do Estado de *NordrheinWestfalen* que regulamentava e permitia a denominada busca ou investigação remota de computadores de pessoas suspeitas de cometerem ilícitos criminais[47].

No Brasil, o direito à autodeterminação dos dados e informações pessoais encontra amparo na Carta de 1988 e na Lei Geral de Proteção de Dados (LGPD). O artigo 5º, inciso XII da Constituição Federal assegura que “é inviolável o sigilo de 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

[46] Cf. MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Edição Kindle. Posição 495 a 555.
[47] Cf. MENKE, Fabiano. A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão. In Revista Luso-Brasileira (RJLB), ano 5 (2019). nº 1, p. 781 a 809.

assim, o artigo 2º, inciso II, da Lei *Geral* de Proteção de Dados elenca a autodeterminação informativa como um dos fundamentos da proteção dos dados pessoais. O inciso X do art. 5º da Constituição, por seu turno, assegura a inviolabilidade da intimidade e da vida privada, da honra e da imagem das pessoas.

No Brasil, portanto, a proteção de dados pessoais é objeto de tratamento constitucional – artigo 5º, inciso X da CRFB/88 – e, também, por legislações ordinárias: a lei do *Habeas Data* – Lei nº 9.507/1997 -; a lei de Arquivos Públicos – Lei nº 8.159/1991 -; o Código Civil – Lei nº 10.406/2002 -; o Código de Defesa do Consumidor – Lei nº 8.078/90 -; a Lei de Acesso à Informação – Lei nº 12.527/2011 -; a lei do Cadastro Positivo – Lei nº 12.414/2011 -; e, mais recentemente, o Marco Civil da Internet – Lei nº 12.965/2014 e a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 18 de setembro de 2020 no sistema jurídico brasileiro passou a ter como objetivo específico a proteção dos dados considerados pessoais e sensíveis, assim definidos pela então legislação, bem como proteger e dar tratamento técnico e jurídico à circulação, transferência e compartilhamento destes mesmos dados pessoais entre pessoas jurídicas de direito privado e público. Esta legislação, com inspiração no Regulamento Europeu de Proteção de Dados Pessoais, foi uma resposta à Lei do Marco Civil da Internet (Lei nº 12.965/2015) que indicou a proteção de dados pessoais, na forma de lei específica, como um princípio do uso da internet no Brasil. Portanto, a edição da Lei de Proteção de Dados pode ser compreendida como a concretização de um dos princípios do uso da internet[48] e como uma legislação que passou a tratar a proteção e dados pessoais como um direito a ser regulado e tratado de forma autônoma.

Em novembro de 2010 teve início no Brasil o debate sobre a proteção de dados pessoais, com o propósito de se elaborar uma lei específica sobre o tema.-Até abril de 2011, foram colhidas manifestações por meio de um *blog* mantido na plataforma Cultura Digital, do Ministério da Cultura. O resultado desse primeiro debate nunca chegou a ser enviado pelo Poder Executivo.

---

[48] No sentido de que as legislações existentes que tratavam no Brasil sobre a proteção de dados eram insuficientes, bem como a proteção da jurisprudência em matéria de sigilo de dados e concessão de *Habeas Data*. Cf. CUEVA, Ricardo Villas Bôas. A Insuficiente Proteção de Dados Pessoais no Brasil. Revista de Direito Civil Contemporâneo, v. 13, ano 4, out-dez. 2017, p. 66.

Em junho de 2012, o Deputado Milton Monti (PR-São Paulo) apresentou na Câmara dos Deputados o Projeto de Lei nº 4060, como produto das discussões do V Congresso Brasileiro da Indústria da Comunicação. E em 2014, o Senador Vital do Rêgo apresentou o PLS 181/2014.

Em janeiro de 2015, o Governo Federal reiniciou, sob a gestão da Secretaria Nacional do Consumidor do Ministério da Justiça, o debate público para a elaboração de um anteprojeto de lei. As duas consultas públicas somaram 2.500 (duas mil e quinhentas) contribuições nacionais e internacionais, de todos os setores, além de incontáveis eventos presenciais de debate. O texto resultante foi apresentado publicamente em outubro do mesmo ano.

Em maio de 2016, a então presidente Dilma Rousseff encaminhou ao Congresso Nacional, em regime de urgência, o anteprojeto de lei, recebido como Projeto de Lei nº 5276/2016. Em julho de 2016, o presidente interino Michel Temer retirou o regime de urgência e o PL 5276/16 tramitou formalmente na Câmara dos Deputados apensado ao PL nº 4060/12.

Em julho de 2018, o Projeto Lei da Câmara nº 53/2018 foi aprovado no plenário do Senado. A Lei Geral de Proteção de Dados foi sancionada em 14 de agosto de 2018, publicada no Diário Oficial da União em 15 de agosto de 2018, e republicada parcialmente no mesmo dia, em edição extra. O início da vigência seria em 18 meses desde a publicação. O projeto sofreu vetos. Sob a alegação, bastante questionada, de vício de iniciativa, o então Presidente Michel Temer vetou a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão de fiscalização. Em dezembro de 2018, o Presidente Temer editou a Medida Provisória nº 869, de 27 de dezembro de 2018, prevendo a criação da Autoridade Nacional de Proteção de Dados e alterando o início da vigência da lei para agosto de 2020. E, finalmente em 18 de setembro de 2020 entrou em vigor a Lei Geral de Proteção de Dados, com a *vacatio legis* estendida para os dispositivos que tratavam das penalidades e multas.

O Supremo Tribunal Federal, por sua vez, em decisão histórica, embora tardia no cenário mundial, teve a oportunidade de reconhecer a existência no ordenamento brasileiro do direito à autodeterminação informativa. O julgamento se deu em apreciação de medida cautelar no bojo da Ação Direta de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do

Brasil (ADI nº 6387) contra a Medida Provisória nº 954/2020 e sob a relatoria da Ministra Rosa Weber[49].

A Medida Provisória impugnada determinava que as empresas de telecomunicações compartilhassem os dados como nome, telefone e endereço, de todos os seus usuários, cerca de 226 (duzentos e vinte e seis) milhões de consumidores só de telefonia móvel, com a Fundação Instituto Brasileiro de Geografia e Estatística -IBGE -, para fins de pesquisas estatísticas, tendo em vista a situação de emergência de saúde pública decorrente da pandemia do Coronavírus.

A Ordem dos Advogados do Brasil arguiu a inconstitucionalidade da medida, tendo em vista a ausência dos requisitos de relevância e urgência, bem como a violação à dignidade da pessoa humana; à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; ao sigilo dos dados e por ferimento ao princípio da proporcionalidade. Pleiteou, ainda, o reconhecimento da presença no ordenamento constitucional brasileiro do direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante terceiros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil.

Conforme asseverou a Ordem dos Advogados, a aludida Medida Provisória violava o sigilo de dados dos brasileiros e invadia a privacidade e a intimidade de todos, sem a devida proteção quanto à segurança de manuseio, sem justificativa adequada, sem finalidade suficientemente especificada e sem garantir a manutenção do sigilo por uma Autoridade com credibilidade, representatividade e legitimidade, a exemplo daquela prevista pela Lei Geral de Proteção de Dados, Lei Federal 13.709 de 2018, elaborada sob inspiração do Regulamento Europeu.

Além disso, arguiu que a Medida não apresentava, de forma transparente, qual seria a proteção dos cidadãos quanto ao uso adequado dos dados, não garantia a participação do Judiciário, do Ministério Público e da Advocacia, além de entidades

[49] O Supremo Tribunal Federal, por sua vez e em decisão pelo pleno, teve a oportunidade de reconhecer a existência no ordenamento brasileiro do direito à autodeterminação informativa. O julgamento se deu em apreciação de medida cautelar no bojo da Ação Direta de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (ADI nº 6387 – MC/DF, Rel.(a) Min. Rosa Weber) contra a Medida Provisória nº 954/2020. Cf. https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em 30/12/2021. O Partido da Social Democracia (PSDB), o Partido Socialista Brasileiro (PSB), o Partido Socialismo e Liberdade (PSOL) e o Partido Comunista do Brasil (PCB), também, ajuizaram ações no mesmo sentido, para questionar a constitucionalidade da mesma Medida Provisória. (ADI 6388; 6389; 6390; 6393).

da sociedade civil, na fiscalização quanto a tal uso. E que a medida Provisória previa uma forma insegura de repasse de informações, por meio eletrônico e que também pretendia acessar os dados de todos os cidadãos brasileiros, quando a pesquisa por amostra de domicílio seria feita em reduzido número de residências.

Embora o Supremo Tribunal Federal tenha proferido reiteradas decisões em proteção aos direitos de intimidade, privacidade, sigilo das comunicações, dos dados etc., ainda não se havia reconhecido expressamente a tutela constitucional do direito à autodeterminação informativa, a ser extraída diretamente do texto constitucional. Por isso, a relevância da decisão proferida pelo Plenário na ADI 6387, em referendo à decisão monocrática da ministra Rosa Weber, que suspendeu a eficácia da MP 954/2020.

Em sua decisão, a relatora, fazendo menção ao artigo *The Right to Privacy*, escrito por *Samuel D. Warren* e *Louis D. Brandeis* consignou que ali já se reconhecia que as mudanças políticas, sociais e econômicas demandavam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. A Ministra asseverou que decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

Os dados são o ativo e o legado do século XXI, da nova era da informação. Esse novo giro histórico requer do Estado a adequada e efetiva proteção dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais. Novos dados de realidade exigem o reconhecimento de novos direitos e o alargamento das garantias jurídicas com vistas a tutelar, com a máxima efetividade, a autodeterminação das pessoas e, ao fim, o direito à dignidade humana. Inegável que o direito ao sigilo dos dados pessoais e à autodeterminação sobre eles seja constitutivo de um direito mais amplo da dignidade e da personalidade humanas. No centro da ordem constitucional estão o valor e a dignidade da pessoa que age com livre autodeterminação enquanto membro de uma sociedade igualmente livre.

Em resumo, portanto, a evolução da jurisprudência, interpretação e aplicação do direito à proteção de dados pessoais no Brasil, e com fundamento na decisão do Supremo Tribunal Federal, pode-se concluir que: i) que se encontram reconhecidos na ordem jurídica brasileira a proteção à inviolabilidade da vida privada

e da intimidade, o direito à autodeterminação informativa, o direito à privacidade e o direito à proteção de dados pessoais; ii) que se exige na ordem jurídica brasileira a proporcionalidade entre os dados necessários para a pesquisa amostral e a imposição de compartilhamento de dados pessoais de milhões de brasileiros; iii) que se deve respeitar um prazo suficiente para discussão e implementação de medidas que impliquem em compartilhamento de dados pessoais; iv) que deve ser apresentado um relatório de impacto de proteção de dados pessoais cuja elaboração e publicização devem ocorrer antes do compartilhamento e do processamento dos dados pessoais; v) e que deve se evitar o caráter vago e genérico da redação normativa empregada frente aos riscos envolvidos, e assim a normativa deve detalhar a finalidade do tratamento de dados almejados e deve descrever minimamente quais procedimentos de segurança serão adotados.

Importa ainda apontar que o direito fundamental à proteção de dados apresenta uma dupla dimensão: i) subjetiva: que impõe ao legislador o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informativa, uma vez que este direito é a regra e o poder público deve, portanto, justificar a intervenção; e ii) objetiva: que impõe ao legislador um verdadeiro dever de proteção do direito à autodeterminação que deve ser colmatado por meio da previsão de mecanismos institucionais de salvaguarda e proteção refletidos em normas de organização, procedimentos e de governança de proteção de dados pessoais que prevejam medidas positivas de implementação e adequação.

O Estado não pode se omitir quanto a esta implantação organizativa e procedimental e de governança de proteção de dados pessoais. O Estado é obrigado a legislar e atuar, segundo uma concepção de ordem objetiva de valores prevista na Constituição. Desta forma, desde a década de 1970, na Europa, ficou clara a exigência da constituição de uma autoridade de proteção de dados, fundada na ideia de que o direito à proteção de dados não será protegido de forma eficiente se for constituída esta autoridade. A própria Carta dos Direitos Fundamentais da União Europeia prevê no artigo 8º, para além do direito à proteção de dados pessoais, também o acesso a uma autoridade de proteção de dados pessoais, concretizando a dimensão positiva e objetiva da autodeterminação informativa.

Em novembro de 2020, foi instituída no Brasil a ANPD – Autoridade Nacional de proteção de Dados – a exemplo do que já existe em outros países como

Itália - *Garante per la Protezione dei Dati Personali* -, Reino Unido – *ICO*. -, França - *CNIL. Commission Nationale Informatique & Libertés* -, dentre outros.

3.2 A perspectiva de uma governança de proteção de dados pessoais no Poder Judiciário brasileiro

Com fundamento constitucional e com vistas à garantia de direitos e liberdades fundamentais, a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados – LGPD, estabelece no ordenamento jurídico brasileiro o marco regulatório geral da atividade de tratamento de dados pessoais. Os seus parâmetros normativos vinculam agentes públicos e privados, que realizam operações de tratamento de dados pessoais.

O Poder Judiciário enquadra-se no âmbito de aplicação da Lei, assim como os seus inúmeros órgãos, que, no desempenho de suas funções e no seu essencial serviço de acesso à justiça, necessariamente tratam dados dos jurisdicionados, terceiros intervenientes, advogados, magistrados, servidores, auxiliares da justiça, entre outros, enquanto dimensão objetiva do direito fundamental à proteção de dados pessoais e enquanto controlador e responsável pela própria dimensão subjetiva do direito à autodeterminação informativa.

Na execução da função típica do Judiciário, a provocação da jurisdição pela demanda instrumentalizada em peça inicial já implica, por exemplo, tratamento de dados pessoais, visto que requer a identificação das partes (v. g., CPC, art. 319, II). O mesmo ocorre com outros atos processuais praticados no exercício do direito constitucional de ação em procedimentos judiciais ou no uso de competências jurisdicionais. Nesse sentido, a Lei Geral de Proteção de Dados, expressamente, reveste de legitimidade, o tratamento de dado pessoal feito no exercício de situações jurídicas subjetivas em processo judicial (LGPD, arts. 7º, VI, 11, II, “d”), e, de igual maneira, dá fundamento jurídico a todo tratamento de informação efetuado em cumprimento de competência jurisdicional legalmente fixada, conforme os arts. 7º, III, 11, II, “d”, c/c art. 23 da própria lei.

Para além do âmbito da função jurisdicional, o tratamento de dados pessoais pelo Poder Judiciário e seus órgãos é também necessário para a prática dos diversos atos de organização administrativa da justiça. Nesta sede, a Lei Geral de

Proteção de Dados prescreve uma série de obrigações, diretrizes e critérios para tratamento de dados pessoais, especificamente direcionados ao poder público, conforme o Capítulo IV da lei. Impõe-se aos Tribunais brasileiros, e órgãos a eles vinculados, a observância dos parâmetros normativos definidos, ao gerir seus serviços administrativos, com as correspondentes e específicas finalidades públicas, na persecução do interesse público e com o objetivo de executar as competências e atribuições administrativas que lhe foram atribuídas por lei e pela Constituição (LGPD, arts. 7º, III, 11, II, "b", c/c art. 23).

O Conselho Nacional de Justiça atento às obrigações, diretrizes e critérios para tratamento de dados pessoais prescritos pela Lei Geral de Proteção de Dados, e cauteloso com a diversidade de possíveis interpretações que podem ser geradas pelos conceitos nela inseridos, entendeu por bem editar: (i) a Portaria CNJ nº 63/2019, que criou Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais; (ii) a Recomendação CNJ nº 73/2020, sugerindo aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados; e iii) a resolução 363/21 que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos Tribunais.

Ao regular a atividade de tratamento de dados pessoais, a referida lei dispõe sobre o tratamento de dados efetuado por órgãos do poder público no exercício de suas atribuições (LGPD, arts. 23-32), isto é, os tribunais e demais órgãos integrantes do Poder Judiciário estão vinculados ao regime jurídico estabelecido na lei de proteção de dados nas operações de tratamento de dados pessoais que pratiquem, como, por exemplo, no tratamento de dados referentes a servidores públicos, em cursos e escolas da magistratura e em licitações e concursos públicos. Ressalte-se que a discussão sobre as medidas de adequação das normativas e procedimentos observados pelo Judiciário em resposta a imperativos de tutela da privacidade e proteção dos dados pessoais tem sido realizada por diversos países, como Estados Unidos, Canadá, Espanha e França, entre outros.

A Lei Geral de Proteção de Dados inovou no ordenamento jurídico brasileiro ao tecer uma série de conceitos até então desconhecidos, mas também desenvolveu e unificou outros já existentes, com a finalidade de (i) delimitar o objeto sobre o qual recai (dados pessoais), (ii) definir a atividade envolvida (tratamento de

dados pessoais), (iii) os agentes que realizam os atos que consubstanciam tal atividade (agentes de tratamento), e (iv) o novo regime de deveres, que passa a configurar a esfera jurídica desses agentes, e (v) de direitos, titularizados pelos destinatários da proteção outorgada pela lei. Como é típico das leis gerais de proteção de dados, especialmente aquelas inspiradas no modelo europeu, o âmbito material de aplicação da Lei Geral de Proteção de Dados abrange, a princípio, a totalidade das operações sobre dados pessoais. Para tanto, o conceito de dado pessoal, em harmonia com o de informação pessoal, já presente no ordenamento pátrio na Lei de Acesso à Informação (Lei nº. 12.527/2011), é amplo e compreende, sem exceções, qualquer informação que possa ser relacionada a uma pessoa natural, seja esta já identificada ou passível de sê-lo (LGPD, art. 5º, I). A Lei não faz categorizações entre dados pessoais, com a única exceção dos chamados "dados pessoais sensíveis", previstos no art. 5º, II, que são elencados taxativamente e são dados cujo tratamento possui maior potencial discriminatório – v. g., informações sobre origem racial ou étnica, dado referente à saúde ou à vida sexual. Por esse motivo, são submetidos a um regime mais rígido de proteção. Igualmente, o conceito de "tratamento" de dado pessoal é extremamente amplo e, inclusive, mencionado em *numerus apertus*, podendo se aplicar a toda atividade ou operação (v. g., coleta, utilização, acesso, processamento, arquivamento, armazenamento, comunicação, transferência, difusão), passível de ser realizada com dados pessoais, nos termos do art. 5º, X da LGPD. O contexto do Poder Judiciário é repleto de exemplos de operações efetuadas com dados pessoais.

A publicação de decisões judiciais (e outros atos processuais) em Diário de Justiça eletrônico envolve o tratamento de dados que identificam diretamente as partes, respectivos advogados, membros do Ministério Público e magistrados. A realização de atos de caráter executório sobre bens patrimoniais também se dá sobre dados que identificam, direta e/ou indiretamente, pessoas naturais, podendo atingir até mesmo terceiros. Outro exemplo é o caso de processamento de dados de juízes e servidores auxiliares da Justiça referentes a folha de pagamento[50]. Vale ressaltar,

[50] Conferir julgamento do Supremo Tribunal Federal, ocorrido na sessão plenária do dia 23 de abril de 2015, por meio do qual foi apreciado o mérito do Tema 483, em sistemática de Repercussão Geral, que tratava da seguinte questão: "EMENTA: CONSTITUCIONAL. ADMINISTRATIVO. DIVULGAÇÃO, EM SÍTIO ELETRÔNICO OFICIAL, DE INFORMAÇÕES ALUSIVAS A SERVIDORES PÚBLICOS. CONFLITO APARENTE DE NORMAS CONSTITUCIONAIS. DIREITO À INFORMAÇÃO DE ATOS ESTATAIS. PRINCÍPIO DA PUBLICIDADE ADMINISTRATIVA. PRIVACIDADE, INTIMIDADE E SEGURANÇA DE SERVIDORES PÚBLICOS. Possui repercussão geral a questão constitucional

ainda, que é comum o tratamento de dados sensíveis no bojo de processos judiciais cujo objeto versa sobre ou revela aspectos compreendidos na categoria especial de dados – v. g., ação em face de ente federado para fornecimento de medicamentos, ação indenizatória por divulgação não consentida de imagens íntimas, ação penal por crime de racismo ou contra a dignidade sexual. Daí decorre a importância de se dar real efetividade ao segredo de justiça sempre que aplicável.

Os chamados "agentes de tratamento" são as pessoas, naturais ou jurídicas, que de fato realizam as operações de tratamento de dados pessoais. O controlador é o agente principal e que está sempre presente em uma operação de tratamento para determinar a sua respectiva finalidade, eis que praticada no seu interesse e de acordo com suas diretrizes e instruções. Por exemplo, se um Tribunal firma contrato administrativo com provedor de serviço de tecnologia para que esta, com uso de sistemas de inteligência artificial, transcreva de forma automatizada as sessões de julgamento, atuará como controlador, visto que a coleta – gravação de voz e imagem de magistrados e demais presentes – e a transferência de informações configuram tratamento de dados pessoais com propósito estabelecido pelo Tribunal (em conformidade ao sistema processual). Já o operador é agente que pode atuar em nome e segundo instruções do controlador, realizando, assim, operações de tratamento de dados pessoais – documentadas e, idealmente, ajustadas em instrumento negocial. Eventualmente, o próprio controlador poderá realizar com seus próprios recursos o tratamento, caso em que haverá somente o controlador. No exemplo aludido, o provedor de serviço de tecnologia contratado pelo Tribunal figura como operador.

Sob o ponto de vista da aplicação da Lei Geral de Proteção de Dados ao Judiciário, convém confrontar, sob uma perspectiva panorâmica, a atividade de tratamento de dados pessoais das cortes nacionais com os cinco eixos principais da Lei, a saber: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; e v) responsabilização dos agentes.

---

atinente à divulgação, em sítio eletrônico oficial, de informações alusivas a servidores públicos." Por unanimidade e nos termos do voto do ministro relator Teori Zavascki, deu-se provimento ao recurso extraordinário (ARE 652.777 RG/SP) do município de São Paulo, fixando-se a tese de que é legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias.

O primeiro eixo, generalidade e unidade de aplicação da Lei, diz respeito ao âmbito de aplicação material da Lei. A Lei Geral de Proteção de Dados tem por escopo a proteção dos dados da pessoa natural, independentemente do agente a efetivar o tratamento, aplicando-se, assim, tanto aos entes privados do mercado, como aos entes públicos e do terceiro setor, sem distinção da modalidade de tratamento de dados (LGPD, art. 3º). O âmbito de aplicação da nova legislação abrange também o tratamento de dados realizado na Internet, seja por sua concepção de lei geral, seja em decorrência da expressa disposição de seu art. 1º. As poucas hipóteses de delimitação negativa do campo de aplicação da Lei são previstas e justificadas de forma particular, seja pela sua fundamentação em um direito fundamental (liberdade de informação, como no caso da exceção à atividade jornalística) ou interesse público relevante (a exemplo das exceções à segurança pública e defesa nacional), nos termos do art. 4º.

O segundo pilar sobre o qual a Lei está assentada é o da legitimidade do tratamento dos dados de caráter pessoal. São as hipóteses autorizativas para o tratamento de dados. Toda operação de tratamento há de ser calcada em suporte normativo do sistema de proteção de dados que lhe dê amparo. O tratamento de dados pessoais deverá passar por um filtro de análise sobre sua legitimidade, porquanto legítimas, serão consideradas apenas aquelas operações que se amoldem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, que perfazem o total de 11 (onze) hipóteses autorizativas de tratamento. Dentre estas, existem mecanismos como o consentimento informado do próprio titular ou a previsão legal ou regulamentar do tratamento, acrescidos, no entanto, de um conjunto de outras hipóteses que conformam um todo coerente. Para o poder público, logo, o Poder Judiciário, que dele é integrante, o art. 23 da Lei é da maior relevância, pois nele conflui a autorização para o tratamento de informações necessárias ao exercício de competências legais, administrativas ou jurisdicionais, e para a prática de atos no interesse público.

O terceiro eixo, princípios e direitos do titular de sustentação da Lei Geral de Proteção de Dados, é composto pelos princípios e direitos do titular. O estabelecimento de uma série de princípios de proteção de dados e de direitos do titular dos dados pela Lei procura garantir, por um lado, unidade sistêmica à própria disciplina de proteção de dados pessoais e, de outro, um arcabouço de instrumentos que proporcionem ao cidadão meios para o efetivo controle do uso de seus dados por

terceiros. Tais mecanismos, verdadeiras salvaguardas que municiam o titular dos dados, e preceitos normativos se inserem no ordenamento jurídico do Brasil com características próprias, seja em razão das peculiaridades da matéria regulada e complexidade de interesses jurídicos envolvidos, ou então pelo fato de muito herdar de uma tradição já amadurecida em outros países. Da mesma forma que se vê na enorme maioria das legislações de proteção de dados hoje existentes, vários dos princípios consagrados na lei brasileira defluem de um tronco comum, cujas expressões normativas são claramente encontráveis em estatutos e documentos internacionais. Pode-se indicar entre estes princípios, a título exemplificativo, os do livre acesso, segurança, transparência e qualidade. No entanto, haja vista que a nova legislação se pretende um instrumento normativo apto a orientar a solução de questões colocadas à sociedade da informação pela economia digital, aspectos contemporâneos da proteção de dados são abordados e se estabelece princípios que refletem novas demandas. O princípio da não-discriminação pelo tratamento de dados, por exemplo, visa resguardar indivíduos (e grupos) em face do potencial discriminatório de tecnologias baseadas em tratamento automatizado de dados pessoais. O princípio da prevenção, por sua vez, se apresenta vocacionado a ser a base para o desenvolvimento de medidas relacionadas à privacidade na concepção (*Privacy by Design*).

No quarto eixo, obrigações dos agentes do tratamento, a Lei estatui obrigações para os agentes de tratamento, de modo a não apenas definir limites ao tratamento de dados em si, como também prever uma série de procedimentos que procuram proporcionar maior segurança e reforçar as garantias dos titulares dos dados. A natureza de diversas destas obrigações dá conta de que a Lei Geral de Proteção de Dados vai além de proporcionar instrumentos para a defesa e proteção do titular numa perspectiva individualista. A respeito da noção de *privacy by design*, ela se baseia na ideia de que:

> "(...) é preferível instituir medidas que visem garantir a privacidade desde o início, ainda na concepção do produto, do que buscar adaptar o produto ou serviço posteriormente, já em um estado mais avançado. O envolvimento no processo de concepção considera todo o ciclo de vida do dado e o seu uso[51]".

[51] Cf. DANEZIS, George et. al. *Privacy and Data Protection By Design – From Policy to Engineering. ENISA (Euroepan Union Agency for Cybersecurity)*, 2015. p. 11, tradução livre. Disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-bydesign. Acesso em: 20 mai. 2021.

A lei de proteção de dados institui uma série de mecanismos que procuram reforçar a segurança e prevenir problemas e danos no tratamento de dados. Ao mesmo tempo, há a preocupação em estabelecer uma sistemática própria para medidas de natureza reparatória na eventualidade de ocorrência de dano. O capítulo de segurança da informação é um pilar fundamental da Lei e traz pelo menos três inovações importantes para o ordenamento jurídico brasileiro quanto às obrigações dos agentes de tratamento.

Primeiramente, ela exige a adoção por todos que tratam dados de medidas que garantam a integridade, a confidencialidade e disponibilidade dos dados sob tratamento. Em segundo lugar, em caso de incidente de segurança, como o vazamento de dados, emerge o dever para o controlador de comunicar a Autoridade Nacional de Proteção de Dados, que, por seu turno, pode determinar a adoção de medidas para mitigar os efeitos do incidente ou a ampla divulgação para a sociedade, a depender do caso (LGPD, art. 48). Em terceiro lugar, há no referido capítulo uma obrigação que se enquadra no conceito de *privacy by design*, conforme se extrai do art. 46, § 2º: "As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

A documentação criteriosa das operações e medidas adotadas pelos agentes no desempenho da atividade de tratamento de dados pessoais é crucial para a demonstração da observância das normas e parâmetros de proteção de dados pessoais. A bem da verdade, o dever de registrar e documentar atos é já há muito observado pelo Poder Judiciário e seus órgãos, visto que são governados por princípios e regras de direito público, tais como a legalidade, publicidade e motivação/fundamentação das decisões, que efetivamente pressupõem o registro dos atos praticados nos autos, tenha o processo natureza judicial ou administrativa. Contudo, o dever imposto pela Lei Geral de Proteção de Dados ao controlador e ao operador é de mais amplo alcance, especialmente no contexto de implementação do processo judicial eletrônico e de uso de tecnologias digitais para outros fins.

Veja-se, por exemplo, o desenvolvimento do Projeto “Victor” pelo Supremo Tribunal Federal[52]. Todas as operações de tratamento de dados de caráter pessoal, ainda que fora de procedimentos judiciais ou administrativos, devem ser registradas,

[52] Sobre o desenvolvimento do projeto “Victor” no âmbito do Supremo Tribunal Federal, cf. LAGE, Fernanda de Carvalho. Manual de Inteligência Artificial no Direito brasileiro. Salvador: Editora JusPodivm, 2021, p. 177 e seguintes.

como nos casos de tratamento automatizado de dados pessoais por sistemas com algoritmos de aprendizado de máquina para o aperfeiçoamento do próprio *software*, ou de transferência de dados para armazenamento por operador de serviço de computação em nuvem. A observância desse dever converge para o cumprimento do regime jurídico instituído ao poder público no Capítulo IV da Lei, visto que é parte de uma necessária organização que requer, entre outros aspectos: (i) a identificação dos fluxos informacionais que ensejam tratamento de dados pessoais e (ii) os setores que necessitam de uso compartilhado de dados, a fim de se implementar prioritariamente infraestruturas tecnológicas interoperáveis; (iii) a eficiente disponibilização ao acesso público de informações não classificadas, nos termos da Lei de Acesso à Informação; e (iv) a capacidade de demonstrar a adequação e conformidade de sua atividade de tratamento de dados pessoais à Lei Geral de Proteção de Dados.

O quinto eixo, responsabilidade civil e administrativa da Lei, é o da responsabilidade dos agentes na hipótese de violação dos seus preceitos normativos e ocorrência de danos decorrentes do tratamento de dados. A consideração da responsabilidade jurídica dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a Lei Geral de Proteção de Dados procura restringir as hipóteses com fundamento legal (LGPD, art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da necessidade – LGPD, art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (LGPD, art. 6º, II). Nesse contexto, verifica-se o tamanho da complexidade e a necessidade de um grande trabalho de implantação.

Sem dúvida, alguns pontos devem ser observados pelos Tribunais no momento da implantação da nova legislação, pontos esses que a seguir merecem ser destacados:

1) implementação de medidas de transparência do tratamento de dados: a computação em nuvem (*cloud computing*) e os serviços nela baseados envolvem arranjos pelos quais recursos computacionais são fornecidos de modo flexível e independentemente da localização, que permitem uma rápida e ininterrupta alocação de recursos sob demanda[53]. O art. 25 da Lei Geral de Proteção de Dados prescreve que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de

[53] Cf. MILLARD, Christopher (Ed.). Cloud Computing Law. Oxford: Oxford University Press, 2013. E-book.

serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Qualificados como agentes de tratamento de dados pessoais, os tribunais e demais órgãos do Judiciário a eles vinculados devem observar o princípio da transparência (LGPD, art. 6º, VI), que impõe o fornecimento de informações claras, precisas e facilmente acessíveis aos titulares de dados sobre o tratamento de dados pessoais. Esse dever de informar é especialmente reforçado em relação aos entes públicos quando do tratamento de informações pessoais no exercício de suas competências, conforme determina o art. 23, I, da LGPD. O direito de acesso facilitado às informações sobre o tratamento de seus dados concretiza o princípio da transparência e está positivado do art. 9º da Lei Geral de Proteção de Dados. De acordo com esse dispositivo, devem ser disponibilizadas informações aos titulares sobre a finalidade do tratamento, sua forma e duração, identificação do controlador, informações sobre uso compartilhado, direitos do titular e responsabilidades dos agentes que hão de efetuar o tratamento.

Nesse ponto pode-se observar como boas práticas internacionais que serão objeto de maior desenvolvimento na dissertação:

1. *European Court of Justice* (https://curia.europa.eu/jcms/jcms/p1_2699100/en/).

2. *Bundesverfassungsgericht* – Corte Constitucional alemã (https://www.bundesverfassungsgericht.de/EN/Service/Datenschutz/Datenschutz_en _node.htmlvou)

3. *Information Commissioner's Office* - Reino Unido *(https://ico.org.uk/global/privacy-notice/)*

2) Elaboração de um plano de ação para implementação da Lei Geral de Proteção de Dados. No momento que o Poder Judiciário Brasileiro intensifica o uso de tecnologia e a sua governança, buscando uma convergência de soluções, por meio de desenvolvimento comunitário (Resolução CNJ n.º 185/2013, Resolução CNJ n.º 211/2015 e Resolução CNJ 335/2020) é importante adotar ações que possam ser utilizadas por todos os Tribunais e que possam se traduzir em melhores soluções e resultados. A Lei Geral de Proteção de Dados impacta diretamente as bases de dados dos sistemas utilizados por os Tribunais do país.

3) Realização de registro do tratamento de dados. A fim de que toda atividade de tratamento de dados pessoais levada a efeito pelos órgãos do Poder Judiciário seja legítima, cada operação terá como fundamento hipótese legal de tratamento (LGPD, art. 7º), orientada a finalidade(s) prevista(s) legalmente e em conformidade com o regime que determina as respectivas competências e atribuições do serviço público prestado (LGPD, art. 23). Uma importante obrigação dos agentes de tratamento, cujo propósito é permitir a verificação do cumprimento dos parâmetros aplicáveis da Lei Geral de proteção de Dados, é a de manter registros das operações de tratamento (LGPD, art. 37). Esta, por sua vez, somada ao princípio da transparência, torna necessária a divulgação pelos Tribunais de tais registros.

Boas práticas internacionais como referência: Conselho Geral do Poder Judiciário espanhol (http://www.poderjudicial.es/cgpj/es/Temas/Proteccion-de-Datos/Registro-deActividades-de-Tratamiento/)

4) Implementação dos direitos do usuário. Os diversos direitos dos titulares dos dados inscritos no art. 18 da LGPD (direito de acesso, direito de oposição, direito de eliminação, etc.) somente poderão ser exercidos mediante requerimento expresso do titular ou de representante legalmente constituído (LGPD, art. 18, § 3º). Sendo este, portanto, um encargo não oneroso (LGPD, art. 18, § 5º), de que o titular dos dados deve se desincumbir para o exercício de direitos, convém que os tribunais disponibilizem o meio para tanto.

Exemplos de boas práticas: Conselho Geral do Poder Judiciário espanhol (http://www.poderjudicial.es/cgpj/es/Temas/Proteccion-de-Datos/Ejercicio-dederechos--formulario-/)

5) Implementação de medidas de segurança da informação. De acordo com o art. 46 da LGPD, os agentes de tratamento possuem o dever em implementar medidas de segurança, técnicas administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Trata-se de obrigação que deve ser observada de modo a estruturar todo o sistema de tratamento de dados pessoais com a adoção de adequados padrões de segurança da informação (LGPD, art. 49), aptos à preservação da confidencialidade, integridade e disponibilidade das informações tratadas nas bases de dados dos tribunais. A execução e publicação de uma política de segurança da informação adequada são

indispensáveis à realização do direito à proteção dos dados pessoais dos titulares dos dados e à confiança na adequação da atividade dos tribunais.

6) Revisão de contratos, convênios e instrumentos congêneres A organização administrativa dos tribunais e demais órgãos da Justiça brasileira implica, necessariamente, no tratamento de dados de caráter pessoal, atividade, entre outros motivos, concretizada em uma série de atos, contratos e convênios firmados pelos tribunais, inclusive com entes privados. Neste sentido, a LGPD estabelece base legal para essas operações de tratamento de dados, nos termos do art. 23, sendo que a transferência de informações pessoais a entidades privadas, ensejada por contratos, convênios ou instrumentos congêneres (art. 26, § 1º, IV), justifica-se sempre que, instrumentalmente, estiver respaldada no devido atendimento da finalidade pública.

7) Encarregado. Com o propósito de criar na estrutura organizacional dos controladores de dados mecanismos que promovam o efetivo do cumprimento das normas do regime geral de proteção de dados pessoais, a LGPD instituiu a obrigação da indicação do encarregado (art. 41). Esta figura funciona como ponto focal na implementação da lei. Os entes públicos que realizam o tratamento de informações pessoais não se eximem desse dever, haja vista a expressa disposição do art. 23, III, da LGPD.

Boas práticas internacionais que serão objeto de maior desenvolvimento na dissertação:

1. European Court of Justice (https://curia.europa.eu/jcms/jcms/p1_641404/en).

2. Bundesverfassungsgericht – Corte Constitucional alemã https://www.bundesverfassungsgericht.de/EN/Service/Datenschutz/Datenschutz_en_node.htmlvou.

É exatamente com o objetivo de se alinhar às diretrizes impostas pelo Conselho Nacional de Justiça e pela Lei Geral de Proteção de Dados, e em razão da necessidade de constante aprimoramento do atual sistema de acesso aos dados processuais, com vistas a uma melhor organização, que a instituição do Comitê Gestor de Proteção de Dados Pessoais e de um grupo de trabalho de Gestão da Proteção de Dados Pessoais no âmbito dos Tribunais revela-se como medida de

governança quando se trata de positivação das diretrizes de proteção e dados pessoais no âmbito dos Tribunais.

Desta forma, aos Comitês poderão ser atribuídas as seguintes atribuições: i) avaliação dos mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade com as disposições da LGPD; ii) formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação; iii) supervisionar a execução dos planos, dos projetos estratégicos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n.º 13.709, de 14 de agosto de 2018; iv) prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na Lei n.º 13.709, de 14 de agosto de 2018 e nas normas internas; v) promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgão; vi) sugerir medidas de transparência do tratamento de dados; vii) analisar a disponibilização no sítio eletrônico do Tribunal de fácil acesso aos usuários, informações básicas sobre aplicação da LGPD, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores de dados e os direitos dos titulares; viii) analisar o plano de ação para implementação da LGPD; e ix) apresentar proposta de disponibilização pública dos registros de tratamentos de dados pessoais.

O Grupo de Trabalho de Gestão da Proteção de Dados Pessoais será uma equipe técnica responsável pela execução das ações deliberadas pelo Comitê e aprovadas pelo Presidente de cada Tribunal, tendo como atribuições: i) propor e manter processo de atendimento aos pedidos dos titulares dos dados pessoais, dentro dos parâmetros da LGPD; ii) propor formas de capacitação dos servidores nos Tribunais, inclusive nas áreas especificas para recebimento das demandas internas e externas relacionadas à LGPD, propostas pelos titulares de dados; iii) propor soluções para as demandas externas e internas relacionadas à LGPD, inclusive aquelas advindas por ocasião de edição de norma técnica expedida pelo Conselho Nacional de Justiça - CNJ; iv) mapear os processos de trabalho em que há tratamento de dados pessoais no âmbito dos Tribunais; v) executar as políticas internas de privacidade e proteção de dados pessoais; vi) promover as ações necessárias à execução de projetos para a adequação de acórdãos e decisões monocráticas à LGPD; vii) conscientizar e divulgar a LGPD junto aos servidores e magistrados; viii) promover a divulgação da LGPD perante os órgãos educacionais e de imprensa, visando

estimular a mudança de cultura necessária em razão da vigência da norma; e ix) apresentar proposta de um plano de ação para implementação da LGPD.

A economia informacional[54] resultante do incremento da tecnologia e da circulação de dados pessoais e corporativos no ambiente da rede mundial de computadores – internet – acelerou o processo de troca de informações e permitiu que os dados/informações sobre pessoas e organizações passassem a ser um fim em si mesmo, com valor econômico de troca e, portanto, um ativo financeiro[55].

Os avanços tecnológicos aumentaram consideravelmente a capacidade de armazenamento de informações pelos computadores, capazes de organizar e estruturar milhares de dados a custo cada vez mais baixo. E esta realidade, hoje, presente em todos os Tribunais, em razão do processo de informatização ou virtualização dos processos judiciais e administrativos e de todos os processos e rotinas, demanda uma governança destas informações arquivadas e registradas em sua grande maioria em meio digital e eletrônico, em razão da crescente preocupação legislativa de proteção dos dados pessoais, expressão do direito fundamental à autodeterminação informativa[56].

Os direitos dos titulares de dados pessoais, foco de atenção central do arcabouço legislativo de proteção dos dados pessoais visa coibir abusos, o uso indevido e ilícito por parte das organizações, assim como os Tribunais.

A relevância do tema é demonstrada pelo enorme volume de dados pessoais dos usuários do sistema de Justiça, não só advogados, como partes e demais sujeitos dos processos judiciais e/ou administrativos. O Poder Judiciário pode ser visto como um grande coletor e armazenador público de dados pessoais que

---

[54] O termo "economia informacional" é um termo equívoco e empregado em contextos diversos, inclusive na sociologia desde a década de 1970, fundado no contexto de uma economia da informação e no fortalecimento do terceiro setor do Estado. Cf. CASTELLS, Manuel. A Sociedade em Rede. Tradução de Alexandra Lemos e Rita Espanha. Sob a coordenação de José Manuel Paquete de Oliveira e Gustavo Leitão Cardoso. Lisboa: Fundação Calouste Gulbenkian, 2003. (A Era da Informação: economia, sociedade e cultura. V. 1). No sentido de que a expressão "sociedade da informação" "(...) não é um conceito técnico: é um *slogan*. Melhor se falaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar toda a mensagem como informação." Cf. ASCENSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Rio de Janeiro: Forense, 2002, p. 71.

[55] A frase "*data is the new oil*" surgiu em 2006 dita por Clive Humby, matemático inglês, e desde então vem sendo utilizada frequentemente em publicações importantes para se referir à importância do dado e da informação na era do *big data*.

[56] Cf. LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. São Paulo: Almedida, 2020, p. 33 e seguintes.

podem se transformar em dados sensíveis a depender das circunstâncias que são utilizados, como são utilizados e para que são utilizados.

Por isso, torna-se imperiosa a necessidade de se construir um projeto de implantação e conformação de uma governança de dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais em âmbito nacional de forma padronizada em todos os Tribunais, até mesmo como sugestão de meta a ser proposta pelo Conselho Nacional de Justiça em uma perspectiva macro.

Não há dúvida, portanto, acerca da aplicação e da importância da conformação da Lei Geral de Proteção de Dados no âmbito do sistema de Justiça e que merece atenção dos gestores jurisdicionais de forma a buscar maior eficiência e enquadramento técnico quanto ao tratamento de dados pessoais sensíveis.

3.3 A necessária construção da governança de proteção dos dados pessoais no Poder Judiciário brasileiro.

A conformação e aplicação da Lei Geral de Proteção de Dados Pessoais no âmbito do Poder Judiciário são objetos da Recomendação nº 73 de 20/08/2020 e da Resolução nº 363 de 12/01/21, ambas editadas pelo Conselho Nacional de Justiça. Estas normas visam padronizar e auxiliar os procedimentos, políticas e a própria arquitetura de governança de implantação da Lei Geral de Proteção de Dados Pessoais no âmbito dos Tribunais e regulamentam diretrizes básicas necessárias ao processo de adequação/conformação (*compliance*) aos princípios e determinações da novel legislação de proteção de dados pessoais.

As recomendações do Conselho Nacional de Justiça dividiram-se em: (i) implementação de medidas de transparência do tratamento de dados; (ii) realização do registro de tratamento de dados; (iii) implementação dos direitos do usuário; (iv) implementação de medidas de segurança da informação; (v) revisão de contratos, convênios e instrumentos congêneres; e (vi) a definição da pessoa do encarregado.

Cada um dos tópicos foi desdobrado em: (i) justificativa – que permitiu compreender o contexto da recomendação na lei protetiva; (ii) recomendações – com prescrições de ações práticas; (iii) boas práticas - identificando as referências no cenário nacional e internacional de aplicação daquela recomendação; e (iv) modelo – consistente numa representação padronizada do artefato gerado pela implementação da recomendação.

Os dados na atualidade representam ativo importante e hoje são protegidos pela legislação de proteção de dados pessoais, eis que segundo uma análise preditiva e analítica (ciência de dados) é possível alcançar resultados positivos e significativos de gestão nas organizações públicas e privadas, contudo, sem descuidar da proteção necessária aos dados pessoais e sensíveis.

Por isso, a padronização, a definição dos processos e procedimentos, além das medidas, estrutura de dados e definição de pessoas e políticas internas de cada Tribunal, compõem a arquitetura de uma necessária governança de dados que apresenta, como um de seus escopos, a proteção de dados individuais e sensíveis, na forma da legislação de proteção de dados. A governança de dados em sentido amplo descreve os processos utilizados e necessários para planejar, especificar, habilitar, criar, adquirir, manter, usar, arquivar, recuperar, controlar e eliminar dados e que pode atuar na infraestrutura necessária de uma nova visão de proteção dos dados pessoais. A governança de dados pode ajudar aos Tribunais a criar uma missão, alcançar transparência, aumentar a confiança no uso dos dados organizacionais, estabelecer responsabilidades, manter o escopo, o foco e definir metas.

Pretende-se desenvolver cada um destes tópicos acima na dissertação, com destaque sobre a importância da governança de dados e da governança de dados pessoais no âmbito de cada Tribunal.

3.4 A regulação da governança de proteção dos dados pessoais no sistema de Justiça brasileiro.

A implementação de uma governança de proteção de dados pessoais pode provocar mudanças radicais nos paradigmas que interferem em valores e princípios, tais como a autonomia e a independência decisórias do Poder Judiciário quanto à implementação das regras de *compliance* impostas pela própria Lei de Proteção de Dados Pessoais e pelas normativas do Conselho Nacional de Justiça – Recomendação nº 73/2020 e Resolução CNJ nº 363/21. Outras questões podem ser levantadas, como por exemplo: i) a dicotomia entre proteção de dados pessoais e o princípio da publicidade, como regra processual constitucional; ii) a dificuldade de configuração do órgão do encarregado de dados no âmbito dos Tribunais, figura central da legislação de proteção de dados pessoais; iii) e as questões relacionadas

a estruturação do modelo e formato dos comitês gestores de proteção de dados pessoais.

A Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018 - passou a permitir maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito ou norma expressa que legitime a coleta e uso dos dados e obriga às organizações públicas ou privadas a ofertar processos e rotinas aos usuários com vistas a visualizar, corrigir e excluir seus dados pessoais.

A Lei Geral de Proteção de Dados encerra capítulo sobre segurança e boas práticas no tratamento de dados, além de adotar claros princípios de governança nos artigos 46 a 51, em especial o caput do artigo 50:

> "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Verifica-se uma interdisciplinaridade quando se pretende abordar o sentido da expressão governança, como elemento prévio à definição de governança de dados proposta pelo legislador, por envolver um sistema composto de regras de natureza diversas com o objetivo de se chegar às melhores práticas que poderão ser estabelecidas pelos Tribunais, enquanto organizações públicas[57]. Há premissas que devem ser construídas, como forma de garantir uma eficiente governança de dados pessoais, tais como: i) a identificação dos possíveis riscos e incidentes (vazamentos, tratamentos de dados pessoais de forma indevida e ilícita, etc.); ii) definição de procedimentos e processos e do canal de atendimento ao titular de dados para requerimentos (acesso, retificação, alteração do consentimento, etc.); iii) definição do fluxo de tramitação interna destes requerimentos; iv) definição do encarregado e criação de um comitê geral de proteção de dados pessoais que será responsável pela implantação e pela conformidade da legislação; v) capacitação dos servidores e

[57] Cf. FILHO, Adalberto Simão. A Governança Corporativa Aplicada às Boas Práticas e *Compliance* na Segurança dos Dados. In Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, 2018, p. 328.

magistrados com foco na mudança da cultura de dados no âmbito dos Tribunais; e vi) criação de protocolos de gestão de crises e de incidentes de dados[58].

A solução destas questões passa por uma necessária governança de proteção de dados pessoais, voltada aos Tribunais e ao Conselho Nacional de Justiça, com vistas a garantir o suporte necessário aos Tribunais quanto à necessária adequação às regras de *compliance*, rotinas e processos de trabalho de forma a garantir maior eficiência no cumprimento da nova legislação.

Há, ainda, importante barreira a ser transposta, que é a natureza heterogênea dos formatos de dados utilizados por cada Tribunal, bem como a atribuição diferenciadas de classes de processos e movimentos processuais, o que acaba por gerar uma baixa qualidade dos dados e uma dificuldade de estruturação (bases de dados não estruturadas). Trata-se de uma barreira técnica, tanto para os provedores quanto para os consumidores de dados, e impede a sociedade de perceber a transparência, confiabilidade e a eficiência concreta dos dados[59], especialmente os dados pessoais inseridos em cada processo judicial eletrônico.

O desenvolvimento destas questões e a análise dos dispositivos legais pertinentes da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 -, da Recomendação CNJ nº 73/2020 e da Resolução CNJ nº 363/2021, serão objeto deste tópico e serão desenvolvidas na dissertação.

3.5 A importância do marco inicial do processo de implantação da governança de proteção de dados pessoais: os casos do Tribunal de Santa Catarina e do Tribunal de Justiça do Estado de São Paulo.

Neste tópico, pretende-se descrever as ações pioneiras da administração dos Tribunais de Justiça de Santa Catarina e de São Paulo e de que forma estas ações impulsionaram o movimento de regulação normativa pelo Conselho Nacional de Justiça de construção de uma governança de proteção de dados pessoais no âmbito de cada Tribunal.

---

[58] Cf. CRESPO, Marcelo. *Compliance* Digital. In NOHARA, Irene Patrícia. PEREIRA, Flávio de Leão Bastos. (Coord.). Governança, *Compliance* e Cidadania. São Paulo: Revista dos Tribunais, 2018, p. 183-184.

[59] Cf. ATTARD, Judie. ORLANDI, Fabrizio. SCERRI, Simon. AUER, Sörenl. A Systematic Review of Open Government Data Initiatives. In Government Information Quarterly. V. 32. Ed. 4. 2015, p.399 a 418, 2015. Disponível em:https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: 12 de julho de 2021.

Este tópico será objeto de desenvolvimento na dissertação.

4 UMA PROPOSTA DE GOVERNANÇA DE PROTEÇÃO DADOS PESSOAIS: ESTUDO DE CASO DO TRIBUNAL DE JUSTIÇA DE SÃO PAULO

4.1 Fase preparatória: formação e capacitação

A tramitação em duas casas legislativas de projetos de lei tendentes a criar uma Lei Geral de Proteção de Dados foi um fato que chamou a atenção da academia quando começaram a surgir notícias na grande imprensa sobre os impactos mundiais do início da vigência do Regulamento Geral de Proteção de Dados europeu, em 25 de maio de 2018 decorrentes de seus efeitos transnacionais.

Até o advento da Lei Geral de Proteção de Dados, em agosto de 2018, o tratamento do tema proteção de dados era feito pelo nosso ordenamento jurídico de forma difusa, esparsa em diversos diplomas legais que, não raramente, demandavam análise interpretativa do aplicador da lei conforme a matéria de fundo que se estava a julgar. Dessa forma, a prometida inovação legislativa trazida por uma lei geral que serviria de referencial normativo a todos os diplomas setoriais foi um tema que passou a frequentar os encontros do Núcleo de Estudos em Direito Digital da Escola Paulista da Magistratura.

Rapidamente identificou-se que a existência de normas gerais de proteção de dados, aplicáveis tanto ao setor privado quanto ao público, traria modificações sensíveis nas rotinas de trabalho da própria Justiça e que a colocaria numa posição deveras peculiar. Ao passo que, tal como os demais órgãos do setor público, o Poder Judiciário deveria se adequar às prescrições da LGPD assim como já ocorrera à época da promulgação da Lei de Acesso à Informação, tem por competência constitucional e missão institucional julgar conflitos a respeito de proteção de dados num matiz que abarca uma multiplicidade de assuntos que vão da responsabilidade civil a questionamentos regulatórios[60].

Portanto, estar em conformidade com a Lei Geral de Proteção de Dados Pessoais ao tempo de sua entrada em vigor passou a ser um pressuposto de legitimidade para o próprio exercício da jurisdição. Ainda na fase dos debates

[60] Cf. TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. In: Cadernos Jurídicos – Escola Paulista da Magistratura. São Paulo: 2020. Disponível em: https://epm.tjsp.jus.br/Publicacoes/CadernoJuridico/60662?pagina=1. Acesso em 03/11/2021.

preliminares se identificou que mais do que uma imposição de conformidade legal, a assimilação da cultura de proteção de dados pelos integrantes do Tribunal seria uma oportunidade de prover a jurisdição em seu melhor alinhamento ao princípio da eficiência, enunciado no artigo 37 “caput” da Constituição Federal. A prestação jurisdicional que, por sua natureza, lida com uma enorme quantidade de dados pessoais e sensíveis das partes, seus procuradores e demais atores processuais, tem o dever de entregar seu resultado útil isento de danos à personalidade ou aos dados pessoais de seu titular. Nesse sentido, voltar a atenção de cada servidor e magistrado para o valor dos dados pessoais tratados no processo judicial e os potenciais danos decorrentes de eventual tratamento irregular mostra-se a abordagem mais efetiva para mitigar o risco de concretização de danos advindos da comunicação ineficiente e do faltoso controle de conformidade, característicos de órgãos públicos de grande porte.

A criação e fomento da cultura de proteção de dados se deu em diversas frentes. A criação de um Núcleo de Estudos foi a forma encontrada de trazer voluntariamente à escola de magistratura juízes interessados no tema e que se tornariam potenciais replicadores de conteúdo. O amadurecimento dos debates entre os membros desse núcleo de estudo resultou na elaboração da obra coletiva: TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor”, publicada pela Escola Paulista da Magistratura em 2020. Este trabalho acadêmico integrou a lista de artigos da bibliografia Selecionada do Superior Tribunal de Justiça sobre a Lei Geral de Proteção de Dados[61].

Além da produção de conteúdo, a realização pela Escola Paulista da Magistratura de eventos abertos ao público interno e externo propiciou que a temática de proteção de dados alcançasse posição de destaque. O primeiro contato oficial com o tema se deu no evento realizado no âmbito do Núcleo de Estudos em Direito Digital da Escola Paulista da Magistratura intitulado “O Regulamento Geral de Proteção de Dados (GDPR), sua estrutura normativa, impacto nos setores privado e público

[61] Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/28092020-LeiGeral-de-Protecao-de-Dados-Pessoais-e-o-tema-da-nova-edicao-de-Bibliografias-Selecionadas.aspx. Acesso em 03/11/2021.

brasileiro – uma visão sobre sua implementação no TJSP" ocorrido no mês de junho de 2018[62].

Nesses eventos, a presença de autoridades estrangeiras de proteção de dados e palestrantes de renome internacional captou e cativou o interesse de servidores e magistrados, mostrando-se crescente a participação de pessoas de fora da instituição.

Já em tempos de pandemia e seguindo a tendência da realização de eventos com participação totalmente remota de palestrantes e participantes, destacou-se a realização de evento na modalidade de webinar em que se debateu a "Proteção de dados e home office: riscos e desafios"[63]. Voltando sua atenção à capacitação dos servidores integrantes da estrutura administrativa da Presidência e Corregedoria Geral da Justiça, a Escola Paulista da Magistratura buscou junto a outras instituições públicas insumos para prover aos seus integrantes um conteúdo de excelência.

Foi em parceria com o Comitê Gestor da Internet no Brasil – CGI.br que se desenvolveu o Seminário "A conformidade do Poder Judiciário à Lei Geral de Proteção de Dados – desafios técnicos e jurídicos sobre privacidade e proteção de dados" em abril de 2019, ainda sob a vacância da lei. Nesse evento, a participação de representantes do Tribunal de Justiça de Santa Catarina liderados pela Desembargadora Denise de Souza Luiz Francoski selou de modo perene o primeiro alinhamento de dois Tribunais de Justiça em torno do tema.

O Corregedor Geral da Justiça do Tribunal de Justiça de São Paulo à época, Desembargador Geraldo Francisco Pinheiro Franco, entusiasta da tecnologia da informação e ex-integrante da Comissão de Informática do Tribunal, vendo nessa iniciativa de capacitação dos servidores da área administrativa uma oportunidade de continuar o estudo, encomendou à Escola a criação de um grupo de estudos específico para a implementação da LGPD na Corregedoria Geral da Justiça. Os catorze encontros realizados, composto pela Coordenadoria de TI e Direito Digital da Escola Paulista da Magistratura, por magistrados paulistas estudiosos no tema, por Juízes Assessores da Corregedoria Geral da Justiça e pelo Diretores das unidades administrativas desse órgão, contaram com a participação de acadêmicos em

[62] Disponível em: https://epm.tjsp.jus.br/Noticias/Noticia/51598. Acesso em 19/12/2021.
[63] Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=61292. Acesso em 19/12/2021.

proteção de dados pessoais para que compartilhassem suas visões sobre os desafios da implementação da LGPD no TJSP, contribuindo para a estruturação de um plano de trabalho para a implementação e de um modelo de governança para sua manutenção.

O então Corregedor Geral da Justiça ainda participou ativamente de iniciativas junto às serventias extrajudiciais incentivando a Escola a promover, em setembro de 2019, o seminário “A Lei Geral de Proteção de Dados em debate – proteção de dados e os Registros Públicos”, com o apoio do Instituto de Registro Imobiliário do Brasil (IRIB) e da Associação dos Registradores de Pessoas Naturais do Estado de São Paulo (ARPENSP), voltando a discussão pragmática a esse importante ramo da atividade judicial, que consiste no maior e mais fidedigno repositório de dados pessoais de cunho registral.

Ao promover a criação de um grupo de estudos para atender a um órgão de cúpula do Tribunal, a Corte Paulista manifestou o primeiro ato inequívoco de patrocínio das ações de implementação da LGPD.

No ano seguinte, ao assumir a Presidência da Corte, o Desembargador Pinheiro Franco deu continuidade ao projeto determinando ações concretas de adequação de toda a estrutura administrativa da Presidência e da Corregedoria à lei protetiva. Uma visão analítica dessa fase preparatória permite concluir que iniciar o projeto de implementação da Lei Geral de Proteção de Dados Pessoais no Tribunal de Justiça de São Paulo, como em qualquer outro órgão público de pequeno, médio ou grande porte, através da criação da cultura de proteção de dados se mostrou um passo acertado. A promoção do contato do público interno com o tema através de palestras, workshops e webinars, abordando os diversos aspectos que envolvem da atividade jurisdicional (atividade fim), sua a função administrativa (atividade meio) e serviços extrajudiciais, bem assim como a criação de conteúdo acadêmico pelos seus próprios integrantes, resultaram em inquestionável engajamento do corpo funcional e permitiram que a alta administração empenhasse esforços por reconhecer a importância do tema, patrocinando ações concretas de adequação.

4.2 Fase executória: requisitos e modo de implementação

4.2.1 Requisitos

A administração moderna diferencia os níveis de atuação de seus integrantes em três planos: estratégico, tático e operacional.

O gestor público, no âmbito da administração pública, é o ocupante do mais alto cargo de competência executiva e, como tal, tem o poder de decidir “o que” será feito durante seu mandato.

Nos Tribunais, o gestor é seu respectivo Presidente que, baseado no Planejamento Estratégico de sua Corte, define quais metas serão sua prioridade, definindo, portanto, o que será realizado no período de seu mandato. Ao fazê-lo, está patrocinando metas e administrando a Corte no plano estratégico. Para a viabilização das metas patrocinadas, conta com uma equipe de gerentes, normalmente composta por juízes auxiliares, que se dedicarão à análise de identificação da melhor forma de fazê-lo, ou seja, de “como fazer”.

Gerenciar é decidir no plano tático, sobre a melhor forma de planejar e executar as metas estratégicas definidas pelo gestor. Árdua é a tarefa dos servidores que, atuando no plano operacional, efetivamente executarão a tática definida no plano gerencial. Eles são os técnicos nos diversos ramos do conhecimento que proverão o projeto da energia e ações práticas necessárias para sua concretização. A par das aptidões pessoais e qualidades buscadas nestes profissionais, o gerente busca além da capacitação e motivação, incutir em cada um dos integrantes da equipe operacional o engajamento pelo compartilhamento da visão do projeto e propósito visado. Esses três elementos, patrocínio, gerência e engajamento são requisitos estruturantes e de importância fundamental para a compreensão de papéis e responsabilidades num projeto como o de implementação da LGPD.

4.2.2. Engajamento

Na mesma medida em que a preparação do projeto de implementação pela criação de uma cultura de proteção de dados proporciona o conhecimento pela alta administração da importância do projeto a empreender, tem a capacidade de criar

naqueles que o executarão o sentido de propósito, necessidade e utilidade nas atividades desempenhadas.

A internalização desses valores em cada um dos servidores é o que se denomina engajamento (*engagement*). A noção de que ações aparentemente pequenas e isoladas estão atreladas a um propósito maior e direcionado ao bem comum, é o engajamento que se busca de cada um dos integrantes desse grande corpo funcional que serve ao público. Portanto, se o impulsionamento do conteúdo referente à proteção de dados alcançar as mais diminutas e remotas unidades administrativas, bem como se tiver a capacidade de transmitir o propósito, a necessidade e a utilidade daquela pequena, porém importante ação para o atingimento de um bem maior, se estará mitigando, sobremaneira, a ocorrência de grande parte dos problemas decorrentes de uma comunicação ineficiente e de um controle ineficaz na fase pós-implementação, como é característico de implementações em grandes estruturas administrativas.

Envolver todas as camadas da estrutura administrativa no processo de conformidade à LGPD evita a existência de “pontos cegos” que, por vezes ao serem revelados no curso do processo de implementação, resultam em retrabalho e extensão dos prazos de conclusão. Nesse sentido, o incentivo à participação dos servidores em cursos, palestras, webinars, preferencialmente atrelados a retornos positivos em seu histórico funcional do servidor mostra-se uma postura de valor e boa gestão. O que se busca com a criação da cultura de proteção de dados é a genuína mudança de cultura do funcionário no desempenho de suas tarefas diárias. É fácil identificar nas rotinas cartorárias diversas atitudes que são potencialmente danosas aos titulares de dados pessoais, decorrentes de um tratamento irregular. O descarte inadequado de minutas impressas sem trituração, a disponibilização de impressões imperfeitas ao lado da impressora para reutilização como rascunho, o abandono da estação de trabalho desbloqueada durante as pausas, o compartilhamento indevido ou mesmo ignorado de arquivos, e a conversa casual sobre casos concretos sob sua análise revelando detalhes e dados sensíveis são apenas alguns exemplos de vulnerabilidades a serem endereçadas pela sensibilização dos servidores públicos quanto aos danos que pequenas ações podem provocar.

A identificação pelo servidor de que o gestor acredita no projeto e nele vê valor e proveito à atividade desempenhada pelo órgão, enobrecendo-o e qualificando-

o, é um fator chave na obtenção do engajamento, pela potencialização do espírito de corpo, de unidade, de coletividade.

4.2.3 Gerência

No processo de implementação da LGPD em instituições públicas, onde as carreiras de seus servidores são tradicionalmente extensas decorrente da estabilidade ou vitaliciedade, a atribuição da gerência deve considerar a perspectiva da futura participação desse mesmo agente nos órgãos de governança de dados ou de controle da atividade fim, sendo essa uma forma de obter coerência e continuidade no desenvolvimento do programa de governança de dados, uma vez concluído o projeto de implementação.

A importância de uma boa gerência (*management*) reside na criticidade da tomada das primeiras decisões táticas que definirão se o projeto se dará no prazo e na forma desejada pela alta administração. Talvez a primeira e mais importante das decisões nesse plano seja entre terceirizar a implementação, contratar uma consultoria em auxílio ou realizar internamente com pessoal e conhecimento próprios. No caso em estudo, o TJSP contava com boas alternativas em todas as abordagens. A atribuição da missão de implementar a LGPD num Tribunal da dimensão e porte do TJSP, tal como qualquer outro projeto que lida com sua característica mais evidente, o porte e magnitude, é tarefa que inspira cuidado e criteriosa análise no caminho a ser trilhado, pois proporcional ao seu tamanho, são as consequências quantitativa e qualitativamente enormes decorrentes de uma decisão administrativa equivocada, dada a questão de escala, comum a todos os órgãos públicos de grande porte.

A terceirização ou contratação de consultoria foi a alternativa inicialmente considerada, sobretudo em decorrência do fato que além de se tratar de projeto de fôlego, não havia à época literatura específica ou casos de implementação anteriores em órgãos públicos ou no sistema de Justiça que pudessem ser replicados ou aprimorados. Naturalmente, a contratação de profissionais especializados permitiria uma não oneração da estrutura administrativa num ciclo de gestão dos cargos de cúpula que se iniciava, embora onerasse o orçamento já comprometido pela situação econômica do país vivida no ano anterior.

O tempo foi um fator decisivo na tomada de decisão de contratar ou não uma assessoria externa, pois em virtude das normas em vigor, especificamente a Lei

de Licitações – Lei 8.666/93 e a Lei 13.019/2014 -, a contratação de empresa ou o estabelecimento de parceria com organizações da sociedade civil sem fins lucrativos, onerosa ou gratuitamente, deveria observar o procedimento licitatório comum, o chamamento ou credenciamento público.

Nesse contexto, ainda que alguma instituição de ensino ou empresa de consultoria se dispusesse a auxiliar gratuitamente o Tribunal na implementação, ele não estaria dispensado da realização de um certame público que garantisse a igualdade de acesso a essa oportunidade e prestigiasse o preceito constitucional da impessoalidade.

Vislumbrou-se que o detalhamento dos requisitos de qualquer certame levaria tempo e demandaria um aprendizado de modalidade licitatória pouco utilizada, correndo-se ainda o risco de eventuais impugnações que atrasariam o processo de contratação ou estabelecimento de um termo de cooperação técnica. Trabalhava-se com a data de 16 de agosto de 2020 para que o TJSP estivesse em conformidade com as disposições da LGPD, tendo em vista que pela sua natureza de órgão jurisdicional deveria intervir em questões que poderiam orbitar sobre conformidade de outros órgãos não era admissível que ao tempo de sua possível entrada em vigor, caso não convertida em lei a MPV nº 959/2018[64], o Tribunal não estivesse em conformidade.

Portanto, a contratação de assessoria ou a terceirização foi alternativa que a despeito dos ganhos que poderia ter trazido, foi oportunamente descartada. Por outro lado, as contribuições acadêmicas dos profissionais referência reunidas no grupo de estudo criado para implementar a LGPD proporcionaram a identificação de temas centrais que deveriam ser abordados num plano de implantação como ações voltadas à transparência do processo de tratamento de dados, a criação de canal para garantia de direitos, a composição do encarregado de tratamento de dados pessoais num órgão de justiça de grande porte, o mapeamento de atividades que envolviam tratamento de dados pessoais e uma metodologia de análise de lacunas de governança (*gap analysis*).

Providencialmente, o TJSP se viu contemplado com um representante no Grupo de Trabalho instituído pelo Conselho Nacional de Justiça pela Portaria CNJ

[64] A MPV nº 959/2020 previa a entrada em vigor plena da Lei Geral de Proteção de Dados no dia 03 de maio de 2021.

nº63, de 26 de abril de 2019[65] destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais, em especial, quando de sua utilização para fins comerciais. No desenvolvimento dos trabalhos do GT-CNJ-Dados foi identificada a importância da proteção de dados e da necessária aderência do acesso às bases de dados dos Tribunais à MPV nº 959/2020 que previa a entrada plena em vigor da LGPD no dia 03 de maio de 2021. Este grupo de estudo do CNJ resultou na Recomendação CNJ nº 73/2020[66] sugerindo aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD.

A Recomendação baseou-se em Nota Técnica ofertada pelo grupo de estudo do CNJ, e pelos Professores Danilo Doneda e Laura Schertel Mendes, que também o integravam, levando em consideração as referências internacionais a respeito do tema cotejando-as às prescrições da LGPD para fornecer como insumo de elaboração da norma recomendações bem definidas para a aplicação da LGPD no Poder Judiciário. As recomendações dividiram-se em (i) implementação de medidas de transparência do tratamento de dados; (ii) realização do registro de tratamento de dados; (iii) implementação dos direitos do usuário; (iv) implementação de medidas de segurança da informação; (v) revisão de contratos, convênios e instrumentos congêneres; e (vi) encarregado.

Cada um dos tópicos foi desdobrado em (i) justificativa – que permitiu compreender o contexto da recomendação na lei protetiva; (ii) recomendações – com prescrições de ações práticas; (iii) boas práticas - identificando as referências no cenário nacional e internacional de aplicação daquela recomendação; e (iv) modelo – consistente numa representação do artefato gerado pela implementação da recomendação.

Dessa forma, a primeira decisão gerencial na implementação da LGPD no TJSP foi a de conduzir o processo com pessoal e meios próprios, utilizando-se dos insumos acadêmicos aqui mencionados. A referência mais próxima de um projeto dessa envergadura foi a implementação da Lei de Acesso à Informação no ano de 2012, cujas lições aprendidas e plano de projeto ainda permaneciam no repositório do setor de planejamento do Tribunal. O desafio a partir da tomada de decisão foi

[65] Disponível em https://atos.cnj.jus.br/atos/detalhar/2890. Acesso em 19/12/2021.
[66] Disponível em https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em 19/12/2021.

transformar as recomendações da nota técnica em um plano de trabalho e formar o comitê gestor de proteção de dados para executá-lo.

4.3 Etapas de implementação

4.3.1 O Comitê Gestor de Proteção de Dados Pessoais

O sucesso do projeto numa instituição de grande porte como o Tribunal de Justiça de São Paulo tinha por pressuposto o atendimento dos requisitos de patrocínio, gerência e engajamento e, por esse motivo, as pessoas que colocariam o projeto em prática deveriam representar os três planos administrativos correlatos: estratégico, tático e operacional.

Nessa linha, sua composição replicou essa estrutura piramidal tendo em seu ápice o Presidente do Tribunal, que designou juiz assessor de seu gabinete, mesclando assim os planos estratégico e tático para exercer a coordenação do Comitê Gestor de Proteção de Dados, instituído pela Portaria 9.912/2020 da Presidência do Tribunal[67].

O plano operacional foi exercido por dois segmentos. O primeiro deles, Comitê Gestor de Proteção de Dados, foi integrado por funcionários do primeiro escalão administrativo de cada uma das áreas administrativas do Tribunal, a saber, orçamento e finanças, planejamento, recursos humanos, administração e abastecimento, tecnologia da informação, controle interno, comunicação social, gestão processual de primeiro e segundo graus de jurisdição, escolas de magistratura e servidores, Ouvidoria e a Corregedoria Geral da Justiça.

A coordenação setorial foi atribuída a um juiz assessor da Presidência ou da Corregedoria Geral da Justiça sendo eles os pontos focais para a interação com o coordenador. Para garantir a capilaridade e participação de todas as mais diminutas unidades administrativas, o segundo segmento do plano operacional foi instituído como sendo um Grupo de Trabalho que tinha a função de prover o Comitê Gestor de dados e executar as tarefas com a granularidade necessária para uma participação ampla e engajamento pleno.

---

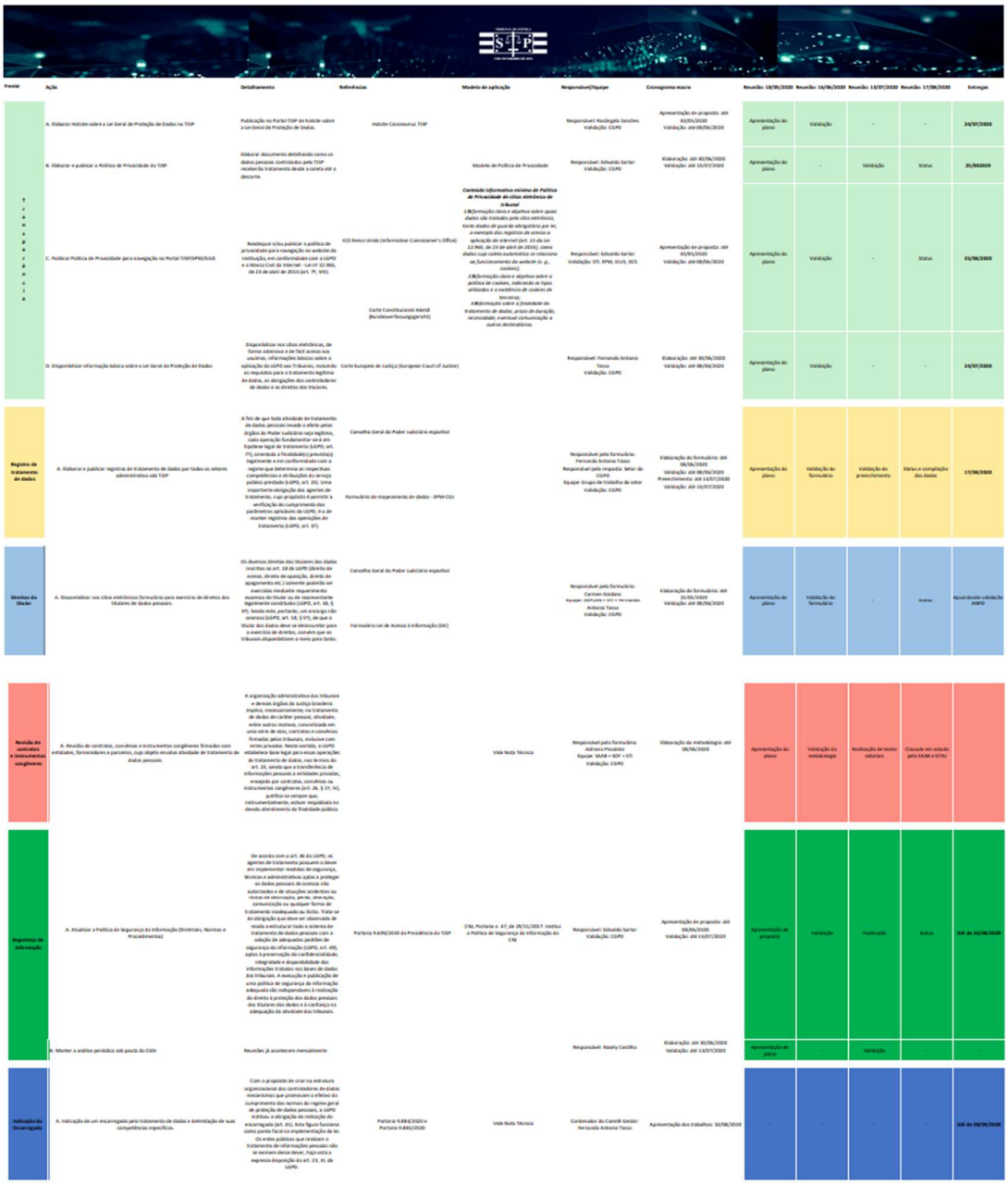
[67] Disponível em https://www.tjsp.jus.br/Download/Portal/LGPD/Portaria_9912_20.pdf?637755309896044180. Acesso em 19/12/2021.

4.3.2 Plano de trabalho

A criação do plano de trabalho consistiu na transposição das recomendações contidas na nota técnica ofertada ao Grupo de Trabalho do Conselho Nacional de Justiça para um formato que permitisse a visualização de cada uma das recomendações como frentes de trabalho, desdobradas em ações, consistentes nas realizações almejadas que, no léxico da gestão de projetos se denominam entregas ou entregáveis.

A utilização do formato de tabela mostrou ter a simplicidade buscada e contemplou nas colunas os campos de detalhamento da ação, referências, modelo de aplicação, identificação do responsável e sua equipe e cronograma.

Além da praticidade de controle, permanecia acessível a todos os participantes do projeto de implementação, de modo que se pudesse acompanhar o andamento de cada uma das ações em suas respectivas frentes. Ainda que se estivesse tratando de um Tribunal de grande porte, esse modelo não ficou aquém da necessidade da instituição, gerando, por via diversa uma demonstração aos participantes que o valor do projeto não estava na sofisticação da ferramenta ou da metodologia empregadas, mas no fácil acesso de seus participantes ao progresso das ações e no crescimento de um salutar espírito colaborativo das diversas áreas envolvidas. A simplicidade gerou engajamento e o alcance de todas as metas ao seu devido tempo.



Frente	Ação	Detalhamento	Referências	Modelo de aplicação	Responsável/Equipe	Cronograma-macro	Reunião: 10/09/2020	Reunião: 16/06/2020	Reunião: 13/07/2020	Reunião: 17/08/2020	Entregas
Transparência	A. Elaborar Hotsite sobre a Lei Geral de Proteção de Dados no TJSP	Publicação no Portal TJSP do hotsite sobre a Lei Geral de Proteção de Dados.	Hotsite Coronavírus TJSP		Responsável: Rodrigeta Sanches Validação: CGPD	Apresentação de proposta: até 31/01/2020 Validação: até 08/04/2020	Apresentação do plano	Validação	-	-	24/07/2020
	B. Elaborar e publicar a Política de Privacidade do TJSP	Elaborar documento detalhando como os dados pessoais controlados pelo TJSP recebem tratamento desde a coleta até a descarte.		Modelo de Política de Privacidade	Responsável: Edvaldo Sartor Validação: CGPD	Elaboração: até 30/06/2020 Validação: até 16/07/2020	Apresentação do plano	-	Validação	Status	31/08/2020
	C. Publicar Política de Privacidade para navegação no Portal TJSP/EPM/EJUS	Readequar e/ou publicar a política de privacidade para a navegação no website da instituição, em conformidade com a LGPD e o Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014 (art. 7º, VIII).	ICO Reino Unido (Information Commissioner's Office) Corte Constitucional Alemã (Bundesverfassungsgericht)	**Conteúdo informativo mínimo de Política de Privacidade de sítio eletrônico de tribunal** **1.A)**Informação clara e objetiva sobre quais dados são tratados pelo sítio eletrônico, tanto dados de guarda obrigatória por lei, a exemplo dos registros de acesso a aplicação de internet (art. 15 da Lei 12.965, de 23 de abril de 2014), como dados cuja coleta automática se relaciona ao funcionamento de website (v. g., cookies); **1.B)**Informação clara e objetiva sobre a política de cookies, indicando os tipos utilizados e a existência de cookies de terceiros; **1.C)**Informação sobre a finalidade do tratamento de dados, prazo de duração, necessidade, eventual comunicação a outros destinatários.	Responsável: Edvaldo Sartor Validação: STI, EPM, EJUS, DCS	Apresentação de proposta: até 31/01/2020 Validação: até 08/04/2020	Apresentação do plano	Validação	-	Status	31/08/2020
	D. Disponibilizar informação básica sobre a Lei Geral de Proteção de Dados	Disponibilizar nos sítios eletrônicos, de forma extensiva e de fácil acesso aos usuários, informações básicas sobre a aplicação da LGPD aos Tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores de dados e as diretrizes dos titulares.	Corte Europeia de Justiça (European Court of Justice)		Responsável: Fernando Antonio Tasso Validação: CGPD	Elaboração: até 30/06/2020 Validação: até 08/09/2020	Apresentação do plano	Validação	-	-	24/07/2020
Registro de tratamento de dados	A. Elaborar e publicar registros de tratamento de dados por todos os setores administrativos são TJSP	A fim de que toda atividade de tratamento de dados pessoais levada a efeito pelos órgãos do Poder Judiciário seja legítima, cada operação fundamental vai ao encontro legal de tratamento (LGPD, art. 7º), orientado a finalidade(s) previstas) legalmente e em conformidade com a regime que determina as respectivas competências e atribuições do serviço público prestado (LGPD, art. 23). Uma importante obrigação dos agentes de tratamento, cujo propósito é permitir a verificação do cumprimento dos parâmetros aplicáveis da LGPD, é a de manter registros das operações de tratamento (LGPD, art. 37).	Conselho Geral do Poder Judiciário espanhol Formulário de mapeamento de dados - EPM-CGJ		Responsável pelo formulário: Fernanda Antonia Tasso Responsável pela resposta: Setor de CGPD Equipe: Grupo de trabalho do setor Validação: CGPD	Elaboração do formulário: até 08/06/2020 Validação: até 08/06/2020 Preenchimento: até 13/07/2020 Validação: até 10/07/2020	Apresentação do plano	Validação do formulário	Validação do preenchimento	Status e compilação dos dados	17/08/2020
Direitos do titular	A. Disponibilizar nos sítios eletrônicos formulário para exercício de direitos dos titulares de dados pessoais.	Os diversos direitos dos titulares dos dados inscritos no art. 18 da LGPD (direito de acesso, direito de oposição, direito de apagamento etc.) somente poderão ser exercidos mediante requerimento expresso do titular ou de representante legalmente constituído (LGPD, art. 18, § 3º). Sendo este, portanto, um encargo não oneroso (LGPD, art. 18, § 5º), de que o titular dos dados deve se desincumbir para o exercício de direitos, cumprindo que os tribunais disponibilizem o meio para tanto.	Conselho Geral do Poder Judiciário espanhol Formulário Lei de Acesso à Informação (SIC)		Responsável pelo formulário: Carmen Giodano Equipe: DMTI/ATA + STI + Fernando Antonio Tasso Validação: CGPD	Elaboração do formulário: até 31/05/2020 Validação: até 08/06/2020	Apresentação do plano	Validação do formulário	-	Status	Aguardando validação ANPD
Revisão de contratos e instrumentos congêneres	A. Revisão de contratos, convênios e instrumentos congêneres firmados com entidades, fornecedores e parceiros, cujo objeto envolva atividade de tratamento de dados pessoais.	A organização administrativa dos tribunais e demais órgãos da justiça brasileira implica, necessariamente, no tratamento de dados de caráter pessoal, dividade, entre outros motivos, concretizada em uma série de atos, contratos e convênios firmados pelos tribunais, inclusive com entes privados. Neste sentido, a LGPD estabelece base legal para essas operações de tratamento de dados, nos termos do art. 23, sendo que a transferência de informações pessoais a entidades privadas, exigida por contratos, convênios ou instrumentos congêneres (art. 26, § 1º, IV), justifica-se sempre que, instrumentalmente, estiver respaldada no devido atendimento da finalidade pública.		Vide Nota Técnica	Responsável pela formulário: Adriano Pissolato Equipe: SAAB + SOF + STI Validação: CGPD	Elaboração da metodologia: até 08/06/2020	Apresentação do plano	Validação da metodologia	Realização de testes setoriais	Cláusula em estudo pela SAAB e STAJ	
Segurança da informação	A. Atualizar a Política de Segurança da Informação (Diretrizes, Normas e Procedimentos)	De acordo com o art. 46 da LGPD, os agentes de tratamento possuem o dever em implementar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. Trata-se de obrigação que deve ser observada de modo a estruturar todo o sistema de tratamento de dados pessoais com a adoção de adequados padrões de segurança da informação (LGPD, art. 49), aptos à preservação da confidencialidade, integridade e disponibilidade das informações tratadas nos bancos de dados dos tribunais. A execução e publicação de uma política de segurança da informação adequada são independentes à realização do direito à proteção dos dados pessoais dos titulares dos dados e à confiança na adequação da atividade dos tribunais.	Portaria 9.699/2020 da Presidência do TJSP	CNJ, Portaria n. 47, de 29/11/2017. Institui a Política de Segurança da Informação do CNJ	Responsável: Edvaldo Sartor Validação: CGPD	Apresentação de proposta: até 06/06/2020 Validação: até 13/07/2020	Apresentação de proposta	Validação	Publicação	Status	Até 31/08/2020
	B. Manter a análise periódica sob pauta do CGSI	Reuniões já acontecem mensalmente			Responsável: Rooty Castilho	Elaboração: até 30/06/2020 Validação: até 14/07/2020	Apresentação do plano			Validação	
Indicação do Encarregado	A. Indicação de um encarregado pelo tratamento de dados e delimitação de suas competências específicas.	Com o propósito de criar na estrutura organizacional dos controladores de dados mecanismos que promovam o efetivo do cumprimento das normas do regime geral de proteção de dados pessoais, a LGPD institui a obrigação da indicação do encarregado (art. 41). Esta figura funciona como ponto focal na implementação de tal. Os entes públicos que realizam o tratamento de informações pessoais não se eximem desse dever, haja vista a expressa disposição do art. 23, III, da LGPD.	Portaria 9.886/2020 e Portaria 9.895/2020	Vide Nota Técnica	Coordenador do Comitê Gestor: Fernanda Antonia Tasso	Apresentação dos trabalhos: 31/08/2020	-	-	-	-	Até 30/09/2020

*Plano de Trabalho, disponível em https://www.tjsp.jus.br/Download/Portal/LGPD/PlanoTrabalho.pdf?637755312636866304. Acesso em 19/12/2021.

4.3.3. Ações de transparência

A implementação de medidas de transparência no tratamento de dados decorre da necessária observância aos princípios da transparência e do livre acesso, concretizados na regra do artigo 9º da LGPD que dispõe:

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e

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

As referências adotadas vieram da Corte Europeia de Justiça[68], da Corte Constitucional Alemã[69] e da autoridade de proteção de dados do Reino Unido[70]. O desdobramento dessa frente se deu em quatro ações distintas. A criação de um hotsite ao invés de uma página no portal eletrônico foi a escolha direcionada para dar especial visibilidade ao tema de proteção de dados, desde o seu lançamento até a conclusão dos trabalhos.

Aproveitou-se o virtuoso resultado dessa mesma modalidade de divulgação e impulsionamento de conteúdo adotada pelo próprio TJSP para a divulgação das informações sobre a pandemia da COVID-19, por ocasião em que toda uma nova modalidade de trabalho remoto foi sendo desenhada na medida em que lições eram aprendidas com o processo de migração. Por meio dessa modalidade de canal foram publicadas informações úteis aos usuários do sistema de justiça sobre as mudanças que a LGPD traria na prestação jurisdicional, quem eram os agentes de tratamento, os conceitos elementares de operação de tratamento de dados pessoais e uma contextualização do papel da Autoridade Nacional de Proteção de Dados.

O envolvimento da Diretoria de Comunicação Social no projeto de implantação da LGPD foi decisivo para que a linguagem empregada promovesse uma fácil compreensão do conteúdo pelo principal destinatário de todo o projeto, o jurisdicionado. A elaboração de uma política de privacidade tinha a finalidade de oficializar e detalhar o compromisso do Tribunal em proceder ao tratamento de dados

---

[68] *European Court of Justice* – Disponível em: https://curia.europa.eu/jcms/jcms/p1_2699100/en/. Acesso em 01/12/2021.
[69] *Bundesverfassungsgericht* – Disponível em: https://www.bundesverfassungsgericht.de/EN/Service/Datenschutz/Datenschutz_en_node.htmlvou. Acesso em 01/12/2021.
[70] *Information Commissioner's Office* – Disponível em: https://ico.org.uk/global/privacy-notice/. Acesso em 01/12/2021.

pessoais que lhe fossem confiados de acordo com as diretrizes de segurança e transparência, levando em conta as disposições da LGPD, da Lei de Acesso à Informação – Lei 12.527/11 - e do Marco Civil da Internet – Lei 12.685/14.

Foi observado o conteúdo da Recomendação CNJ nº 73/2020 que tinha por desiderato fornecer informações claras e objetivas sobre a finalidade do tratamento de dados, seu prazo de duração, necessidade e eventual comunicação a outros destinatários. O último desdobramento das ações de transparência foi a publicação da política de cookies, com o relacionamento entre os utilizados e sua finalidade, bem como a declaração de utilização de cookies de terceiros.

Diante do tratamento não específico constante do Marco Civil da Internet sobre a guarda de registros a provedores de aplicações pertencentes ao setor público, optou-se por adotar paralelismo às aplicações privadas, prevendo a guarda de logs pelo prazo de 06 meses, conforme dispõe o artigo 15 da Lei 12.965/14.

Frente	Ação	Detalhamento	Referências	Modelo de aplicação	Responsável/Equipe	Cronograma	Reunião 1: data	Reunião 2: data	Reunião 3: data	Reunião 4: data	Entregas
Transparência	A. Elaborar Hotsite sobre a Lei Geral de Proteção de Dados no TJSP	Publicação no Portal TJSP de hotsite sobre a Lei Geral de Proteção de Dados.	Hotsite Coronavírus TJSP		Responsável: nome Validação: CGPD	Apresentação de proposta: até data Validação: até data Publicação: até data	Apresentação do plano	Validação	-	-	data
	B. Elaborar e publicar a Política de Privacidade do TJSP	Elaborar documento detalhando como os dados pessoais controlados pelo TJSP receberão tratamento desde a coleta até o descarte.		Modelo de Política de Privacidade	Responsável: nome Validação: CGPD	Elaboração: até data Validação: até data Publicação: até data	Apresentação do plano	-	Validação	Status	data
	C. Publicar Política de Privacidade para navegação no Portal TJSP/EPM/EJUS	Readequar e/ou publicar a política de privacidade para navegação no website da instituição, em conformidade com a LGPD e o Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014 (art. 7º, VIII).	ICO Reino Unido (Information Comissioner's Office) Corte Constitucional Alemã (Bundesverfassungsgericht)	**Conteúdo informativo mínimo de Política de Privacidade de sítios eletrônico de tribunal** *1.Informação clara e objetiva sobre quais dados são tratados pelo sítio eletrônico, tanto dados de guarda obrigatória por lei, a exemplo dos registros de acesso a aplicação de Internet (art. 15 da Lei 12.965, de 23 de abril de 2014), como dados cuja coleta automática se relaciona ao funcionamento do website (v. g., cookies);* *2.Informação clara e objetiva sobre a política de cookies, indicando os tipos utilizados e a existência de cookies de terceiros;* *3.Informação sobre a finalidade do tratamento de dados, prazo de duração,*	Responsável: nome Validação: STI, EPM, EJUS, DCS	Apresentação de proposta: até data Validação: até data Publicação: ate data	Apresentação do plano	Validação	-	Status	data
	D. Disponibilizar informação básica sobre a Lei Geral de Proteção de Dados	Disponibilizar nos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários, informações básicas sobre a aplicação da LGPD aos Tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores de dados e os direitos dos titulares.	Corte Europeia de Justiça (European Court of Justice)		Responsável: nome Validação: CGPD	Elaboração: até data Validação: até data Publicação: até data	Apresentação do plano	Validação	-	-	data

*Plano de Trabalho – frente I – Ações de Transparência[71].

4.3.4 Registro e mapeamento das atividades de tratamento

Certamente a mais desafiadora das frentes de trabalho, o mapeamento de dados, como ficou popularmente conhecida a atividade mais bem designada como sendo registro de tratamento de dados pessoais, foi objeto de extensa reflexão quanto ao modelo a ser adotado. Tinha-se em mente que a mobilização de todos os setores

[71] Disponível em https://nam10.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.fiscosoft.inf.br%2Flivros%2F10326_LGPD_Cap_3_FIGURA_1.jpg&data=04%7C01%7C%7Cce946134400f4969dede08d9c32f271e%7Cce4e1164986f413285d11e3c17cf7d6e%7C0%7C0%7C637755429547160150%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=tpDkX20BL7UAWrL9C31xkqVQfM2g%2FBioxRsBRwsiV2g%3D&reserved=0. Acesso em 19/12/2021.

administrativos de um tribunal deve ter como resultado final um produto útil, que seria revertido em benefício da atividade fim, a jurisdição.

Diversos modelos trazidos da iniciativa privada não abordavam particularidades de uma grande estrutura de órgão judiciário, revelada pela alta granularidade de atribuições administrativas em diversas unidades especializadas em determinada matéria e, por outro lado, pela constatação de que uma mesma unidade administrativa praticava atividades que tratavam dados pessoais e outras que não. Identificou-se como sendo necessária a adoção de um modelo de mapeamento que observasse o vetor da simplicidade, de modo a permitir que diminutos setores administrativos fossem atingidos pela atividade de mapeamento e, ainda mais importante, que tivessem por metodologia o mapeamento de cada uma das atividades que envolvessem o tratamento de dados pessoais naquele setor, e não unicamente o mapeamento da atividade genérica consistente em sua atribuição administrativa.

Esse último fator foi decisivo para a utilização do modelo de referência do Conselho Geral do Poder Judiciário Espanhol que, além de simples por ser fruto do refinamento do tema num país com tradição em proteção de dados, trabalha com cada uma das atividades específicas do setor mapeado como fator preponderante. Com isso, ao passo que se evitou a coleta de respostas binárias e inservíveis para a finalidade visada, ou seja, se determinada unidade administrativa trata ou não dados pessoais, a metodologia permitiu a rastreabilidade de todo o ciclo de vida do dado pessoal apenas nas atividades que procedem ao tratamento de dados pessoais naquela unidade administrativa evitando a dissipação de esforços no mapeamento de outras atividades.

Portanto, em caso de tratamento irregular de dados, compartilhamento indevido, vazamento ou acesso não autorizado, a rastreabilidade da causa raiz é enormemente facilitada, pois se elimina, de partida, atividades que não envolvem tratamento de dados pessoais ou até mesmo setores que não praticam aquela espécie de atividade. Por outro lado, referida metodologia elimina uma dúvida recorrente em órgãos que possuem bases de dados híbrida - em meio físico (papel) e em meio digital (em estrutura própria ou em nuvem) – a respeito de qual a melhor abordagem para mapear os dados em cada meio.

A metodologia de mapeamento pelo registro de cada uma das atividades de tratamento de dados pessoais tem como item de registro o meio em que determinada atividade se desenvolve, físico ou digital. Dessa forma, a questão do

meio passa a ser uma informação importante do mapeamento e não seu principal vetor. Evita-se a dissipação de esforços na varredura de infindáveis registros eletrônicos ou físicos para se identificar a atividade, que, eventualmente, por não tratarem dados pessoais, implicam em descarte do esforço. A proposta espanhola faz exatamente o contrário. O registro de atividades de tratamento de dados pessoais foi a tarefa que demandou o maior esforço do Comitê Gestor de Proteção de Dados e de seu Grupo de Trabalho. Competiu aos pontos focais de cada disciplina administrativa identificar na estrutura abaixo do primeiro escalão todas as unidades a serem consultadas e mapeadas, de modo a promover engajamento e capilaridade, evitando a existência de "pontos cegos".

A coleta por formulário eletrônico[72] é medida de eficiência em órgãos públicos de grande porte, bem assim como a consolidação desses registros em ferramenta específica. Naturalmente, maior será a qualidade das respostas ao formulário quanto tiver sido o investimento na prévia capacitação dos servidores ao seu preenchimento. Inconsistências como a utilização de termos sinônimos, imprecisos, incorreto atrelamento de base legal a determinada atividade, são apenas alguns exemplos das dos pontos de atenção nas tarefas subsequentes à coleta dos registros de atividade para a completa conformidade. Enquanto a maioria dos órgãos públicos compilou os dados de registros de atividades em ferramenta de planilha eletrônica, o TJSP, objeto do estudo, utilizou a ferramenta de gestão de risco (*risk management*) que compilou os dados e forneceu um painel gráfico (*dashboard*) que permite a análise direcionada ao risco, priorizando as atividades que tratam dados pessoais sensíveis, dados de crianças e adolescentes, dados compartilhados com instituições públicas ou privadas e transferências internacionais de dados pessoais.

A adequação das atividades de tratamento às disposições da LGPD que se inicia com o registro das atividades, tem como fases subsequentes a normalização dos registros, para o tabelamento de situações idênticas, unificação da linguagem e padronização das respostas. Superadas essas etapas, será possível adequar as atividades de tratamento, fazendo o correto atrelamento à base legal e observando os princípios de tratamento.

Embora o mapeamento deva ser revisto periodicamente, a primeira fase de conformidade termina com a comunicação dos achados às unidades envolvidas,

[72] A matriz de elaboração do formulário eletrônico utilizado no TJSP encontra-se disponível em: https://www.tjsp.jus.br/Download/Portal/LGPD/Anamnese.pdf. Acesso em 01/12/2021.

fechando o ciclo de retroalimentação do fluxo informacional interno. A evolução da atividade de mapeamento contempla ainda a atividade de realizar igual mapeamento nas partes relacionadas com o órgão público, sendo estas as que mantêm com o ente público relação negocial por contrato, convênio ou instrumento congênere. Sua finalidade consiste em identificar a exigir do parceiro externo a observância de igual nível de maturidade e conformidade legal ao tratamento de dados pessoais.

A fase primeira de registro e mapeamento de dados incluiu no formulário eletrônico as seguintes perguntas às unidades administrativas[73]:

> "Registro de Tratamento de Dados – Fase 1 –
> Anamnese organizacional e Registro de atividades de tratamento
>
> 1. Nome da Secretaria/Diretoria.
> 2. Vinculada a qual órgão de cúpula? Presidência / Corregedoria
> 3. Missão (qual é a função da Secretaria/Diretoria)
> 4. Elenque 5 ou mais atividades primárias da Secretaria/Diretoria e descreva cada uma.
> 5. Qual(is) a(s) finalidade(s) do tratamento. (Descrição do propósito específico a motivar a operação de tratamento de dado pessoal em questão)
> 6. Qual a base legal para tratamento? (escolha uma) (Fundamento legal da LGPD que legitima o tratamento de dado pessoal) I - mediante o fornecimento de consentimento pelo titular II - para o cumprimento de obrigação legal ou regulatória pelo controlado 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 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 X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente).

[73] Disponível em https://www.tjsp.jus.br/Download/Portal/LGPD/Anamnese.pdf. Acesso em 01/12/2021.

> 7. Quem são os titulares dos dados? (Classes de pessoas naturais identificadas ou identificáveis sobre quem as informações objeto de tratamento dizem respeito)
> 8. Qual a categorias de dados? (Tipos de dados pessoais objeto da operação de tratamento)
> 9. Qual a categorias de destinatários? (Caso haja previsão da comunicação de dados pessoais, a qual(is) sujeito(s) as informações são destinadas)
> 10. Existe possibilidade de transferência internacional? (Caso haja previsão de transferência internacional, qual país estrangeiro ou organismo internacional será o receptor dos dados)
> 11. Qual o prazo de conservação dos dados? (Período razoavelmente estimado para a conservação dos dados, considerando o cumprimento da(s) finalidade(s) estipulada(s)) 12. Quais medidas de segurança foram adotadas? (Medidas de segurança, técnicas e administrativas a serem implementadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito).”

4.3.5 Garantias institucionais dos direitos dos titulares de dados pessoais

A implementação dos direitos do titular é indiscutivelmente a mais nobre e valorosa realização em um projeto de implementação da LGPD, uma vez que pela efetiva salvaguarda dos direitos fundamentais do jurisdicionado e de seus integrantes, o órgão público qualifica o serviço público prestado.

A eficiência é princípio constitucional aplicável a todo o poder público e tem como aspecto importante a prestação do serviço sem a geração de danos ao usuário do serviço público. Significa dizer que mais qualificada será a prestação jurisdicional se tanto o trâmite processual como o tratamento dos registros funcionais de seus integrantes forem tratados com especial observância à importância de questões como o segredo de justiça, o sigilo legal de um documento e o controle de acesso a determinada informação sensível.

Ocorre que seja pelo investimento insuficiente na criação de uma cultura organizacional de proteção de dados, ou pela comunicação ineficaz ou controle tardio, eventual dano decorrente da malversação dos dados pessoais controlados pelo ente público somente será identificado uma vez concretizado. A criação de um canal para que o titular dos dados pessoais exerça diretamente seus direitos consignados em toda a LGPD, em especial nos artigos 18 e 19, consiste na aplicação concreta do

princípio constitucional da eficiência, permitindo que antes mesmo de eventual fato danoso, o ente público tome ciência e corrija procedimentos viciosos debelando tratamento irregular de dados pessoais.

A disponibilização de formulário para exercício de direitos dos titulares nos sítios eletrônicos dos órgãos públicos tem hoje boas referências nacionais, como o Portal da Autoridade Nacional de Proteção de Dados e os Tribunais de Justiça de São Paulo e de Santa Catarina. À época em que o modelo europeu era o único paradigma, nos pareceu que o modelo espanhol era o mais adequado à realidade local. Duas questões foram cruciais nas primeiras reflexões da implementação. A validação do acesso consistia na escolha da ferramenta ou procedimento que permitisse ao ente público receber a solicitação do titular e fornecer a resposta em meio eletrônico calcado certeza de que o solicitante é efetivamente a pessoa natural que alega ser. Suponha-se a hipótese em que terceiro de posse dos dados pessoais do titular formula uma demanda de garantia de direito a um órgão público. Em não havendo validação idônea, a pretexto de garantir o direito, o ente público poderia estar violando-o, falhando em garantir nessa específica atividade de tratamento a segurança que dela se espera.

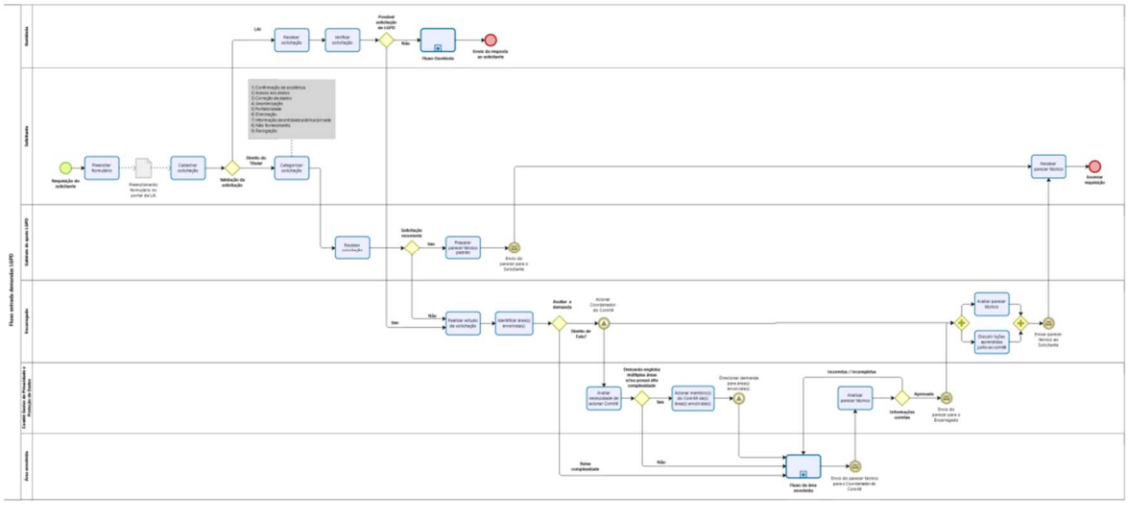
No atual contexto tecnológico, uma alternativa idônea é a validação da identidade do titular pela ferramenta de validação do Governo Eletrônico (gov.br) que é utilizada pelo governo federal em diversos serviços eletrônicos e inclusive pela ANPD. A identificação pela certificação digital padrão ICP-Brasil é talvez a mais confiável de todas as ferramentas, não apenas por utilizar criptografia de chaves assimétricas, mas por ser investida do atributo do não repúdio. Porém, por se tratar de recurso tecnológico dispendioso e ainda de pouca utilização geral, ficaria restrito a uma parcela muito pequena da população potencialmente atendida.

Dessa forma, com o viés de prover amplo atendimento àqueles que não se encontram cadastrados para utilização da ferramenta, há Tribunais que, como o Tribunal de Justiça de São Paulo, optaram por também garantir o acesso do titular pelo formulário eletrônico ou e-mail mediante o fornecimento da resposta em meio físico com checagem de identidade presencial.

A segunda reflexão na concretização desta ação consistiu no estabelecimento de um fluxo de trabalho que permitisse, dentro dos prazos legais de atendimento das demandas de garantia de direitos, tramitar o expediente interno entre o encarregado, as unidades administrativas responsáveis pela informação solicitada

e, eventualmente, contar com a análise da solicitação sob o enfoque da Lei de Acesso a Informação pelo seu responsável. Mostraram-se recorrentes as solicitações que evolviam o acesso a dados públicos, sob os auspícios da Lei de Acesso a Informação, que tinham em seu bojo dados pessoais, passíveis de garantia pela Lei de proteção de dados pessoais.

No Tribunal de Justiça de São Paulo essa função é atribuída à sua Ouvidoria e a tramitação da demanda é dos requerimentos um fator chave de sucesso na implementação desta frente de trabalho. Ainda na questão do fluxo, identificou-se a oportunidade da criação de um subfluxo de trabalho para o atendimento de demandas repetitivas, como a consulta de lotes de dados processuais, que por se tratar de uma questão eminentemente de direito, prescindia da mobilização das áreas administrativas, encerrando o atendimento no próprio órgão encarregado. Finalmente, mostrou-se proveitosa a indexação das decisões e pareceres por ementas, tal como em votos de órgãos jurisdicionais colegiados, como forma de endereçar a gestão do conhecimento produzido e promover a retenção do conhecimento na instituição, com facilidade no acesso e busca.



*Fluxo de trabalho das solicitações/requerimentos dos titulares de dados no âmbito do Tribunal de Justiça do Estado de São Paulo.

4.3.6 Revisão dos contratos, convênios e institutos congêneres

Nesta frente de trabalho, foi duramente sentida até a efetiva constituição da Autoridade Nacional de Proteção de Dados, a falta do estabelecimento de diretrizes

e cláusulas padrão a constarem dos contratos, convênios e instrumentos congêneres celebrados entre órgãos públicos e atores privados.

Dada a grande quantidade de instrumentos dessa natureza celebrados por órgãos públicos de grande porte, a varredura e adequação no âmbito do Tribunal de São Paulo teve um alcance restrito, porém consonante com os princípios norteadores das atividades de proteção de dados pessoais do artigo 6º da Lei Geral de Proteção de Dados Pessoais.

Como base na nota técnica ofertada ao Grupo de Trabalho no Conselho Nacional de Justiça que ensejou a Recomendação nº 73/2020, a revisão dos instrumentos teve como ponto de partida a identificação de alguma operação de tratamento de dado de caráter pessoal no objeto do contrato. Procedeu-se à análise de atrelamento da referida operação de tratamento aos princípios da necessidade e da finalidade, uma vez que no instrumento deveria constar de forma clara sua finalidade específica, em consonância com o interesse público e com lastro em regra de competência administrativa aplicável à situação concreta.

Referido documento técnico preconizou a realização de prévio relatório de impacto à proteção de dados pessoais dos atos que potencialmente gerariam risco a direitos e liberdades fundamentais, prevendo medidas de salvaguarda e mitigação do risco. A conformidade do contratado às normas protetivas passou a ser requisito contratual e tem no mapeamento de dados das partes relacionadas seu instrumento de controle, inclusive quanto à eliminação dos dados ao final do tratamento.

A despeito das boas iniciativas no Tribunal de Justiça de São Paulo, o papel regulatório da Autoridade Nacional de Proteção de Dados será fundamental para o amadurecimento e padronização do tratamento de dados pessoais nos contratos administrativos.

4.3.7 Segurança da informação: ações de gerenciamento de riscos

Uma política de segurança da informação deve contemplar um conjunto hierárquico de regras formado por diretrizes, normas e procedimentos. Sua finalidade é preservar os atributos de confidencialidade, integridade e disponibilidade da informação e, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.

Neste passo, se diferencia da política de privacidade pelo fato de que esta aborda a informação, não sob o ponto de vista de seus atributos, mas do tratamento dispensado ao ciclo de vida dos dados pessoais tendo como anteparo o paradigma jurídico quanto à preservação dos direitos de seu titular.

O nível de detalhamento das três espécies de regras é relacionado ao nível de gestão a que está atrelada. As diretrizes fornecem direcionamentos de nível estratégico; as normas, de nível tático; e os procedimentos, de nível operacional. A instituição de uma Política de Segurança da Informação nos órgãos de Justiça não é algo novo uma vez que a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) instituída pelo Conselho Nacional de Justiça contemplou sua obrigatoriedade junto aos Tribunais brasileiros, tendo sua primeira versão no Tribunal de Justiça de São Paulo no ano de 2008 pela Portaria nº 7.560/2008. Este é um elemento fundamental na instituição de um programa de governança de dados, tema relacionado à Lei Geral de Proteção de Dados, à Gestão Documental e à Lei de Acesso à Informação, em alinhamento com as posturas normativas do Conselho Nacional de Justiça. Conclui-se que o estabelecimento de regras claras e alinhadas às boas práticas internacionais de segurança da informação não consistem em restrição ao acesso à informação, garantido pela Lei de Acesso à Informação e de observância obrigatória em todos os órgãos públicos, mas na atribuição de transparência e segurança na guarda das informações controladas pelo ente público.

4.3.8 O órgão do encarregado

O encarregado é, por definição legal, a 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).

Em virtude da definição legal, tem sua função muitas vezes comparada ao *ombudsman*, mas dele se diferencia por ser figura ativa e de crucial importância na garantia dos direitos do titular, ainda que não seja, por definição um agente de tratamento.

Na redação original da Lei nº 13.709/18 – LGPD - foi definido como sendo uma pessoa natural. A mudança anunciada pela MPV nº 869/2018 e consagrada pela Lei 13.853/2019, passou a defini-lo somente como pessoa, abrindo as possibilidades

para que a figura do encarregado fosse constituída nas mais diversas modalidades, de modo a atender a peculiaridade de cada órgão.

A mudança foi bem-vinda, sobretudo, nos entes públicos de grande porte, como o Tribunal de Justiça de São Paulo, que devido à sua dimensão estrutural teria enorme dificuldade em concentrar a tarefa em uma única pessoa natural. Dessa forma, uma estrutura colegiada, em rede ou mesmo a terceirização da tarefa eram alternativas disponíveis.

A experiência europeia permitiu concluir que, conquanto prescindisse de uma certificação específica, o encarregado deveria reunir conhecimento jurídico sobre direitos fundamentais, além de conhecimento técnico sobre segurança da informação e gestão.

Nos estudos que precederam o projeto de implementação da Lei Geral de Proteção de Dados Pessoais no Tribunal de Justiça de São Paulo foi consenso de que caberia a um magistrado exercer a função do encarregado. Inicialmente, esta escolha apresentou alguns questionamentos. Questões como se este desempenharia a função em regime de dedicação exclusiva com afastamento da jurisdição, bem como se deveria necessariamente pertencer ao primeiro ou segundo grau de jurisdição e, finalmente, se seria um órgão singular ou colegiado, foram equacionadas, segundo informações coletadas pelos membros do encarregado de proteção de dados pessoais, pela adoção inédita de um modelo colegiado. Inspirado na composição do Conselho Diretor da Autoridade Nacional de Proteção de Dados, composta por cinco membros, o órgão encarregado no Tribunal de Justiça de São Paulo foi formado por magistrados, sendo quatro de seus integrantes Desembargadores.

O encarregado de tratamento de dados pessoais do Tribunal de Justiça de São Paulo foi formado buscando o debate construtivo entre as mais proeminentes vozes da Corte para a formação do conhecimento. Cada desembargador se debruça sobre o objeto de análise com o viés de uma Presidência de Seção (Público, Privado e Criminal) e da Corregedoria Geral da Justiça, enquanto o juiz de direito representa a visão do primeiro grau de jurisdição[74].

Como paradigma, o Tribunal de São Paulo levou em conta a estrutura de governança da Autoridade Nacional de Proteção de Dados e contemplou o Conselho

[74] A norma de estruturação do encarregado do tratamento de dados pessoais do TJSP e Comitê Gestor de Privacidade e Proteção de Dados Pessoais encontra-se disponível em: https://www.tjsp.jus.br/LGPD/ LGPD/Encarregado. Acesso em 19/12/2021.

Nacional de Proteção de Dados que desempenha função propositiva de diretrizes estratégicas, avaliação da execução de políticas públicas e fomento da cultura de proteção de dados pela realização de estudos, debates e audiências públicas. A decisão administrativa baseou-se no pleno desempenho da função do encarregado na estrutura de governança de um Tribunal ou qualquer outro órgão público de grande porte, contudo sem dispensar a criação de um comitê com tarefa análoga.

Outra importante referência de governança foi o exitoso modelo multisetorial do Comitê Gestor da Internet, parceiro acadêmico na fase preparatória de implantação, cujo modelo participativo advém do sucesso de sua atividade regulatória.

Nesse contexto, foi criado na base da estrutura de governança, o Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPPDP -, composto por um servidor de primeiro escalão de cada unidade administrativa, contemplando as áreas de administração e abastecimento, gestão de pessoas (magistrados), gestão de pessoas (servidores), organização cartorária de primeiro e segundo graus de jurisdição, orçamento e finanças, tecnologia da informação, planejamento, controle interno, precatórios, gestão do conhecimento judiciário, comunicação social, diretorias da Corregedoria Geral da Justiça, escolas de magistratura e de servidores e ouvidoria, além de contemplar os temas de gestão de precedentes e métodos consensuais de solução de conflitos.

A área de gestão documental, de crucial importância em toda e qualquer estrutura administrativa, especialmente no tema de proteção de dados, se viu contemplada na grande área de organização cartorária de primeiro e segundo graus uma vez que a ela se submete na estrutura administrativa do Tribunal de Justiça de São Paulo, muito embora ostente grau de importância equivalente às demais áreas administrativas elencadas. Isso porque a Resolução CNJ nº324/2020, regulamentada pela Portaria CNJ nº 295/2020, estabelece a clara e estreita interação entre a questão arquivística, os sistemas processuais eletrônicos e a proteção de dados.

A coordenação do CGPPDP coube a um magistrado de primeiro grau, que tem a importante função de prover o encarregado de informações e pareceres, tendo o poder de acionamento de uma ou mais áreas administrativas, conforme a necessidade de manifestação ou prospecção e coleta de dados. Na prática experimentada nas reuniões semanais de governança de dados, o magistrado coordenador do CGPPDP funciona como um efetivo sexto integrante do órgão

encarregado que, conquanto não tenha formalmente o poder de voto, consiste na voz que mais próxima está da atividade meio, fato este que o qualifica como o interlocutor das reflexões da área administrativa nas discussões do órgão encarregado.

Tal como ocorre nas estruturas administrativas da Ouvidoria e do Serviço de Informação ao Cidadão – SIC -, a organização dos trabalhos exige desforço concentrado não assimilável, pelo menos no caso em estudo, por qualquer outra unidade administrativa. Por esse motivo entre o Encarregado e o CGPPDP criou-se um Gabinete de Apoio ao Encarregado, integrado por três servidores de carreira que possuem a função administrativa e organizacional de gerenciamento de demandas do Encarregado.

O modelo estrutural da governança de dados criado pelo Tribunal de Justiça de São Paulo, em funcionamento desde a data da entrada em vigor da Lei Geral de Proteção de Dados Pessoais, tem se mostrado virtuoso e apto a produzir decisões e conteúdo compatíveis com o porte da Corte. Conclui-se que, observadas as necessárias alterações quanto às posições ocupadas por magistrados, o modelo estrutural tem a aptidão de bem atender a outros órgãos públicos de grande porte, suprindo eventual lacuna normativa quanto à sua estruturação na novel legislação.

5 CONSIDERAÇÕES FINAIS

BIBLIOGRAFIA

ASCENSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Rio de Janeiro: Forense, 2002.

ATTARD, Judie. ORLANDI, Fabrizio. SCERRI, Simon. AUER, Sörenl. A Systematic Review of Open Government Data Initiatives. In Government Information Quarterly. V. 32. Ed. 4. 2015, p. 399 a 418, 2015. Disponível em:https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: 12 de julho de 2021.

BARBIERI, Carlos. Governança de Dados: prática, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2020.

BENNET, Colin. Regulating Privacy. Data Protection and Public Policy in Europe and the United States. Ithaca and London: Cornell Univerty Press, 1992.

CASTELLS, Manuel. A Sociedade em Rede. Tradução de Alexandra Lemos e Rita Espanha. Sob a coordenação de José Manuel Paquete de Oliveira e Gustavo Leitão Cardoso. Lisboa: Fundação Calouste Gulbenkian, 2003.

CRESPO, Marcelo. *Compliance* Digital. In NOHARA, Irene Patrícia. PEREIRA, Flávio de Leão Bastos. (Coord.). Governança, *Compliance* e Cidadania. São Paulo: Revista dos Tribunais, 2018.

CASTELLS, Manuel. A Sociedade em Rede. Tradução de Alexandra Lemos e Rita Espanha. Sob a coordenação de José Manuel Paquete de Oliveira e Gustavo Leitão Cardoso. Lisboa: Fundação Calouste Gulbenkian, 2003.

CUEVA, Ricardo Villas Bôas. A Insuficiente Proteção de Dados Pessoais no Brasil. Revista de Direito Civil Contemporâneo, v. 13, ano 4, out-dez. 2017.

DANEZIS, George et. al. Privacy and Data Protection By Design – From Policy to Engineering. ENISA (Euroepan Union Agency for Cybersecurity), 2015. p. 11, tradução livre. Disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-bydesign. Acesso em: 20 mai. 2021.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020. 2ª Edição.

FERREIRA, Eliana Junqueira Munhós. A Lei de Acesso à Informação no Âmbito do Judiciário e a Vinculação do SIC às Ouvidorias Judiciárias: uma proposta para o monitoramento e gestão da informação. In CUEVA, Ricardo Villas Bôas e al (coord.). Belo Horizonte: Fórum, 2019.

FILHO, Adalberto Simão. A Governança Corporativa Aplicada às Boas Práticas e *Compliance* na Segurança dos Dados. In Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, 2018.

FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais. Noções Introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVIA, Milena. Lei Geral de Proteção de Dados

Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Revistas dos Tribunais, 2019.

GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. São Paulo: Atlas, 2020 (4ª reimpr.).

GONÇALVES, Pedro. Entidades Privadas com Poderes Públicos. Coimbra: Almedina, 2005.

HUGHES, Owen. Does Governance Exist? In The New Public Governance. Emerging Perspectives on the Theory and Practice of Public Governance. Editado por Stephen P. Osborne. Londres, Nova York: Routledge, 2010.

LAGE, Fernanda de Carvalho. Manual de Inteligência Artificial no Direito brasileiro. Salvador: Editora JusPodivm, 2021.

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

LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. São Paulo: Almedida, 2020.

MENDES, Laura Schertel. BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção Dados Brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor. Vol. 124. Ano 28, p. 157 a 180. São Paulo: Revista dos Tribunais. Julho-Agosto, 2019.

MENDES, Laura Schertel. DONEDA, Danilo. Comentários à Nova Lei de Proteção de Dados (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil. Revista de Direito do Consumidor. Vol. 120. Ano 27, p. 555 a 587. São Paulo: Revista dos Tribunais. Novembro-Dezembro 2018.

MENDES, Laura Schertel. DONEDA, Danilo. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor. Vol. 120. Ano 27, p. 469 a 483. São Paulo: Revista dos Tribunais. Novembro-Dezembro 2018.

MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Edição Kindle.

MENKE, Fabiano. A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão. In Revista Luso-Brasileira (RJLB), ano 5 (2019). nº 1.

MILLARD, Christopher (Ed.). Cloud Computing Law. Oxford: Oxford University Press, 2013. E-book.

MONCAU, Luiz Fernando Marrey. Direito ao Esquecimento. São Paulo: Thomson Reuters Brasil, 2020.

PASQUALE, Frank. The Black Box Society. The Secret Algorithms that Control Money and Information. Cambridge: Harvard University Press, 2015.

RODOTÁ, Stefano. A Vida na Sociedade de Vigilância. A Privacidade Hoje. Tradução de Danilo Doneda e Laura Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTAMARÍA PASTOR, Juan Alfonso. Principios de Derecho Administrativo General I. Madrid: Iustel, 2004. (reimpressão, 2006).

SIMITIS, Spiros. Crisi Dell'informazioni Giuridica ed Elaborazione Elettronica dei Dati. Milano: Giuffrè, 1977.

SCHWAB, Klaus. A Quarta Revolução Industrial. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2019.

SCHWARTZ, Paul M. PEIFER, Karl-Nikolaus. Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept? California Law Review. vol. 98. Pág. 1925. 2010. UC Berkeley Public Law Research Paper nº. 1816885. Disponível em SSRN: https://ssrn.com/abstract=1816885. Acesso em 01/12/2021.

SRNICEK, Nick. Platform Capitalism. Cambridge: Polity Press, 2018.

TASSO, Fernando Antonio. Do Tratamento de Dados Pessoais pelo Poder Público. In MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019, p. 245 a 289.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. In: Cadernos Jurídicos – Escola Paulista da Magistratura. São Paulo: 2020. Disponível em: https://epm.tjsp.jus.br/Publicacoes/CadernoJuridico/60662?pagina=1. Acesso em 03/11/2021.

VENTURA, Leonardo Henrique de Carvalho. Considerações sobre a Nova Lei Geral de Proteção de Dados. Revista Síntese: Direito Administrativo, v. 13, n. 155, nov. 2018.

WARREN, Samuel D. BRANDEIS, Louis D. Harvard Law Review. v. IV, nº 5, dec. 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em 03/12/2021.

WESTIN, Alan. Privacy and Freedom. New York: Atheneum, 1967.

WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In DONEDA, Danilo. SARLET, Ingo Wolfgang. MENDES, Laura Schertel. RODRIGUES JUNIOR, Otavio Luis (Org.). Tratado da Proteção de Dados no Brasil, no Direito Estrangeiro e Internacional. Rio de Janeiro: Forense, 2021. Edição Kindle, p. 385 a 743.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism. Londres: Profile Books Ltd, 2019. Kindle.

Sites internet

BRASIL. Conselho Nacional de Justiça. Justiça em Números 2021. Brasília: CNJ, 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/11/relatorio-justica-em-numeros2021-221121.pdf. Acesso em 11/12/2021.

Bundesverfassungsgericht – Corte Constitucional alemã https://www.bundesverfassungsgericht.de/EN/Service/Datenschutz/Datenschutz_en_node.html. Acesso em 14/07/2021.

European Court of Justice - https://curia.europa.eu/jcms/jcms/p1_2699100/en/. Acesso em 14/07/2021.

ICO. 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 23/01/2021.

Information Commissioner's Office - Reino Unido - https://ico.org.uk/global/privacy-notice/. Acesso em 14/07/2021.

https://www.ibge.gov.br/cidades-e-estados/sp.html. Acesso em 14/07/2021.

https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em 30/12/2021

https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: 12 de julho de 2021.

https://www.youtube.com/watch?v=1Vk6bAlLB_o. Acesso em 12 de junho de 2021.

https://atos.cnj.jus.br/atos/detalhar/3489. Acesso em 01/12/2021.

https://www.tjsp.jus.br/Download/Portal/LGPD/Portaria_9912_20.pdf?637755147157389963. Acesso em 10/12/2021

https://www.tjsp.jus.br/lgpd. Acesso em 30/12/2021.

http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em 03/12/2021.

https://ssrn.com/abstract=1816885. Acesso em 01/12/2021.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434#B-1. Acesso em 02/01/2021.

Resolução do Parlamento Europeu de 06 de outubro de 2021, sobre a inteligência artificial no direito penal e sua utilização pelas autoridades policiais e judiciárias em casos penais: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso em 02/01/2021.

A matriz de elaboração do formulário eletrônico utilizado no TJSP encontra-se disponível em: https://www.tjsp.jus.br/Download/Portal/LGPD/Anamnese.pdf. Acesso em 01/12/2021

ANEXOS

Lei Geral de Proteção de Dados – LGPD – Lei nº 13.709/2018.

Lei do Cadastro Positivo – Lei nº 12.414/2011.

Lei de Acesso à Informação – Lei nº 12.527/2011.

Marco Civil da Internet – Lei nº 12.965/2014.

Lei do Habeas Data – Lei nº 9.507/1997.

Lei dos Arquivos Públicos – Lei nº 8.159/1991.

Recomendação CNJ nº 73

Resolução CNJ nº 363

Recomendação CNJ nº 89

Resolução CNJ nº 334

Resolução CNJ nº 335

Resolução CNJ nº 215

Resolução CNJ nº 121

Portaria CNJ nº 41

Portaria CNJ nº 212

E-mail/ofício enviado ao órgão do Encarregado de proteção de dados pessoais do Tribunal de Justiça do Estado de São Paulo.

Resposta ao e-mail enviado ao órgão do Encarregado de proteção de dados pessoais do Tribunal de Justiça do Estado de São Paulo.

Links na plataforma *Teams* das entrevistas realizadas com os membros integrantes dos órgãos de governança de proteção de dados pessoais no âmbito do Tribunal de Justiça do Estado de São Paulo.

Tabela de cookies do portal do Tribunal de Justiça do Estado de São Paulo.

Portarias expedidas pela Presidência do Tribunal de Justiça do Estado de São Paulo que instituíram: i) a política de privacidade; ii) a política de proteção de dados pessoais; e iii) a política de segurança da informação.

Portaria expedida pela Presidência do Tribunal de Justiça do Estado de São Paulo que instituiu o órgão do Encarregado de proteção de dados pessoais, o Comitê Gestor de Privacidade e Proteção de Dados Pessoais.

Registro de tratamento de dados – anamnese organizacional e registro de atividades de tratamento. Procedimento de mapeamento de dados.