(IN)CONSTITUCIONALIDADE DO DECRETO N.0.046/2019 À LUZ DOS PRINCÍPIOS POSITIVADOS NA LEGISLAÇÃO DE PROTEÇÃO DE DADOS

Josias Ezequiel Julierme Mazzurana[1]
Aleteia Hummes Thaines[2]

Introdução

Avanços da tecnologia da informação e seus impactos na vida em sociedade elucidaram a importância dos dados ao desenvolvimento econômico, político e social. A massificação no uso de dados, assim como otimização de processos, fez com que esses fossem comparados ao petróleo, um novo petróleo, visto a plasticidade desta informação e sua fundamental importância ao desenvolvimento de um Estado moderno. No entanto, se expôs a fragilidade com que dados pessoais podem ser tratados de forma a intervir no cotidiano das pessoas, inclusive fragilizando o direito fundamental de privacidade e, por vezes, até o próprio Estado Democrático de Direito.

De forma a assegurar o livre desenvolvimento da personalidade, autodeterminação informativa e a privacidade, o direito à proteção de dados ganhou assento constitucional, assim como norma protetiva desse direito, representada pela Lei n. 13.709/2018, caracterizada por ser principiológica. Essas diretrizes devem pautar o tratamento de dados pelo poder público. Neste contexto, no uso do poder discricionário, promulgou-se o Decreto n. 10.046/2019, com a finalidade de disciplinar o compartilhamento de dados no âmbito da administração pública federal, instituir o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Assim, este estudo apresenta como tema a Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Para tanto, delimitou-se a ele à análise quanto à (In)Constitucionalidade do Decreto n. 10.046/2019, à luz dos princípios positivados na legislação de proteção de dados. Diante do exposto, a pesquisa apresenta o seguinte questionamento: Há ofensa ao direito fundamental de proteção de dados e aos princípios da LGPD nos procedimentos contidos no Decreto n. 10.046/2019, em especial, às regras gerais de compartilhamento, ao desenho institucional do Cadastro Base do Cidadão, o acesso a dados pessoais para além das finalidades para a realização dos objetivos, configurando sua inconstitucionalidade?

Objetivos

A presente pesquisa tem por objetivo analisar a (in)constitucionalidade do Decreto n. 10.046/2019 frente aos princípios da LGPD e ao direito fundamental de proteção de dados. Como objetivos específicos, delineou-se: a) analisar a lógica procedimental de salvaguardas na Lei Geral de Proteção de Dados Pessoais e seu impacto junto ao Decreto 10.046/2019; b) examinar a proteção de dados pessoais como valor social e não apenas individual; c) verificar se o tratamento de dados,

[1] Graduado em Direito pela FACCAT. Graduado em História pela FACCAT. Endereço eletrônico: josias@faccat.br

[2] Doutora em Direito com estágio Pós-doutoral em Direito. Professora do Curso de Direito e do Programa de Pós-Graduação em Desenvolvimento Regional das Faculdades Integradas de Taquara/RS (FACCAT). Pesquisa vinculada ao Curso de Direito e a linha de pesquisa **Economia, Meio Ambiente e Dinâmicas de Desenvolvimento Territorial Sustentável**, do Programa de Pós-Graduação em Desenvolvimento Regional, da Faccat. Endereço eletrônico: aleteiathaines@faccat.br

ainda que realizado pelo Poder Público, estaria, de fato, servindo ao interesse público, mesmo que não observe os princípios basilares da Proteção de dados pessoais; e, d) analisar a (in)compatibilidade do Decreto n. 10.046/2019 com os princípios constitucionais e basilares da LGPD no que tange a proteção de dados.

Metodologia

O estudo trata de uma investigação que está envolta do direito fundamental à proteção de dados. Assim, para confirmação dos objetivos propostos e rigor científico, aspectos metodológicos apresentam-se da seguinte forma: a pesquisa está pautada no método hipotético-dedutivo, pois, em um primeiro lugar, defende o aparecimento do problema e da conjuntura, como ocorre no objeto de análise da presente pesquisa (a (in)constitucionalidade do Decreto n. 10.046/2019).

Ademais, a pesquisa é caracterizada como básica, qualitativa, bibliográfica e documental. Quanto aos dados coletados, o mesmo se consubstanciada em livros e artigos relevantes publicados, bem como em atos normativos e jurisprudências atinentes à matéria, em formato físico ou em digitais. Ademais, a documentação foi utilizada com a finalidade de corroborar e valorizar as evidências oriundas das fontes bibliográficas. Quanto aos atos normativos e jurisprudências, estes foram coletados junto ao site do Planalto (planalto.gov.br) e, em razão da matéria, no portal do Supremo Tribunal Federal (https://portal.stf.jus.br/). As fontes bibliográficas foram acessadas, no formato virtual, junto a Minha Biblioteca, por meio do site das Faculdades Integradas de Taquara (www.faccat.br). Já as obras físicas foram consultadas na Biblioteca da referida Instituição. No que tange a análise e interpretação dos dados, visto tratar-se de uma pesquisa qualitativa, ocorreu em concomitância à coleta destes.

Resultados e Discussão

Atualmente, se assiste a uma escalada de incidentes relacionados ao tratamento de dados pessoais, em diversas esferas, públicas e privadas. Não diferente ocorreu com o Conselho Nacional de Justiça (CNJ), na tarde de 1º de abril de 2019, ao ser objeto de ataque de hackers, em que informações pessoais e credenciais de acesso para serviços do CNJ foram vazadas (CONJUR, 2019).

Em pesquisa realizada pelo Massachusetts Institute of Technology (“MIT”), publicada no Journal of Data and Information Quality da ACM (Association for Computing Machinery), destaca-se a evolução do vazamento de dados no Brasil, com aumento de 493%, entre 2018 e 2019 (VCS/A, 2021). O elevado tráfego de dados no país apresentou, também, como estatística relevante o roubo de credenciais.

Em relatório da Empresa Akamai (especializada em segurança digital), no ano de 2020, foram 3 bilhões de tentativas de roubo de credenciais no Brasil, com 1,6 bilhão tendo origem no próprio país (CANALTECH, 2021). Ainda, a empresa de segurança cibernética PSafe, noticiou dois megavazamento de dados. O primeiro, envolveu o vazamento de 223 milhões de CPFs, “como identidades e datas de nascimento, bem como informações de 104 milhões de veículos e de 40 milhões de empresas, como CNPJ, razão social, nome fantasia e data de constituição” (VCS/A, 2021). E um segundo vazamento de 140 milhões de dados pessoais, abrangeu “telefone, formação acadêmica, salário, endereços e fotos” (VCS/A, 2021). A referência demonstra que, mesmo instituições com elevado grau de segurança na proteção de dados, elas objeto de ataques e consequentes incidentes.

O tratamento de dados pessoais estão no centro das mais diversas discussões, bem como temas a ele correlacionados, como a higidez do Estado, a

privacidade, a liberdade de informação, o desenvolvimento econômico e tecnológico. De modo a salvaguardar o direito à proteção de dados pessoais, esta foi elevada ao status de direito fundamental (art.5, LXXIX, da Constituição Federal de 1988, alterada por meio da Emenda Constitucional 115/2022), bem como editada norma procedimental de salvaguarda, atualmente conhecida como Lei Geral de Proteção de Dados (Lei n 13.709/2018).

Os referidos marcos regulatórios, ao estabelecer direitos e garantias aos titulares quanto à proteção de dados, reconhecem a relevância jurídica deste fenômeno, buscando diminuir os riscos quando de seu tratamento. Ademais, a salvaguarda legal busca proporcionar maior controle e proteção às informações pessoais, proporcionando espaços para o tratamento legítimo e lícito, de modo a garantir a autodeterminação informativa de seu titular (BIONI, 2020). No entanto, em que pese a regulamentação constitucional e infraconstitucional no que tange a proteção de dados pessoais, há necessidade de sedimentar contornos ainda existentes. Parte das discussões estão em torno dos parâmetros do tratamento de dados pessoais pelo Estado, por meio de um grande banco de dados, como resultado do Decreto n. 10.046/2019.

Na Sociedade da Informação, em que seu titular é mero expectador (BIONI, 2021), um sofisticado sistema de dados, em que diferentes órgãos do governo terão acesso, sob o argumento de maior eficiência na prestação de serviços públicos, poderá resultar no controle dos cidadãos. Assim como, a exemplo do que ocorreu com o Conselho Nacional de Justiça, resultar, em razão do grande volume de informações, em um incidente de difícil reparação, não atingindo somente a esfera individual do sujeito (privacidade), mas, também, toda a coletividade, visto o caráter metaindividual que envolve a autodeterminação informativa.

Considerações finais

A necessidade de preservação da dignidade da pessoa humana, associada ao uso indiscriminado de dados pessoais, levantou o debate acerca da autonomia deste direito como integrante da personalidade humana, sendo construído, nas últimas décadas, um novo direito fundamental, um direito à proteção de dados, que se efetivou com a Emenda Constitucional n.115/2022. O Brasil, com a promulgação da Lei n. 13.709/2018 - LGPD -, inspirada no Regulamento Geral de Proteção de Dados (RGDP), definiu regulamentação própria no que tange ao tratamento de dados pessoais, passando a integrar, mesmo que tardiamente, com entrada em vigor em agosto de 2020, em razão de um período de vacatio legis, o grupo de países com diretrizes próprias de coleta, gerenciamento e proteção de informações pessoais à luz do desenvolvimento econômico, tecnológico e da inovação.

No entanto, a lei protetiva, com fundamento no direito à privacidade e autodeterminação informativa, além de definições de obrigações aos controladores e operadores de dados, como alicerce normativo a proteção de dados, traz, consigo, reflexões acerca da vulnerabilidade das informações pessoais tratadas. E, neste panorama jurídico foi promulgado o Decreto n. 10.406/2019, com a finalidade de disciplinar o compartilhamento de dados no âmbito da administração pública federal, instituir o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Em análise, percebe-se que o Decreto n. 10.046/2019 traz inovações acerca do tratamento de dados pela administração pública, sem, no entanto, regular efetivamente o Capítulo IV da Lei nº 13.709/2018. Ademais, o decreto destoa de disposições da LGPD ao ordenar regras contrárias ao marco protetivo de dados, inovando em questões de tratamento de dados, assumindo feições

autônomas, a partir de características genéricas e abstratas, violando, a priori, dispositivos constitucionais (art. 5º, X, XII e XXXIII da CF/1988), ensejando a proposição de remédios de controle de constitucionalidade.

Neste cenário, importa destacar a Ação Direta de Inconstitucionalidade n. 6.649/2021 e a Arguição de Descumprimento de Preceito Fundamental n. 695/2021, que, em julgamento conjunto datado de 15 de setembro de 2022, o Supremo Tribunal Federal decidiu pela constitucionalidade do Decreto n. 10.046/2019, compreendo por legítimo o compartilhamento de dados por órgãos da administração pública, uma vez observados parâmetros como a legitimidade e especificidade do propósito no tratamento de dados, restrito, ainda, apenas às informações indispensáveis ao interesse público.

No entanto, em que pese a decisão da Suprema Corte, a criação de um grande banco de dados, com livre compartilhamento de informações no âmbito da administração pública federal, destoa das salvaguardas para a proteção de dados pessoais contidas na LGDP, bem como vai na contramão das garantias e direitos constitucionais. Com isso, acentua-se a qualidade de mero expectador do titular dos dados, expondo sua fragilidade quanto aos interesses do Estado ao deter o controle concentrado de suas informações pessoais, podendo interligá-las a uma variedade de dados tratados nos diferentes órgãos da administração pública, justificando-se, apenas, pelo requisito abstrato do interesse e eficiência das políticas públicas, sem serem esclarecidas previamente.

Assim, o compartilhamento de dados entre as diferentes bases, conforme proposto junto ao Decreto n. 10.046/2019, sem critérios claros e definidos, está em desconformidade com os preceitos de salvaguarda constantes na LGPD, bem como ofende o princípio constitucional de proteção de dados e privacidade.

Dessa forma, ao não se harmonizar aos regulamentos de salvaguarda à proteção de dados, como a Lei n. 13.709/2018, o Poder Público, no uso de um instituto de origem democrática (poder regulamentar), moldou o ato executivo de forma a representar riscos à democracia e aos direitos fundamentais. Assim, o retrocesso democrático e ameaça ao constitucionalismo dá-se, quanto ao Decreto n. 10.046/2019, como resultado de promulgação normativa pontual, com aparência válida em relação ao aspecto formal (competência discricionário do executivo); porém, quando de sua análise, de forma isolada, evidenciam-se inquietações acerca da sua constitucionalidade. A norma que se diz regulamentar, externa medidas que, de forma progressiva, desgastam a tutela do direito à proteção de dados, bem como o regime Democrático de Direito.

Grupo de Trabalho a ser submetido: GT 4 - Direito, Propriedade Intelectual e Proteção de Dados

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A Função e os Limites do Consentimento. 3 ed. São Paulo: Grupo GEN, Edit. Forense, 2021.

BIONI, Bruno Ricardo. **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, Edit. Forense, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 de maio de 2022.

BRASIL. **Decreto n. 10.046**, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm.Acess o em: 3 de maio de 2022.

BRASIL. **Lei n. 13.709**,de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 3 de maio de 2022.

CANALTECH. **Brasil teve mais de 3 bilhões de roubos de credenciais em 2020**. Disponível em: https://canaltech.com.br/seguranca/relatorio-aponta-mais-de-3-bilhoes-de-roubos-decredenciais-no-brasil-em-2020-183762/. Acesso em: 03 de dezembro de 2022.

CONSULTOR JURÍDICO. **CNJ sofre ataque de hacker e dados de milhares de pessoas são vazados**. Disponível em: https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pess oas-vazam. Acesso em: 29 de maio de 2022.

VCS/A. **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT**. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-br asil-segundo-pesquisa-do-mit/. Acesso em: 03 de dezembro de 2022.