ARTIGO

DADOS PESSOAIS: A VERTIGEM DEMOCRÁTICA CATALISADA ATRAVÉS DA "INDEPENDÊNCIA" DOS ÓRGÃOS FISCALIZADORES

Alencar Barbieri
Marine Lauschner
Rodrigo da Costa Morais
Alexandra Vanessa Klein Perico

Resumo

Ante o prisma da demasiada valoração econômica conferida aos dados pessoais como o petróleo do século XXI, o Brasil criou normas que tutelam as arbitrariedades de amplos setores. Em que pese tenha ocorrido a criação da Lei Geral de Proteção de Dados e a posterior elaboração do anteprojeto que resguarda, nos mesmos moldes, os dados vinculados ao sistema penal, a lei e o anteprojeto demonstram-se ambíguas e controversas, levando em conta as autoridades competentes pela fiscalização e resguardo dos dados pessoais. Portanto, o presente artigo alude os principais aspectos que permeiam o assunto, no intento de alcançar meios capazes de minorar a disparidade social ocasionada pelo poderio estatal alinhado à fragilidade e prepotência dos órgãos fiscalizadores. Assim, evitando que se retroceda a tempos longínquos em que o titular dos dados, erroneamente, era mero espectador de um palco constantemente visível, tal qual aos panópticos, que numa única estrutura física segregacionavam temerariamente presidiários, criando ditaduras irremovíveis, semelhante às estruturas virtuais contemporâneas que discretamente colocam em xeque a Democracia.

Palavras-chave: Lei Geral de Proteção de Dados; Finalidade pública; Tratamento de dados; Segurança Pública; Persecução Penal.

1 INTRODUÇÃO

Alguns países, diante da propagação desenfreada de dados no século XX, marcada pela exploração, concentração e capitalização crescente e exponencial de informações e de dados alusivos à pessoa natural, despertaram para a necessidade de buscar meios de proteção aos dados de seus cidadãos. Esse desprovimento legislativo levou a Alemanha ao pioneirismo normativo na esfera protetiva de dados, com a primogênita legislação sobre a temática em 1975, aclarando o caminho às outras nações.

No Brasil, o embrião da proteção de dados adveio com a Constituição Cidadã de 1988 que positivou, no artigo 5°, a inviolabilidade da intimidade, vida privada e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, dentre outros direitos fundamentais. Essa proteção foi ampliada através de legislações esparsas que previam singularmente a proteção às informações que constavam nos bancos de dados estatais e privados.

Outrossim, com o propósito de consolidar plenamente a salvaguarda destes dados, o Poder Legislativo brasileiro promulgou, em agosto de 2018, a Lei 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD). Ato contínuo pôs em debate um anteprojeto de desígnio análogo ao da lei citada, que albergasse as lacunas penais públicas outrora ignoradas.

Ante ao exposto, o corrente artigo visa, através de revisões bibliográficas obtidas em artigos, legislações e nos meios eletrônicos, contrastar particularidades ambíguas das autoridades reguladoras, guiadas pelas rédeas da conveniência estatal em trilhos antagônicos aos princípios e diretrizes constitucionais, de modo que, a "finalidade pública" se adequa à ótica oportuna, conforme o transcender dos tempos e das políticas governamentais.

O subterfúgio da finalidade, sutilmente aquiesce a formação de ditaduras digitais através da capitalização dos dados pessoais, onde constantes violações são sinônimo de habitualidade e a demasiada visibilidade enaltecida nos panópticos que corrobora para atos arbitrários, como o fruto da ADPF 722, que culminam na vertigem da democracia.

No entanto, quiçá a maior adversidade brasileira na efetiva proteção dos dados pessoais esteja na submissão das autoridades reguladoras ao poder estatal, de modo que, a questão a enaltecer neste artigo consiste em responder se realmente é possível assegurar a ínfima proteção de dados pessoais frente a desvirtualização da democracia.

2 **DESENVOLVIMENTO**

2.1 LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD introduziu normas para o tratamento de dados realizado por pessoas naturais ou pessoas jurídicas de direito público ou privado, cujo objetivo é garantir a proteção dos dados pessoais, possuindo como fundamentos precípuos o respeito à privacidade, a autodeterminação informativa, inviolabilidade da intimidade, da honra e da imagem (BRASIL, 2018).

A lei discrimina e conceitua três espécies de dados. Os pessoais, como as informações relacionadas à pessoa natural identificada ou identificável, por exemplo, nome, RG, CPF e endereço residencial. Os sensíveis, informações atinentes à convicção religiosa, opinião política, dados referentes à saúde, além de dados genéticos ou biométricos, quando vinculados a uma pessoa natural. E, os anonimizados, são os dados que não podem ser relacionados ao titular através da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (BRASIL, 2018).

Ainda, no inciso X, do artigo 5º, conceituou o tratamento de dados, como toda operação realizada com os dados pessoais, referente a coleta, produção, utilização, acesso, reprodução, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nesse sentido, qualquer coleta e operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenham por finalidade a oferta de produtos ou serviços no país, estão

sujeitos a LGPD, que passa a exigir o consentimento expresso do usuário para a utilização e tratamento dos seus dados para uma finalidade determinada e específica, sendo vedado o consentimento genérico.

2.1.1 As exclusões de alguns agentes no tratamento de dados

Dentre as exceções singulares à aplicação da LGPD, destaca-se, no presente artigo, os aspectos concernentes à segurança pública, defesa nacional, segurança do Estado e atividade de investigação e repressão de infrações penais.

A ausência normativa no tratamento dos dados aludidos, é motivada pelo fato dessas atividades se revestirem de caráter puramente estatal e como escudo protetivo da administração pública de qualquer responsabilidade quanto aos procedimentos realizados. Entretanto, apesar de abrangente as situações de tratamento de dados nessas atividades, nada justifica, sob o argumento de garantir a segurança pública, a lesão à proteção desses dados (ROSSO, 2019).

Inobstante, na perspectiva penal, relativa ao tratamento de dados pessoais, há que se levar em conta o titular dos dados como o autor de uma infração ou como vítima dela. E também que, numa investigação criminal, os dados de testemunhas, peritos ou mesmo de terceiros, sem nenhuma relação com o fato a ser provado, poderão ser submetidos à ingerência do Estado, especialmente no curso da investigação criminal (ARAS et al., 2020).

Além disso, a única legislação abordando a temática, não de proteção, mas de tratamento desses dados na segurança pública e persecução penal, é a Lei 12.850 de 2013, que confere amplos poderes aodelegado e ao promotor de justiça na persecução de infrações penais. Essalei não protege o titular dos dados e tão pouco oportuna o mínimo de segurança a todos os envolvidos, na realidade, ela mitiga uma ampla gamade direitos fundamentais inerentes aos sujeitos.

Nesse sentido, as normas de proteção de dados pessoais devem aplicar-se também ao Estado quando coleta, manipula e difunde dados

pessoais de investigados, suspeitos, réus, vítimas, testemunhas, peritos, autoridades e funcionários que atuam na persecução criminal e de terceiros, eventualmente alcançados por medidas de apuração de investigações criminais e de segurança pública, cujas atividades estatais interferem rotineiramente na vida dos cidadãos, tornando-se valorável a perspectiva da privacidade (ARAS et al., 2020).

2.2 A INSEGURANÇA NA PROTEÇÃO DE DADOS REFERENTE À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A redação original da LGPD previa, como autarquia vinculada ao Ministério da Justiça, a ANPD (Agência Nacional de Proteção de Dados), cuja criação teria o intento elementar de zelar pela proteção de dados pessoais, fiscalização e aplicação de sanções em caso de descumprimento da legislação. Contudo houve o veto presidencial, motivado pelo advento de suposto vício de iniciativa para sua criação, por ser resultante de ato do Poder Legislativo (VILHALBA, 2018).

Posteriormente, a Lei 13.853 de 2019 alterou alguns dispositivos da LGPD e criou a Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, sanando a lacuna deixada pelo veto presidencial quando da sanção da lei. Porém, diferente do previsto no texto original aprovado pelo Congresso e vetado pela presidência, a lei criou a ANPD como órgão da administração pública federal, integrante da Presidência da República (BONFIM, 2019).

No tangente à pluralidade de competências conferidas à ANPD, por pertinência, cita-se: editar normas e procedimentos sobre a proteção de dados pessoais, fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, comunicar às autoridades competentes as infrações penais das quais tiver conhecimento e comunicar aos órgãos de controle interno o descumprimento do disposto na lei praticado por órgãos e entidades da administração pública (BONFIM, 2019).

Ademais, esta subordinação direta da Agência ao órgão máximo do Executivo Federal afeta em demasia a autonomia, independência, fiscalização e as decisões de caráter técnico inerentes ao tema, em relação ao conceito previsto na primeira versão da Lei, hospedando a dúvida sobre até que ponto uma futura decisão política do Executivo Federal poderá suplantar uma análise técnica e independente sobre o escopo da LGPD (ATHENIENSE, 2018).

2.3 AS EXPECTATIVAS DE PROTEÇÃO DO TRATAMENTO DE DADOS NA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL

Hodiernamente tramita no Congresso Nacional, sob a alcunha de "LGPD Penal", o anteprojeto de Lei Geral de Proteção de Dados para segurança pública e persecução penal, no qual o legislador pretende estabelecer princípios basilares e diretrizes para que a futura autoridade competente da "LGPD Penal" possa desempenhar suas funções com maior segurança jurídica e também proteger o cidadão contra eventuais abusos e arbitrariedades estatais. Em síntese, o objetivo é compatibilizar os deveres do Estado quanto à prevenção, repressão de ilícitos criminais e às garantias processuais e prerrogativas fundamentais dos cidadãos no âmbito da proteção de dados pessoais (FIGUEIRA, 2020).

O Anteprojeto prevê, como autoridade, o Conselho Nacional de Justiça (CNJ) responsável pela aplicação, supervisão e monitoramento dos procedimentos. O CNJ foi escolhido graças a sua autonomia e composição plural (indicações do STF, STJ, TST, PGR, Conselho Federal da OAB, do Congresso Nacional), além da natureza financeira, a qual evitaria novos gastos exacerbados na criação de um órgão específico, e principalmente pela independência de que dispõe esse órgão, cujas políticas permitiriam ser uniformes em todo o país (FIGUEIRA, 2020)

A intenção é concentrar os poderes de supervisão num órgão externo ao Executivo. Todavia, trata-se de uma proposta inicial da "LGPD Penal" e o Congresso debaterá se manterá essa proposta ou se definirá como

autoridade a prevista na LGPD, isto é, a Autoridade Nacional de Proteção de Dados Pessoais, vinculada à Presidência da República.

Nesse ponto, vale frisar a possibilidade de um conflito de competência entre a ANPD e o CNJ. O art. 4º, inciso III, §3º da LGPD estabelece que "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais." Ora, se a LGPD não se aplica às hipóteses de segurança pública, defesa nacional e persecução penal, como pode prever também a atuação da ANPD na matéria (FIGUEIRA, 2020).

Não se pode esquecer, qualquer que seja o órgão responsável pela supervisão da "LGPD Penal", este concentrará demasiado poder e poderá influenciar os rumos da política nacional de segurança pública e por esse motivo, necessita de autonomia e independência, caso contrário, reunirá, nas mãos da alta cúpula política brasileira, poderes ilegítimos, que podem ser utilizados com fins diversos ao interesse público e quiçá eleitorais, em afronta ao Estado Democrático de Direito.

2.3.1 Considerações sobre a ADPF 722 e o Decreto 9.662

Corroborando o tópico anterior, o Supremo Tribunal Federal fora instado a decidir a ADPF 722 correlacionada ao suposto dossiê antifascita, fomentado pelo poder estatal vigente, sob o argumento de prevenção de danos à segurança nacional, em especial no que tange a necessidade de prevenir, neutralizar e reprimir atos criminosos.

Conseguinte as notícias vinculadas ao caso, o Dossiê produzido pela SEOPI (Secretaria de Operações Integradas) ancorada ao Ministério da Justiça, conteria 579 nomes, fotografias, endereços de redes sociais das pessoas intituladas de "antifascistas" (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020). Esse relatório estaria sendo distribuído às administrações públicas, dilatando o âmbito de controle desses dados, além da previsão de acesso restrito pelos próximos 100 anos.

Neste ínterim, o dossiê, cuja criação se deu a partir das assinaturas de um manifesto que pugnava pela resposta governamental contrária à ruptura institucional, os participantes foram monitorados e seus dados sensíveis tratados entre a Polícia Rodoviária Federal, Casa Civil da Presidência da República, Abin, Força Nacional e três centros de inteligência vinculados à SEOPI (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020).

Conforme a Rede Sustentabilidade - autora da ADPF- o Ministério da Justiça, sob o pretexto mascarado de exercer atividade de inteligência, estaria se utilizando do aparato estatal para fins de perseguição política e ideológica, interferindo ilicitamente nos direitos à liberdade de expressão, vida privada e à intimidade.

Inclusive porque, no modelo brasileiro, a inteligência de Estado opera somente diante de ameaças, reguladas pela ação de investigação criminal. Nesta, é substancial a existência de um fato criminoso originário, capaz de dar mobilidade aos legitimados do sistema para investigar e tomar as medidas cabíveis de modo a repreender práticas ilegais (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020). Nada obstante, resta a incógnita acerca da dimensão da atemorização que os cidadãos descritos no Dossiê possam oferecer ao Estado brasileiro.

Em decisão acertada, em agosto de 2020, o STF suspendeu, por medida cautelar, a continuidade do documento, nos termos do voto da Ministra Cármen Lúcia, transcrito abaixo:

[...] Suspender todo e qualquer ato do Ministério da Justiça e Segurança Pública de produção ou compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas, as práticas cívicas de cidadãos, servidores públicos federais, estaduais e municipais identificados como integrantes de movimento político antifascista, professores universitários e quaisquer outros que, atuando nos limites da legalidade, exerçam seus direitos de livremente expressar-se, reunir-se e associar-se [...]

Assentes aos votos do julgado, a escusa da finalidade de preservação da segurança pública e do serviço de inteligência estatal não pode, sob qualquer circunstância, mitigar os direitos de privacidade relativos aos dados pessoais de cada cidadão, sob pena de debilitar a sustentação republicana exaustivamente alcançada.

Outro ponto também questionável, situa-se no Decreto 9.662 de 2019 que dispõe das atribuições dadas à SEOPI, relativas ao assessoramento ao Ministério da Justiça, principalmente nas atividades de inteligência conxas ao setor público, além das investigações penais salutares. No entanto, não há qualquer limitação referente à obtenção e tratamento dos dados por ela colhidos, de modo que suas ações são regidas unicamente pelo livre arbítrio e pela conveniência do Ministério (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020).

Ocorre que, na LGPD, o tratamento e compartilhamento de dados pessoais devem ser geridos no intuito de uma finalidade legítima e específica, ao conhecimento do titular do dado - art. 9º, incisos I e V, da LGPD - de modo que, as autorizações genéricas sobre o consentimento de determinada finalidade serão consideradas nulas - art. 4º. Inclusive, a lei possui a finalidade como princípio próprio - art. 6º, inciso I - segundo o qual, a realização do tratamento deve respeitar propósitos legítimos, específicos, explícitos e informados ao titular, sem qualquer possibilidade de desvio na forma de seu tratamento.

Ainda, no mesmo termo legislativo, encontram-se os princípios da necessidade e da não incriminação que pugnam pela limitação do tratamento ao mínimo necessário para a realização de suas finalidades, dados proporcionais, pertinentes e não excessivos, bem como a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos, circunstâncias que pela notoriedade dos fatos, não foram observadas quando da criação da SEOPI.

Nesse mesmo norte, outro ponto diverso a ser ressaltado, centra-se no tratamento de dados pessoais pelas pessoas jurídicas de direito público - art. 23 - que deverá, no caso do Ministério da Justiça, ser realizado para o

atendimento de sua finalidade pública, ou, não enquadrando-se, recairá na exceção do art. 4º, inciso III. Por conseguinte, explora-se o vácuo legislativo de requisição de finalidade no tratamento de dados realizado pela SEOPI, haja vista todo o exposto, em que qualquer utilização carece de finalidade legítima.

Nada obstante, a inexistência de limitação legislativa no tratamento de dados pessoais pela Secretaria de Operações Integradas, vem a ser contraditória frente ao arcabouço de proteção instituído pela LGPD, uma vez que o dossiê produzido só fora possível graças à carência de desígnio legislativo, ferindo a própria razão do Estado Democrático de Direito.

2.4 DADOS PESSOAIS: O PETRÓLEO DO SÉCULO XXI

Voga-se à oração proferida pelo sábio professor israelense Yuval Noah Harari (2018, p. 10) "Algoritmos de Big Data poderiam criar ditaduras digitais nas quais todo o poder se concentra nas mãos de uma minúscula elite enquanto a maior parte das pessoas sofre não em virtude de exploração, mas de algo muito pior: irrelevância". Isto é, vislumbra-se que o aludido fito se situa no campo atemporal dos fatos, de modo que hodiernamente constitui uma pungente ferramenta da minoria.

Neste ínterim, vários são os acontecimentos que concretizam tal pensamento. Na China, o governo local implementou um projeto estatal para repreender e gratificar o comportamento de seus cidadãos, denominado de "sistema de crédito social". Transcendidos dois anos, em 2019, o departamento chinês já havia barrado 17,5 milhões de viagens de avião e 5,5 milhões, de trem (TRINDADE, 2018), com base nas notas instituídas pelo sistema de *score* social, realizado através da massiva coleta de dados pessoais sensíveis relacionado ao dia-a-dia dos chineses (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020).

De modo análogo, o sistema jurídico estadunidense instaurou nas cortes e tribunais o software *Correctional Offender Management Profilingfor Alternative Sanctions - Compas* - , responsável pela avaliação célere da

probabilidade de reincidência para fins de dosimetria da pena. O resultado é alcançado através de algoritmos que foram alimentados com dados da sociedade norte americana, de modo que, baseado em pesquisas da estrutura social, concluíram erroneamente que um negro não reincidente possui maior grau de risco social quando comparado a um branco reincidente (ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, 2020).

Outrossim, após a entrada em vigor da LGPD, a empresa PSafe anunciou o vazamento aproximado de cem milhões de contas de celulares, oportunidade em que o Departamento de Proteção e Defesa do Consumidor, da Secretaria Nacional do Consumidor, notificou as operadoras Claro, Oi, Tim e Vivo. Assentes ao relatório, ainda incerto, informações como valor da conta, minutos gastos por dia, número de celular, filiação, data de nascimento e CPF teriam sido vazadas na *deepweeb*, onde cada registro está sendo comercializado por um dólar, via *bitcoin* (GIMENEZ, 2021).

Destarte, nota-se que, além dos dados facilmente acessíveis, os setores econômicos, no intento de realizar a manutenção da comercialização da rede de dados, criaram os programas de fidelidade, em que cada compra é registrada no histórico da empresa adjunto dos dados convencionais e posteriormente comercializada como "ferramenta de garantia" a outros setores, dos quais, cita-se o aumento no plano de saúde, rejeição na entrevista de emprego, créditos bancários recusados, dentre outros inimagináveis.

Nesse diapasão, vislumbra-se a tese de Yuhal no que concerne à irrelevância dos indivíduos no modelo econômico de comercialização de dados pessoais que ora se impõe. A formação do perfil do indivíduo, baseada sobre seu consumo, leva a interpretações discriminatórias e a demasiada negligência dos direitos fundamentais constitucionais inerentes a qualquer relação, de modo que estes carecem do amparo ínfimo estatal.

Em suma, denota-se os malefícios ocasionados pela capitalização dos dados pessoais, como o mais novo petróleo hodierno, de tamanha força econômica capaz de criar ditaduras digitais ancoradas nos algoritmos como parâmetros de exclusão, ou, inclusão, privada e governamental, em

detrimento de todos os anos de constante luta pela privacidade e livre arbítrio próprios e singulares a cada cidadão.

2.5 PANÓPTICO ESTATAL DE DADOS

Assentes à ambiguidade estrutural consolidada nos órgãos regulatórios e no subterfúgio de "finalidade pública", evidencia-se o ábdito pensamento de Foucault - no que tange ao Panóptico, estrutura arquitetônica que concretiza a microfísica do poder em uma torre central, em que pese tenha sido criada em períodos longínquos, denota-se extremamente nupérrima.

Na estrutura, o vigilante não pode ser visto através das persianas, mas aufere da visibilidade de todos, onde a própria visibilidade é uma armadilha e a penalização é a docilização do corpo e da mente, de modo que as cicatrizes se situam na alma e na racionalidade.

Por sua vez, a sociedade atual e a sua relação com o Estado, regada pelos canais dos algoritmos, assemelha-se com o panóptico. Em que pese inexistir estrutura arquitetônica, persiste a digital. Enquanto o Estado, de dentro da torre, assiste e detém os dados, o sujeito "é visto, mas não vê; objeto de uma informação, nunca sujeito numa comunicação" (FOUCAULT, 1999, p. 224).

A posição de espectador do indivíduo frente ao monopólio estatal de dados, impede que este saiba a finalidade originária destinada aos seus dados pessoais. Nada sabe sobre como o instrumento funciona, tornando-se incognoscível aos seus olhos, situação que por si só viola e denigre o princípio da transparência, no qual há "Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível" (FOUCAULT, 1999, p. 224).

A constante visibilidade de dentro da torre favorece a ocorrência de ilícitos similares ao dossiê, criado pelo "vigilante" do departamento da SEOPI. A coleta massiva de dados pessoais sensíveis realizada outrora testemunha que essa instância é abstrata e completamente longínqua da lucidez dos indivíduos comuns, haja vista que estes são os verdadeiros detentores que

possuem a prerrogativa decisória de sua destinação. Portanto o Estado deve agir pautado nestes mesmos limites, constitucionais e legais, pois direitos fundamentais não são moldáveis pela conveniência do aparato governamental.

3 CONCLUSÃO

A sociedade digital trouxe consequências catastróficas, as quais incitaram o legislador a majorar a proteção de dados do titular. Todavia, os parlamentares falharam em dois aspectos: ao não estabelecer de imediato a criação da ANPD como agência reguladora autônoma da administração; e, ao não regular o tratamento de dados na segurança pública e investigação criminal. Esses aspectos deixam o titular dos dados desprotegido e à mercê de intromissões e até mesmo, de modo exagerado, mas não excludente, manipulação social, cultural, econômica e política.

Uma das possíveis soluções, além de garantir autonomia às agências reguladoras de proteção de dados pessoais, seria a criação de: dois bancos de dados de segurança máxima; e, duas instituições responsáveis por cada um desses bancos, as quais estariam vinculadas a suas respectivas agências fiscalizadoras, ou seja, uma para a ANPD e outra para a futura "LGPD Penal". As instituições armazenariam, nas suas competências, os dados imprescindíveis do titular, na forma de uma única chave criptografada, similar ao pix.

A chave criptografada poderia ser subdividida em três tipos de dados: pessoais, sensíveis e anonimizados. Ainda, poderia ser utilizada pelo titular, com comodidade e segurança, ao fazer um cadastro num estabelecimento físico ou digital, que fosse privado ou público, com fins econômicos ou não, pois não precisaria apresentar inúmeros documentos seguidos de cópias e tão pouco deixaria seus dados espalhados pelos diversos ambientes, físicos ou digitais, da sociedade.

O acesso aos bancos de dados seria condicionado a um cadastro nacional, no qual cada pessoa jurídica de direito privado ou público

especificaria a finalidade do tratamento de dados. Para a autorização do cadastro e do acesso, seria imprescindível a aprovação conjunta pela respectiva instituição de segurança máxima e pela autoridade nacional de proteção de dados.

Destarte, o titular dos dados estaria protegido contra abusos da iniciativa pública e privada; a segurança pública e investigação criminal respeitariam os direitos fundamentais, atuando dentro de procedimentos claros. Assim, ante estes dispositivos, seria possível assegurar a ínfima proteção dos dados pessoais e consequentemente a democracia brasileira seria preservada em toda sua magnitude, pois assentes a Ministra Cármen Lúcia "A República não admite catacumbas, a democracia não se compadece com segredos, a não ser para se lembrar de situações que precisamos ter como superadas".

REFERÊNCIAS

ARAS, Vladimir Barros et al (org.). PROTEÇÃO DE DADOS PESSOAIS E INVESTIGAÇÃO CRIMINAL: a título de introdução: segurança pública e investigações criminais na era da proteção de dados. A TÍTULO DE INTRODUÇÃO: SEGURANÇA PÚBLICA E INVESTIGAÇÕES CRIMINAIS NA ERA DA PROTEÇÃO DE DADOS. 2020. Disponível em: http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf. Acesso em: 01 maio 2021.

ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA. Proteção de dados pessoais e investigação criminal. Brasília: Anpr, 2020. 593 p.

ATHENIENSE, Alexandre. Impactos das mudanças na Lei de Proteção de Dados Pessoais. 2018. Disponível em: https://www.conjur.com.br/2018-dez-29/opiniao-impactos-mudancas-lei-protecao-dados-pessoais. Acesso em: 02 maio 2021.

BONFIM, Natália Bertolo. MP 869/18 e alterações na LGPD. 2019. Disponível em: https://www.migalhas.com.br/depeso/293658/mp-869-18-e-alteracoes-na-lgpd. Acesso em: 02 maio 2021.

BRASIL. Tribunal Pleno. Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 722 Distrito Federal nº 722, Processo Adpf 0098926-29.2020.1.00.0000 Df 0098926-29.2020.1.00.0000. Reqte. Rede Sustentabilidade.

Intdo. Ministro de Estado da Justiça e Segurança Pública. Relator: Ministra Cármen Lúcia. Brasília, DF, 20 de agosto de 2020. Diário Oficial da União. Brasília, . Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/1108681512/medida-cautelar-na-arguicao-de-descumprimento-de-preceito-fundamental-adpf-722-df-0098926-2920201000000. Acesso em: 03 maio 2021.

BRASIL. Decreto nº 9.662, de 1 de janeiro de 2019. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública, remaneja cargos em comissão e funções de confiança e transforma cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS.. : legislação federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9662.htm. Acesso em: 21 abr. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 maio 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). : legislação federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2021.

FIGUEIRA, Hana Mesquita Amaral. "LGPD penal", vigilantismo e o papel do CNJ como autoridade competente: considerações iniciais acerca do anteprojeto de lei. 2020. Disponível em: https://www.migalhas.com.br/depeso/337223/lgpd-penal---vigilantismo-e-o-papel-do-cnj-como-autoridade-competente--consideracoes-iniciais-acerca-do-anteprojeto-de-lei. Acesso em: 02 maio 2021.

FOUCAULT, Michel. Vigiar e Punir. 20. ed. Petrópolis: Vozes, 1999. 348 p. Tradução de Raquel Ramalhete.

GIMENES, Diego. Vazamento de dados: Claro, Oi, Tim e Vivo podem ser multadas em R$ 60 mi: operadoras são notificadas sobre o vazamento de 103 milhões de contas de celular e têm 15 dias para responder; irregularidades podem culminar em sanções. Operadoras são notificadas sobre o vazamento de 103 milhões de contas de celular e têm 15 dias para responder; irregularidades podem culminar em sanções. 2021. Disponível em: https://veja.abril.com.br/economia/vazamento-de-dados-claro-oi-tim-e-vivo-podem-ser-multadas-em-r-60-mi/. Acesso em: 01 maio 2021.

HARARI, Yuval Noah. 21 lições para o século 21. São Paulo: Schwarcz S.A, 2018. 314 p. Tradução de Paulo Geiger.

ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. 2019. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios. Acesso em: 01 maio 2021.

TRINDADE, Rodrigo. Grande Irmão: China proibiu 23 milhões de viagens de avião ou trem em 2018. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/03/grande-irmao-china-proibiu-23-milhoes-de-viagens-de-aviao-ou-trem-em-2018.htm. Acesso em: 30 abr. 2021.

VILHALBA, Sabela Moreira. Clipping Migalhas: O que muda com a sanção da lei geral de proteção de dados. 2018. Disponível em: http://www.saianiesaglietti.com.br/notcias-1/2018/9/28/o-que-muda-com-a-sano-da-lei-geral-de-proteo-de-dados. Acesso em: 02 maio 2021.

Sobre o(s) autor(es)
Alencar Barbieri. Acadêmico do Curso de Direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. E-mail: alencarbarbieri@hotmail.com

Marine Lauschner. Acadêmica do Curso de Direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. E-mail: marinelauschner@gmail.com

Rodrigo da Costa Morais. Acadêmico do Curso de Direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. E-mail: rodrigocmbe@gmail.com

Alexandra Vanessa Klein Perico. Mestre em Direito pela Universidade do Oeste de Santa Catarina (UNOESC) Chapecó, na área de concentração em Dimensões materiais e eficaciais dos Direitos Fundamentais, na linha de pesquisa de Direitos Fundamentais sociais: relações de trabalho e seguridade social. Pós-graduada em Direito e Processo do Trabalho Contemporâneo pela Universidade de Passo Fundo (UPF) e Universidade do Oeste de Santa Catarina (UNOESC). Graduada em Direito pela Universidade do Oeste de Santa Catarina (UNOESC); professora do Curso de Direito da Universidade do Oeste de Santa Catarina - UNOESC. E-mail: alexandra.perico@unoesc.edu.br