XXIII SEMEAD
Seminários em Administração

novembro de 2020
ISSN 2177-3866

O tratamento de dados pessoais por governos no combate à COVID-19 de acordo com a legislação do Brasil e do governo central da União Europeia

MARIANA LEITE FERNANDES DA SILVA
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO (FGV-EAESP)

O TRATAMENTO DE DADOS PESSOAIS NO COMBATE À COVID-19 DE ACORDO COM A LEGISLAÇÃO DO BRASIL E DO GOVERNO CENTRAL DA UNIÃO EUROPEIA

INTRODUÇÃO

A proteção de dados entrou na agenda pública a partir de eventos como a tentativa de unificação do armazenamento de dados pessoais norte-americanos, a partir do *National Data Center*, por volta de 1965. A ideia foi baseada em um projeto que propunha a unificação dos cadastros da previdência social, do Censo, do fisco e dos registros trabalhistas. A motivação para isso era trazer maior eficiência por parte do Estado, mas os cidadãos da época notaram que o custo seria a perda de privacidade. Com isso, foi estabelecido um receio generalizado quanto ao poder do governo, uma vez possuindo tais dados. (DONEDA, 2006, p. 187)

No processo, foi concluído que a disposição de informações pessoais em diversas fontes já não se tratava mais de uma regra, mas de uma opção, com pontos positivos e negativos. Além disso, concluiu-se que nem todos os dados pessoais possuem igual importância, o que traz implicações para a forma como eles devem ser protegidos. Ressalta-se que esse processo levou em conta a dignidade e a proteção da personalidade, mas não discutiu a regulação de dados pessoais sensíveis e nem como solucionar o embate entre a privacidade e a necessidade governamental de informações pessoais. (DONEDA, 2006, p. 188-190).

Um segundo caso em que foi pautada a proteção de dados devido a ações tomadas pelo Estado ocorreu na França, no início da década de 1970. Foi criado um instituto visando a facilitar a comunicação e o armazenamento de dados sobre os cidadãos dentro da administração pública. Este instituto criou o Sistema Automatizado para Arquivos Administrativos e Diretório dos Indivíduos, chamado de projeto SAFARI, que consistiria em transferir dados pessoais dos cidadãos para sistemas informatizados da administração pública.

A justificativa para isso era aumento na eficiência administrativa, mas o evento que causou seu encerramento foi que a ideia era baseada em um projeto com pretensões discriminatórias. Após o ocorrido, criou-se uma comissão que elaborou a lei nacional de proteção de dados de 1978. (DONEDA, 2006, p. 190-191)

Na Alemanha, destaca-se um caso que ocorreu no início da década de 1980, portanto, em um momento em que já havia uma cultura de proteção de dados, tendo em vista que a primeira lei sobre a matéria é alemã e que havia uma lei federal de proteção de dados pessoais desde 1977. Nesse contexto, um conflito se iniciou à medida que diferentes setores da sociedade passaram a questionar o censo a ser finalizado em 1983, devido à forma de coleta de informações e ao destino delas (DONEDA, 2006, p.192).

Este caso foi levado à Corte Constitucional Alemã, que averiguou que o problema estava na lei que organizava o censo, aprovada em 1982. Isto porque a lei possibilitava que os dados coletados pelo censo fossem confrontados com os dados do registro civil; que estes mesmos dados, desde que sem identificar o nome do titular fossem transmitidos às autoridades federais; e que fossem multados aqueles que não respondessem e que fossem favorecidos os que denunciassem tais pessoas.

Devido ao fato de que a lei em vigor não fornecia garantias suficientes, a Corte Constitucional declarou esta lei inconstitucional. Uma das justificativas foi que, no caso de utilização dos dados para fins estatísticos e administrativos, haveria a diversidade de finalidades, de forma que não seria possível para o cidadão reconhecer o uso efetivo que seria

feito das suas informações. Portanto, a decisão reconheceu a necessidade de observar o princípio da finalidade desde o momento da coleta de dados pessoais.

Vale destacar que esta sentença utilizou a expressão "autodeterminação informativa" como o direito dos indivíduos de “decidirem por si próprios quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2006, p. 196), elemento já presente na doutrina norte-americana da década de 1970. Ainda, a discussão não abordou apenas a natureza dos dados pessoais, mas também a sua necessidade e utilização como fatores relevantes para a privacidade. O desfecho do caso foi a elaboração de uma nova lei que corrigiu as questões controversas e foi promulgada em 1985, prevendo um novo censo para 1987.

A doença: COVID-19

A doença COVID-19 é causada pelo vírus SARS-CoV-2. Esta possui em seu nome o numeral "19" devido à data do primeiro alerta da OMS para a doença, em 31 de dezembro de 2019 (MINISTÉRIO DA SAÚDE, [2020]). Quanto à sua procedência, o vírus SARS-CoV-2 é origem da seleção natural, conclusão tirada da análise do genoma do vírus, segundo a revista acadêmica Nature Medicine, no artigo The proximal origin of SARS-CoV-2. Assim, descarta-se a possibilidade do vírus ter sido criado em laboratório (ANDERSEN et al, 2020, p. 452).

Além disso, o quadro clínico da doença varia de infecções assintomáticas a quadros respiratórios graves. Isso significa que nem todos os infectados apresentam sintomas, mas todos os infectados podem transmitir a doença. Além desse fator, devido ao fácil contágio, o sistema de saúde pode ficar sobrecarregado, não garantindo o atendimento a todos os que necessitam dele. Sendo assim, o isolamento social horizontal foi adotado por diversos países, visando ao achatamento da curva de contágio para que o sistema de saúde não entre em colapso.

Destaca-se que escolher o isolamento vertical significaria atrasar e não prevenir o contágio de pessoas do grupo de risco de desenvolver um quadro mais grave de COVID-19, pois isso não evita completamente o contato entre pessoas do grupo de risco e portadores do vírus. Isso porque é possível que pessoas fora do grupo de risco contraiam a doença e contaminem pessoas do grupo de risco, caso morem na mesma residência, por exemplo.

Dados pessoais e o ciclo de políticas públicas

No ciclo de políticas públicas, dados pessoais são tratados nas etapas de diagnóstico, formulação e avaliação da política pública. No momento de diagnóstico, os dados compõem indicadores sociais, que mapeiam a realidade social, tornando uma dimensão de interesse da ação pública simplificada e padronizada. (JANNUZZI, 2009, p.13). Com isso, há delimitação do alvo da política pública. Na formulação, estes mesmos indicadores sociais integram um cruzamento de dados para fornecer uma avaliação preliminar de sua viabilidade. Na avaliação da política, por sua vez, os dados passam a incorporar os indicadores de monitoramento da ação governamental, cuja função é o registro das ações do governo e a mensuração de esforços e efeitos (JANNUZZI, 2009, p.30).

No contexto de COVID-19, há urgência na execução do ciclo de políticas públicas, de forma que a coleta e o tratamento de dados são demandados em grande volume e com constantes atualizações. Isso se deve à rápida transmissão da doença e à sua letalidade.

Apesar disso, destaca-se que a legislação que deve ser respeitada mesmo quando há caráter de urgência, inclusive quanto à saúde pública.

PROBLEMA DE PESQUISA E OBJETIVO

Como problema de pesquisa, foi questionado: "de que legislação o governo brasileiro e o governo central da União Europeia dispõem para o tratamento de dados pessoais no combate à COVID-19?".

Como objetivo geral, visa-se a mapear a legislação brasileira e do governo central da União Europeia que seja aplicável ao tratamento de dados pessoais por governos no combate à COVID-19. Como objetivos específicos, por sua vez, busca-se (i) compreender o papel da LGPD em *vacatio legis* no cenário da crise de COVID-19 e (ii) apresentar os usos de dados respaldados por lei em cada governo.

FUNDAMENTAÇÃO TEÓRICA

Para compreender de que legislação o governo brasileiro e o governo central da União Europeia dispõem para o tratamento de dados pessoais no combate à COVID-19, serão abordados elementos constitucionais e infraconstitucionais. Acerca da legislação brasileira, serão discutidas a LGPD, a Constituição Federal do Brasil; o Decreto nº 7.724/2012, que regulamenta a LAI; o Decreto nº 10.046/2019, que aborda a governança de dados; o Marco Civil da Internet (MCI), que apresenta alguns princípios já em vigência para o tratamento de dados pessoais; o Código Civil; e o Código de Defesa do Consumidor, sendo que os três últimos abordam a responsabilidade civil. Já acerca da legislação do governo central da União Europeia, será abordado o *General Data Protection Regulation* (GDPR).

A vigência da LGPD, até o momento de confecção deste artigo, está prevista para maio de 2021, com exceção de suas sanções administrativas, conforme a Medida Provisória nº 959/2020. A aplicação de sanções administrativas, por sua vez, passa a valer a partir de agosto de 2021.

A temática na Constituição Federal

Na Constituição Federal, são assegurados direitos fundamentais pelo Artigo 5º. Quanto aos direitos fundamentais relativos à proteção de dados, a Constituição disciplina que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988, art. 5º, X)

No caso de um tratamento desarrazoado de dados pessoais, um mecanismo de responsabilização civil previsto pela Constituição é o mandado de segurança. Este tem como finalidade: "proteger direito líquido e certo, não amparado por habeas corpus ou habeas data, quando o responsável pela ilegalidade ou abuso de poder for autoridade pública ou agente de pessoa jurídica no exercício de atribuições do Poder Público "(BRASIL, 1988, art. 5º, LXIX).

Princípios a serem seguidos

Para discutir a legislação, é necessário ter em mente seus princípios. Com a situação de *vacatio legis* da LGPD, o quadro a seguir apresenta os princípios para o tratamento de

dados pessoais já vigentes no Brasil devido ao MCI, os princípios que passarão a ser vigentes uma vez que a LGPD entre em vigor e os princípios vigentes na União Europeia devido ao GDPR.

Quadro 1. Princípios Previstos em Lei para o Tratamento de Dados Pessoais no Brasil e na União Europeia

MCI (Brasil)	LGPD (Brasil)	GDPR (UE)
Proteção à privacidade	Adequação	Adequação e Limitação da Finalidade
Finalidade	Finalidade	Limitação da conservação
Transparência	Transparência	Licitude, Lealdade e Transparência
Finalidades que não sejam vedadas pela legislação	Necessidade	Necessidade ou Minimização
Proteção de dados pessoais na forma da lei	Qualidade dos dados	Qualidade dos dados ou Exatidão
–	Segurança	Segurança, Integridade e Confidencialidade
–	Responsabilização e prestação de contas	Prestação de contas ou Responsabilização
–	Livre acesso	–
–	Não discriminação	–
–	Prevenção	–

Fonte: compilado pela autora

Além disso, há mais direitos garantidos pela legislação vigente no momento de escrita deste artigo. O direito à exclusão já consta no MCI, assim como o direito ao "não fornecimento a terceiros de seus dados pessoais (...), salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei." (BRASIL, 2014, art. 7º, VII)

Consentimento

Quanto ao consentimento, há a hipótese prevista no Decreto nº 7.724/2012, em que o consentimento pode não se exigido. As situações em que isso se verifica constam no Artigo 57 do Decreto, que determina que o consentimento não será exigido caso o acesso à informação seja necessário "à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, vedada a identificação da pessoa a que a informação se referir" (BRASIL, 2012, art. 57, II), ou "à proteção do interesse público geral e preponderante" (BRASIL, 2012, art. 57, V), sendo o segundo caso o mais relevante para a situação de tratamento de dados pessoais por governos no combate à COVID-19.

Além disso, o MCI afirma, em seu Artigo 24, que todos os entes federativos devem atuar no desenvolvimento da internet no Brasil, de modo a respeitar diretrizes como o "estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica" (BRASIL, 2014, art. 24, I). Sendo assim, o MCI abordou em termos gerais a temática de governança de dados, o que se refletiu no Decreto n° 10.046/2019, que dispõe sobre a governança no compartilhamento de dados dentro da Administração Pública Federal, entre outros temas.

Neste Decreto, o compartilhamento de dados entre órgãos e entidades da administração pública federal direta, autárquica e fundacional e demais poderes da União, estabelecem-se normas e diretrizes com finalidades dentre as quais está "promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal" (BRASIL, 2019, art. 1º, IV). Esta finalidade demonstra que há disposições legais que visam a garantir a qualidade dos dados, que se consolida como princípio na LGPD.

Governança de dados

Quanto à governança de dados, o Decreto traz como diretriz: "a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações" (BRASIL, 2019, art. 3º, I). Ainda, destaca-se a necessidade de dados pessoais no ciclo de políticas públicas, presente no seguinte fragmento do Decreto em questão: "os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades (...), para facilitar a execução de políticas públicas orientadas por dados;" (BRASIL, 2019, art. 3º, III).

Instrumentos de responsabilização civil

O MCI prevê a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2014, art. 7º, I). Isso se trata da responsabilização civil, que, portanto, já vigente antes da LGPD. Este tipo de responsabilização se concretiza a partir do disposto no Código Civil e no Código de Defesa do Consumidor.

O Código Civil é um mecanismo de responsabilização civil que pode ser acionado na relação entre o Estado e o cidadão ou nas relações entre empresas e o cidadão que não são mediadas pelo consumo, sendo relevante, para este artigo, apenas o primeiro caso. Para que ocorra a responsabilização civil, é necessário que haja a judicialização da questão, tal como previsto no Código Civil: "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar

ato contrário a esta norma" (BRASIL, 2002, art. 21, caput). Nesse sentido, "pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei." (BRASIL, 2002, art. 12, caput)

Ademais, o Código Civil dispõe que causar danos a outrem, mesmo que morais, é um ato ilícito, conforme o trecho: "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (BRASIL, 2002, art. 186, caput). Ainda, a reparação destes danos é obrigatória independentemente da culpa, conforme previsto em lei ou quando a atividade normalmente desenvolvida por quem causou dano oferecer, por sua natureza, risco aos direitos de outrem (BRASIL, 2002).

Já o Código de Defesa do Consumidor é um mecanismo de responsabilização civil acionável em relações de consumo entre empresas e o cidadão. Nesse sentido, ele será abordado porque os dados pessoais obtidos pelo governo para o tratamento no combate à COVID-19 podem não ter sido por ele coletados, de forma que, caso as empresas não compartilhem dados anonimizados, elas estarão sujeitas à responsabilização, caso cometam as infrações descritas no Código de Defesa do Consumidor.

O destaque para o que o Código de Defesa do Consumidor disciplina vai no sentido dos direitos básicos do consumidor: "a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos" (BRASIL, 1990, art. 6º, I). Para cumprir isso, o Artigo 8º disciplina que "os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito" (BRASIL, 1990, art. 8º, caput).

Ainda, a reparação dos danos causados ao consumidor independe da existência de culpa, uma vez que houve defeitos no projeto, na fabricação, construção, manipulação, apresentação ou acondicionamento dos produtos oferecidos ou defeitos devido ao provimento de informações insuficientes ou inadequadas em relação à utilização do produto ou aos riscos que ele oferece (BRASIL, 1990, art. 12, caput). Nesse sentido, um produto defeituoso é aquele que não oferece a segurança legitimamente esperada, considerando "o uso e os riscos que razoavelmente dele se esperam" (BRASIL, 1990, art. 12, § 1°)

Os dados pessoais úteis no combate à COVID-19

Para esta discussão, cabe discriminar os dados que possuem papel relevante no combate à COVID-19 por parte dos governos. Estes dados são, principalmente, dados de geolocalização de indivíduos, para comprender onde há concentração de suspeitas, casos e mortes por COVID-19 e os dados de indivíduos em relação a sintomas, internações, óbitos e afins. Sendo assim, são apresentadas as definições de dado pessoal, dado pessoal sensível e dados relativos à saúde.

A definição que consta no GDPR acerca de dado pessoal é "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)" (UNIÃO EUROPEIA, 2016, art. 4º, 1). Já na LGPD, dado pessoal é definido como
"informação relacionada a pessoa natural identificada ou identificável." (BRASIL, 2018, art. 5º, I).

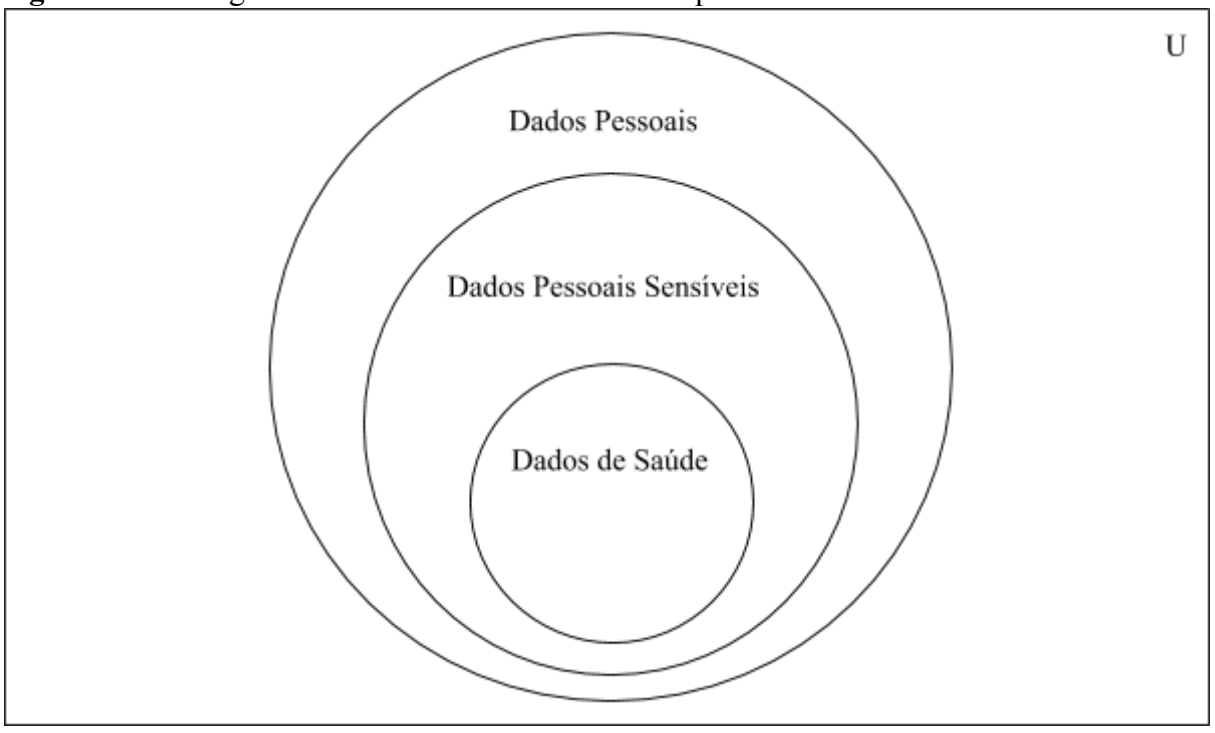
Na LGPD, dado pessoal sensível é definido como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de

caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018, art. 5º, II). No GDPR, dado pessoal sensível é o dado que deve ser inserido em um regime de proteção específica, dada sua natureza especialmente snesível quanto a direitos e liberdades fundamentais porque "contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais" (UNIÃO EUROPEIA, 2016, considerando 51). Destaca-se que o dado pessoal sensível pertence a uma categoria especial de dados, de forma que lhe é conferido um regime especial.

Na LGPD, não consta definição de dados relativos à saúde. Já no GDPR, dados relativos à saúde são definidos como "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (UNIÃO EUROPEIA, 2016, art. 4º, 15).

Para compreender como as definições se relacionam entre si, foi elaborada a Figura 1, que ressalta que dados relativos à saúde são dados pessoais sensíveis, mas não são o único tipo de dados pessoais sensíveis.

Figura 1. Diagrama de Venn sobre os Tipos de Dado Pessoal Abordados



Fonte: compilado pela autora

As bases legais aplicáveis no caso da COVID-19

Para tratar dados pessoais, é necessário que seja apresentada uma base legal que justifique o tratamento. No contexto de tratamento de dados por governos no combate à COVID-19, as bases legais que podem justificar este tratamento estão dispostas no quadro a seguir:

Quadro 2. Bases Legais que Justificam o Tratamento de Dados por Governos no Combate à COVID-19 por cada Governo Estudado

LGPD (Brasil)	GDPR (UE)
Consentimento	Consentimento
Obrigação legal	Interesse público
Implementação de políticas públicas pela Administração Pública	–
Pesquisa por entidades públicas de estudo	–

Fonte: compilado pela autora

Destaca-se que o Artigo 57 do Decreto nº 7.724/2012 disciplina que não há exigência de consentimento, caso o acesso à informação seja necessário para estatísticas e pesquisas científicas de interesse público ou geral, conforme a lei, vedada a identificação do titular dos dados; ou para a proteção do interesse público ou geral. Sendo assim, a LGPD não apresenta o interesse público como base legal propriamente dita, tal como o GDPR faz, ressaltando que a base legal de interesse público não exige consentimento, mas o interesse público pode ser utilizado como justificativa para a coleta, o tratamento e o não apagamento de dados pessoais sem consentimento.

Com isso, estabelece-se um *trade-off*, em que se escolhe priorizar o interesse público ou as garantias individuais. Vale destacar que a priorização de um dos lados não significa que o outro lado está completamente anulado. Nesse sentido, percebe-se que o interesse público e as garantias individuais não se relacionam a partir de uma hierarquia fixa, portanto, cada caso deve ser avaliado em particular.

Na União Europeia, as garantias aos cidadãos a partir dos princípios, das bases legais e de artigos específicos para cada situação obrigam o governo, no caso em questão, a deixar claro como será o tratamento de dados, qual sua finalidade, sua extensão, sua necessidade e a forma como ocorrerá. Com isso, o interesse público prevalece, mas sem que isso cause danos à proteção dos dados dos usuários, devido às garantias estabelecidas pela legislação.

Já no Brasil, como a LGPD não está em vigor, não há uma proteção de dados tão minuciosa como na União Europeia. Dessa forma, o tratamento de dados pessoais devido ao interesse público pode ocorrer, porém é necessário comprovar o interesse público, no caso de seu questionamento, e também é necessário explicitar sua finalidade, ser transparente quanto à extensão do tratamento e enquadrar o tratamento na forma da lei, tal como prevê o MCI. Caso essas informações não estejam claras, o tratamento de dados não ocorrerá.

Assim, nota-se que o Estado permitir o uso de dados pessoais sem consentimento à medida que legisla em favor do cidadão é uma forma de garantir que o interesse público prevaleça apenas se o cidadão estiver protegido pela lei quanto ao tratamento destes dados. Mas o Estado não permitir ou permitir em raras situações o uso de dados sem consentimento

porque não há legislação vigente em favor do cidadão no caso em questão também é proteger o cidadão.

DISCUSSÃO

Optou-se por também discutir a LGPD, mesmo esta não sendo vigente no momento de escrita deste artigo. Isso porque a LGPD é uma legislação brasileira aprovada e alinhada aos padrões internacionais de melhores práticas, em termos de privacidade e proteção de dados pessoais. Nesse sentido, a LGPD segue o paradigma inaugurado pelo GDPR, que retira o titular de dados de uma situação de hipossuficiência por vias de privilegiar a autodeterminação informativa.

Além disso, o Estado adotar a LGPD como lei de referência significa que quando a LGPD entrar em vigor, haverá disponível aos controladores um inventário dos dados que foram tratados até aquele momento, portanto pode haver referência de acordo com as melhores práticas internalizadas pela LGPD, ou não. Caso o inventário de dados não esteja de acordo com a LGPD, serão necessários ajustes, uma vez a LGPD em vigência, para que o Estado não incorra em uma infração.

Ademais, a aplicação de leis já existentes como a Constituição, o MCI, o Código Civil e o Código de Defesa do Consumidor já está de acordo com os princípios que constam na LGPD. A LGPD também vem sendo citada em preceitos, doutrinas e jurisprudências e também, de modo formal, na MP nº 954/2020, que faz referência a artigos da LGPD, utilizando-se de seus dispositivos.

Ainda, o Supremo Tribunal Federal também leva em conta direitos relacionados à proteção de dados em suas decisões, direitos estes cuja tendência é serem ponderados por câmbios interpretativos e tendências doutrinárias típicos da proteção de dados pessoais. Portanto, a LGPD se faz influente em decisões tomadas mesmo antes da sua vigência, dada uma cultura de proteção de dados, em certa medida, já existente.

Responsabilização civil e responsabilização administrativa

A responsabilização civil é consolidada no Brasil pelos mecanismos presentes no MCI, no Código Civil, no Código de Defesa do Consumidor e na Constituição Federal do Brasil, mas não é vigente uma base de responsabilização administrativa até agosto de 2021. Assim, há mecanismos consolidados no direito brasileiro para mitigar os riscos desta envergadura constitucional, mas isto não é suficiente devido à falta de uma autoridade nacional e de regulamentação dos dispositivos que contam na LGPD. Isso torna a situação desprovida de segurança, pois não se sabe se os dados serão utilizados em conformidade com as melhores práticas, de acordo com Ana Frazão. (FGV, 2020)

Vale destacar que independentemente da LGPD estar em vigor, o sistema de responsabilização civil pode ser acionado em grande escala, mas não há responsabilização administrativa até que as sanções da LGPD entrem em vigor, em agosto de 2021. Na União Europeia, por sua vez, ambas responsabilizações civil e administrativa podem ser acionadas em acordo com o GDPR.

Como a legislação guia o tratamento de dados pessoais no combate à COVID-19

Para além dos princípios presentes na legislação dos governos estudados, dos mecanismos de responsabilização civil no Brasil e de responsabilização civil e administrativa na União Europeia, o combate à COVID-19 ainda deve cumprir com alguns procedimentos, cujo objetivo é fornecer garantias aos indivíduos que têm seus dados pessoais tratados. Porém, há a ressalva de que a legislação de referência do Brasil é a LGPD, mas ela não está em vigência no momento de escrita deste artigo. Ainda, como o GDPR foi o paradigma para a elaboração da LGPD, há muitas semelhanças em relação aos procedimentos obrigatórios para o tratamento, buscando garantir a segurança do titular de dados.

A anonimização é um procedimento que remove o caráter identificável de um dado pessoal, portanto elimina a identificação do titular e também formas de identificá-lo. Para que o processo de anonimização seja considerado e, portanto, o objeto tenha se transformado de modo a não ser mais um dado pessoal, o processo deve acontecer de forma que, para sua reversão, esforços razoáveis precisem ser colocados. Isto é estabelecido tanto na LGPD, quanto no GDPR – embora as definições de esforços razoáveis em cada uma seja diferente – e, há diretrizes de responsabilização civil na legislação brasileira vigente para o caso da anonimização ser revertida e isso gere riscos ou cause danos ao titular de dados.

Além disso, está previsto em ambas as leis de referência estudadas o apagamento dos dados uma vez cessada a finalidade, quando há violação da legislação, quando os dados deixaram de ser necessários ou pertinentes à finalidade ou quando o titular revoga seu consentimento – resguardado o interesse público. Com isso, observa-se que estas leis priorizam que a conservação dos dados pessoais ocorra pelo menor prazo possível. Na legislação vigente no Brasil, por sua vez, também estão presentes estas mesmas justificativas para o apagamento, no MCI.

Destaca-se que tanto as legislações brasileiras, quanto o GDPR observam que os dados pessoais ser tratados com outra finalidade para além da coletada, o que, significaria o tratamento de dados para uma finalidade para a qual não foi fornecido o consentimento do titular de dados, o que, no caso da COVID-19, justifica-se pelo interesse público. Nesse sentido, destaca-se que em todas as situações abordadas – baseando-se apenas na legislação brasileira vigente, tendo a LGPD como modelo e com o GDPR–, o interesse público pode ser justificativa para o tratamento de dados pessoais sem o consentimento do titular. Esse tipo de tratamento de dados deve seguir medidas específicas e adequadas, para garantir os direitos e liberdades do titular de dados pessoais. Assim, LGPD e o GDPR, com sua vigência, reiteram o direito à autodeterminação informativa.

Em caso de tratamento de dados sem consentimento sob justificativa do interesse público, ainda há transparência em relação à finalidade, à extensão do tratamento, entre outras informações e o apagamento é garantido, uma vez extinta a finalidade do tratamento. Ademais, os dados pessoais não podem ser compartilhados com terceiros pelo controlador sem o consentimento do titular, resguardado o interesse público, situação em que ainda deve haver notificação do titular de dados, para respeitar o princípio da transparência em todas as situações estudadas.

CONCLUSÃO

Tendo em vista a legislação de que o governo brasileiro e o governo central da União Europeia dispõem para o tratamento de dados pessoais no combate à COVID-19, nota-se que a administração pública e o direito representam diferentes pontos de vista em relação ao uso de dados pessoais por governos. A administração pública historicamente visa à eficiência e,

na discussão especificamente sobre a COVID-19 como uma questão de saúde pública, a administração visa ao interesse público. Enquanto isso, o direito busca fornecer garantias individuais e estabelecer o que são meios legais para atingir o interesse público.

Nesse embate, percebe-se que nenhum dos lados pode ser escolhido completamente, em detrimento do outro. Isso porque visar apenas à eficiência e ao interesse público pode causar danos aos indivíduos em diversas esferas, que deverão ser reparados e terá de ser feito um retrabalho, nesse sentido. Ao mesmo tempo, caso o Estado não regule a necessidade de dados por governos, a gestão pública não poderá atuar em diversas áreas até que haja uma legislação completa sobre a temática e inclusive sobre proteção de dados devido à necessidade de dados para o ciclo de políticas públicas e, no caso estudado, isso significaria um combate muito mais lento à COVID-19, que é uma questão urgente, envolvendo o direito à saúde e o direito à vida.

Sendo assim, os três poderes se regulam de modo a buscar a medida exata em que as garantias individuais e o interesse público dialogam e protegem tanto a esfera individual, quanto a coletiva, de forma que o Estado possa extrair benefícios disso. Nesse sentido, não haveria uma morosidade na gestão como um todo porque, se necessário, casos podem ser avaliados separadamente e também é evitado um retrabalho, no caso de ameaça aos direitos individuais, a partir da definição de leis.

IMPACTO

As informações discutidas apresentam as leis a serem seguidas, no Brasil, tanto apenas de acordo com a legislação vigente, quanto na situação dos tomadores de decisão do governo decidirem se equiparar às melhores práticas – portanto, seguindo a LGPD –, tornando suas atitudes parte de um inventário de acordo com a legislação de referência, garantindo maior segurança e segurança jurídica, tal como ocorre na União Europeia com o GDPR. Com isso, a utilização de dados pessoais no combate à COVID-19, em ambos os casos, fomenta o ciclo de políticas públicas a partir da construção de indicadores sociais e indicadores do monitoramento da ação governamental, facilitando, assim, o gerenciamento da crise resultante da pandemia. Isso porque a coleta e o tratamento de dados ocorre de maneira mais assertiva e precisa, tendo a legislação em observância, portanto evitando retrabalhos e responsabilização. Sendo assim, observar a legislação a ser seguida no tratamento de dados pessoais por governos no combate à COVID-19 significa mais eficiência nos processos que envolvem o ciclo de políticas públicas, e também oferece garantias individuais em todo o tratamento de dados pessoais.

Portanto, adquirir dados pessoais em conformidade com a legislação para nutrir o ciclo de políticas públicas significa prover informações para que seja estabelecido com precisão um foco de ação, pois a formulação da política pública depende de seu diagnóstico, que, por sua vez, depende de indicadores consolidados e testados para elaborar uma resposta ao problema. Estes dados também impactam a implementação, direcionando respostas de acordo com a diversidade de problemas. Na etapa de avaliação e monitoramento, por sua vez, os dados conferem mais segurança ao conjunto de decisões de combate à COVID-19, como a necessidade de ampliar ou diminuir o número de hospitais de campanha, mudança de fase no plano de saída do isolamento social e retorno seguro à normalidade. Assim, os dados são essenciais ao ciclo de políticas públicas, que deve buscar não apenas a eficiência e o interesse público, mas também respeitar a lei, que, neste caso, faz o contraponto das garantias individuais a serem respeitadas no processo.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSEN, K. et al. **The proximal origin of SARS-CoV-2.** Nature Medicine. Vol. 26. Abril 2020. P. 450-455. Disponível em <https://www.nature.com/articles/s41591-020-0820-9.pdf> Acesso em 20 abril 2020.

DONEDA, D. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

FGV. **Webinar | Impacto da COVID-19 na LGPD: desafios regulatórios e à proteção de dados.** YouTube. 14 de maio de 2020. Disponível em <https://www.youtube.com/watch?v=IKPv5-8PxmE&feature=youtu.be> Acesso em 14 maio 2020.

JANNUZZI, P. de M. **Formulação e Avaliação de Políticas Públicas: conceitos, técnicas e indicadores.** IV Seminário de Políticas Culturais: Reflexões e Ações. Rio de Janeiro. 23 a 25 de novembro de 2009. Disponível em <http://www.casaruibarbosa.gov.br/dados/DOC/palestras/Politicas_Culturais/IV_Seminario_Reflexoes_e_acoes/FCRB_Formulacao_e_Avaliacao_de_Politicas_Publicas_Conceitos_tecnicas_e_indicadores.pdf> Acesso em 08 maio 2020.

MINISTÉRIO DA SAÚDE. **Coronavírus (COVID-19). Sobre a doença.** Portal Ministério da Saúde. [2020]. Disponível em <https://coronavirus.saude.gov.br/sobre-a-doenca#sintomas> Acesso em 19 abril 2020.