Artigo
“Novos rumos da advocacia no pós-pandemia”

LGPD e o tratamento de dados pessoais pelo Poder Público

Autor: William Lima Rocha ([*])

RESUMO: O presente artigo visa analisar as bases legais para o tratamento de dados pessoais pelo poder público na Lei Geral de Proteção de Dados brasileira (LGPD – Lei n. 13.709/18). A LGPD e o tratamento de dados pelo poder público: trataremos hipóteses, requisitos, responsabilidades e restrições. Seguindo a temática “Novos rumos da advocacia no pós-pandemia” e diante da necessidade, como regra, de se enquadrar todo tratamento de dados em uma base legal determinada. É preciso compreender que o compartilhamento de dados deve ser verificado à luz das Políticas Públicas e finalidades institucionais dos receptores do envio de dados pessoais, com vistas ao cumprimento da LGPD. Resta claro que além da privacidade, a LGPD busca resguardar o compartilhamento ou acesso de dados e vinculá-lo às suas finalidades (art. 6º, incs. I, II e III, LGPD),

PALAVRAS-CHAVE: Dados pessoais; tratamento de dados; poder público; bases legais.

Introdução

Matéria de Direito Civil e previsão constitucional, a proteção de dados pessoais pode ser interpretada como um desdobramento do direito fundamental à privacidade, protegido pela Constituição Federal de 1988 (CF)[2], em seu artigo 5º, inciso X, que prevê que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Competência para legislar sobre proteção de dados pessoais, cabe à União legislar sobre Direito Civil. “art. 22, inciso I da Constituição da República”.

Esse direito também está garantido pelo art. 21 do Código Civil[3], que prevê que “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”.

Em matéria de competência legislativa, rege o princípio da predominância do interesse, “segundo o qual à União caberá aquelas matérias e questões de predominante interesse geral, nacional, ao passo que aos Estados tocarão as matérias e assuntos de predominante interesse regional, e aos Municípios concernem os assuntos de interesse local” No caso dos Municípios, a aplicação desse princípio está expressamente consagrada na Constituição Federal, na regra geral contida no artigo 30, I.

Ao se fazer uma análise das competências constitucionais, podemos observar a seguinte divisão: competência exclusiva, privativa, concorrente, suplementar, comum, cumulativa,

residual e remanescente. Em um primeiro momento, as palavras “exclusiva” e “privativa” parecem significar a mesma coisa, entretanto, competência exclusiva da União é aquela que não pode ser delegada, enquanto a privativa é delegável a outros entes.

Dessa forma, verificamos que o artigo 21 da CF prevê as competências exclusivas da União, ou seja, aquelas que não poderão ser delegadas por esta. Já no artigo 22, temos elencadas as matérias de competência privativa da União, ou seja, aquelas que a União poderá delegar aos Estados e Municípios, através de Lei Complementar, para que esses entes criem leis específicas.

A Constituição Federal em seu artigo 22, inciso I, determina que é competência privativa da União Federal legislar sobre Direito Civil. Considerando que a proteção de dados pessoais está abrangida pela noção de privacidade e consequentemente pelo Direito Civil, chegaríamos à conclusão inicial de que os estados e municípios só poderiam legislar sobre o tema, caso a União delegasse expressamente, através de Lei Complementar.

Porém, está tramitando no Congresso Nacional um Projeto de Emenda Constitucional (PEC) de nº 17[4] de 2019 que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. A proposta também fixa competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais.

A PEC 17/19 dá nova redação ao artigo 5º da Constituição Federal. O texto inicial acrescenta ao dispositivo o inciso XII-A, estabelecendo que “é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais”.

Há também o objetivo inserir a proteção de dados pessoais como direito fundamental do cidadão, bem como fixar a competência privativa expressa da União para legislar a matéria, ou seja, incluindo um inciso no artigo 22 da CF, de modo a não deixar dúvidas de que a proteção de dados pessoais será de competência privativa da União, não sendo exclusiva.

Caso a PEC seja aprovada, os estados e municípios poderão legislar sobre o tema proteção de dados pessoais, desde que a União delegue essa competência, através de Lei complementar.

Cumpre informar também, com a edição da Lei 13.709, em 14/08/2018, a chamada LGPD[5] - Lei Geral de Proteção de Dados Pessoais –, o Brasil passou a ter sua própria lei de proteção dos dados pessoais[6]. Deve-se destacar que o texto original da LGPD teve alguns dispositivos modificados pela Lei 13.853/2019, especialmente no tocante à constituição e ao funcionamento da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade[7].

Além disso, a LGPD tem capítulo específico sobre o tratamento de dados pelo Poder Público, no qual explicita sua aplicabilidade a todos os entes da administração direta e indireta da União, dos Estados, dos Municípios e do Distrito Federal, inclusive suas Cortes de Contas, Ministérios Públicos e entidades privadas sem fins lucrativos que recebam recursos públicos.

1.1 - Origem das definições da privacidade e dos dados pessoais:

O conceito de dados pessoais surgiu com a Internet, auto-determinação na sociedade da informação (jurisp. Alemanha) vindo a exigir a transparência sobre coleta, finalidades, utilização, direito de acesso, retificação.

Na União Européia: pessoa identificada ou identificável, direta ou indiretamente por meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa (ex. nome, número de identificação, dados de localização, elementos específicos próprios à sua identidade física, fisiológica, genética, psíquica, econômica, cultural ou social) (correlações)

Nos Estados Unidos: consumer centered, 'personally identifiable information' (varia segundo o setor, o Estado. ex. na legislação bancária, informação pública é excluída) decorre de tradição cultural diferente.

Qual o conceito de dado pessoal? A LGPD traz um conceito bem abrangente de dado pessoal, definindo-o como toda informação relacionada a pessoa natural (pessoa física) identificada ou identificável.

São exemplos de dados pessoais: nome, CPF, RG, filiação, e-mail, endereço, data de nascimento, hábitos de consumo, geolocalização, identificadores eletrônicos, entre outros.

Quem é o titular dos dados pessoais? O titular dos dados pessoais é a pessoa natural (pessoa física) a quem se referem os dados pessoais que são objetos de tratamento.

O respeito à vida privada é essencial para a liberdade e a felicidade individuais e o funcionamento democrático da sociedade. Necessário liberar o indivíduo dos imperativos comerciais (profiling do consumidor) e dos imperativos institucionais (profiling do "dissidente" que contesta a ordem estabelecida) => espaço para respirar e ser criativo.

Necessária para salvaguardar interesses importantes numa sociedade democrática ou outros direitos fundamentais (ex. segurança pública, liberdade de expressão/de imprensa).

Em recente decisão[8], a 3ª Turma do Superior Tribunal de Justiça entendeu pela obrigatoriedade da prévia autorização do consumidor para o compartilhamento de seus dados.

A relatoria reafirmou a impreteribilidade do notificar o consumidor acerca do compartilhamento de dados comuns fornecidos durante a prestação, ainda que não se configurem como dados sigilosos ou sensíveis, não podendo a empresa responsável pelo tratamento de dados cedê-los de qualquer forma, salvo mediante anuência expressa. Neste sentido, cumpre observar que o entendimento do STJ vai ao encontro da Lei Geral de Proteção de Dados - LGPD, que apesar de ainda não estar vigente, foi contemplada adequadamente.

Segundo a ministra Nancy Andrighi, relatora, em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, deve ser observada a regra do inciso V do artigo 5º da Lei 12.414/2011[9] (Lei do Cadastro Positivo), a qual assegura ao cadastrado o direito de ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais.

1.2 – A Proteção de dados como direito fundamental:

Tramita no Senado a PEC 17/19, que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. A proposta também fixa competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais.

Para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, a PEC 17/19, dá nova redação ao artigo 5º da Constituição Federal. O texto inicial acrescenta ao dispositivo o inciso XII-A, estabelecendo que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".

A aplicação da publicidade nunca foi absoluta e uma interpretação mitigada tem por base a dualidade existente entre a necessidade de produzir efeitos erga omnes e a proteção de dados pessoais voltados para tutelas específicas, como direito de família ou proteção de crianças, adolescentes e incapazes, limitações que têm por escopo proteger a dignidade humana (art. 1º, inc. III, CF/88), a intimidade (art. 5º, incs. X e LX e art. 93, inc. IX, CF/88) ou o interesse social (art. 5º, inc. LX, CF/88).

O STF reconhece o direito fundamental à proteção de dados pessoais em julgamento sobre a suspensão da MP n. 954/2020[10].

Em um julgamento histórico de 5 (cinco) Ações Diretas de Inconstitucionalidade (ADIn), ocorrido nos dias 06 e 07 de maio de 2020, o Supremo Tribunal Federal (STF), por maioria, determinou a suspensão da eficácia da Medida Provisória n. 954/2020. A decisão do Plenário referendou a liminar anteriormente deferida pela Relatora das ações, Ministra Rosa Weber.

A ministra do Supremo Tribunal Federal (STF) Rosa Weber atendeu ao pedido de liminar feito pelo Psol, por meio da Ação Direta de Inconstitucionalidade (ADI) 6390, para suspender a Medida Provisória 954/2020. A MP determina que empresas de telefonia repassem dados de clientes pessoa física e jurídica, como nome, endereço e telefone, para o IBGE realizar a Pesquisa Nacional por Amostra de Domicílios Contínua, que mede o desemprego.

As cinco ADIn[11], ajuizadas por partidos políticos e pela Ordem dos Advogados do Brasil (OAB), questionavam dispositivos da MP, que autorizava o compartilhamento de dados pessoais pelas empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE). O objetivo do tratamento das informações pessoais seria possibilitar a produção estatística oficial, durante a situação de emergência decorrente da pandemia da Covid-19[12].

A Suprema Corte entendeu que a Medida Provisória poderia trazer riscos a direitos fundamentais, como a intimidade, a privacidade e a proteção de dados.

Como regra, o tratamento das informações deve ater-se à finalidade para qual foi realizada (Ex. Dados coletados pelo IBGE devem ser utilizados, apenas, para as políticas públicas cuja execução depende das informações da coleta).

Em outro julgamento[13], o Supremo Tribunal Federal (STF), deferiu parcialmente medida cautelar na Ação Direta de Inconstitucionalidade (ADI) 6529 para estabelecer que os órgãos componentes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin)[14] quando for comprovado o interesse público da medida, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados. Segundo a decisão majoritária, que deu interpretação conforme a Constituição ao parágrafo único do artigo 4º da Lei 9.883/1999, toda e qualquer decisão que solicitar os dados deverá ser devidamente motivada, para eventual controle de legalidade pelo Poder Judiciário.

Os ministros também decidiram que, mesmo se houver interesse público, os dados referentes às comunicações telefônicas ou sujeitos à análise da Justiça não podem ser compartilhados com base no artigo 4º da Lei 9.883/1999, que instituiu o Sisbin e criou a Abin, em razão de limitação aos direitos fundamentais. O STF declarou, ainda, que, nas hipóteses cabíveis de fornecimento de informações e dados à Abin, é imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

Ao dar interpretação conforme a Constituição à lei que criou a Abin, o Plenário afastou a possibilidade de que o compartilhamento atenda a interesses pessoais ou privados

As decisões vão ao encontro da Proposta de Emenda à Constituição 17/2019[15] que propõe a inclusão da proteção de dados pessoais dentre os direitos e garantias fundamentais, bem como a fixação de competência privativa da União para legislar sobre o tema.

Tratamentos de Dados Pessoais pelo Poder Público
Toda decisão de solicitação de dados deve ser motivada, ou seja, precisa ficar documentado qual o objetivo do pedido de informações. A LGPD, inclusive, traz um capítulo específico sobre o tratamento de dados pessoais pelo Poder Público.

O principal requisito permissivo para o tratamento de dados pessoais pela Administração Pública é o que está presente no artigo 7º, III

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

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; (grifado)

Execução de políticas públicas é, portanto, a principal e indubitavelmente a melhor justificativa para que o setor público realize qualquer tipo de tratamento de dados. Sendo este um conceito muito amplo, dando larga margem para a manipulação dos dados pessoais pelo setor público, uma vez que é inerente à própria existência do Estado a consecução de políticas públicas.

Ocorre que a LGPD não define o que seria considerado um “incidente de segurança” e também não traz delimitações do que seria um incidente com potencial de risco, tendo deixado tais parâmetros para a Autoridade de Proteção de Dados Pessoais (ANPD), criada pela medida provisória 869/18, convertida na Lei nº 13.853, de 8 de julho de 2019.

Enquanto a ANPD não regulamenta estas lacunas, o Regulamento Geral Europeu de Proteção de Dados Pessoais (GDPR)[16] se mostra como uma direção interpretativa que não pode ser ignorada, principalmente, pela semelhança da lei brasileira com este texto.

Vale ainda dizer que a LGPD, em seu Art. 6º, busca garantir que nossos dados pessoais sejam utilizados com propósitos legítimos, com finalidades específicas; exige que haja informação sobre a forma e a duração do tratamento; exige informações claras e precisas sobre a realização do tratamento; determina medidas aptas a proteger os dados pessoais de acessos não autorizados; proíbe o tratamento de dados pessoais para fins discriminatórios, etc.

Deve ser tratada considerando a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. A LGPD define, por exemplo, que uma organização pode, sem precisar pedir novo consentimento, tratar dados tornados anterior e manifestamente públicos pelo titular.

Ao analisar a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/18, precisamente no artigo 7º, verifica-se que o texto legal é categórico ao elencar o rol taxativo das hipóteses para tratamento de dados, sendo cristalina a necessidade do consentimento do titular nos termos do §5º deste dispositivo.

Vejamos: § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

O objetivo deste artigo, no entanto, é tratar de um específico ponto da nossa nova lei, uma exceção ao consentimento exigido do titular para o uso de suas informações pessoais (uma das principais hipóteses autorizadoras para o processamento de dados por entes privados), descrita de forma tímida em um parágrafo, mas cujo papel pode ser estratégico na atividade de quem está sujeito a essa legislação. Trata-se do §4º do art. 7º da LGPD, no qual se lê:

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

I - mediante o fornecimento de consentimento pelo titular;

4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta lei.
O Art. 7º, § 7º, da LGPD, estipula que o tratamento de dados pessoais disponíveis publicamente, sejam eles tornados públicos pelo próprio titular ou disponibilizados por ente público, pode ser realizado para finalidades diferentes daquela que motivou sua publicização inicial.

Devem ser observados nestes casos, porém, os propósitos legítimos e específicos para o novo uso dos dados, sendo o conceito do “propósito legítimo” a chave para avaliar a licitude de tal uso.

Com a opção legislativa por exigir somente o propósito legítimo – e não legítimo interesse – para fundamentar o tratamento de dados disponíveis publicamente, depreende-se que a intenção do legislador foi criar um fundamento legal mais flexível para esse tipo de tratamento, reconhecendo a importância e finalidade de fontes públicas de dados pessoais. Na própria exposição de motivos da emenda parlamentar que levou à criação do Art. 7º, § 7º, relator reconhece que, “quando ele é publicamente acessível, o dado pessoal passa a ser um importante elemento para a realização de análises e estudos, […] promovendo competividade, inovação, empregabilidade e prosperidade”.

Em um ambiente de análise de enorme volume de dados – big data – é comum haver usos secundários mais inovadores do que aqueles que justificaram a própria coleta original de dados pessoais. Daí a relevância desse tipo de tratamento e, como consequência, da discussão sobre o seu cabimento ou não.

Assim, o art. 7º, § 7º da LGPD, pode oferecer maior maleabilidade para o tratamento de dados pessoais disponíveis publicamente, mas também não deve ser compreendido como uma carta branca para uso irrestrito dessas informações – o princípio da finalidade aplicado às atividades de tratamento de dados pessoais deve prevalecer.

E, no mesmo §7º acrescentado pela nova redação da MP 869/2018, a LGPD ainda garante a preservação dos direitos do titular no caso de tratamento de dados disponíveis publicamente. Isso inclui, por exemplo, o direito do titular receber informações claras e precisas sobre o tratamento de suas informações pessoais, bem como de solicitar acesso a seus dados e exigir a correção de informações incorretas.

Ao mencionar os propósitos legítimos como fundamento para o tratamento posterior de dois grupos de dados pessoais – aqueles cujo acesso é público (art. 7º, §3º) e os tornados manifestamente públicos pelo titular (art. 7º, §4º) –, a MP 869/2018 parece conferir maior segurança ao uso de dados para novas finalidades não imaginadas por ocasião de sua coleta. É certo, porém, que o conteúdo normativo desses propósitos legítimos, que servirão de fundamento para o uso secundário de dados pessoais, ainda deve ser lido em atenção às finalidades de cada tratamento, a serem examinadas mesmo quando o acesso a esses dados for público.

2.1 - Informação pessoal na Lei de Acesso à Informação (LAI)

Segundo a LGPD, a informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. Neste caso existe restrição de acesso: respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais Ex.: endereço residencial e eletrônico; número do telefone; informações médicas e sociais; informações financeiras (sigilo bancário e fiscal); informações sobre relacionamentos amorosos; preferências pessoais; divulgação de fotos e dados biométricos.

A LGPD afirma que as pessoas jurídicas de direito público referidas na Lei de Acesso à Informação (LAI) estarão submetidas à legislação.

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Artigo 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)[17], deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Segundo a Lei Geral de Proteção de Dados Pessoais, o tratamento de dados pessoais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (art. 1º - LGPD)

A LGPD em seu Art. 5º. X – dispõe sobre tratamento: como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Sobre este tema os autores Chiara Spadaccini de Teffé e Mario Viola[18] tratam a despeito:

“Voltando para os parágrafos do Art. 11 da LGPD, a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da Autoridade Nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. Segundo a Lei, é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.” (TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. 2020)

O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado.

Já as empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas, terão o mesmo tratamento dispensado aos órgãos públicos. (art. 24)

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Já os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

Para os cartórios, a LGPD definiu que se aplicarão as mesmas regras do tratamento pelo Poder Público (artigo 23 e seguintes), e, considerando a natureza dos serviços previstos nas leis 6.015/73 e 8.935/945, é evidente que uma imensa quantidade de dados pessoais é diariamente tratada pelos cartórios extrajudiciais, exigindo dos notários e registradores muita precaução.

Serviços notariais e de registro (art. 23 § 4º)

Art. 23 da LGPD

4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.
A verdade é que a LGPD, com suas diversas obrigações e princípios traz uma série de desafios a serem vencidos pelos agentes de tratamento, como – por exemplo: (i) garantir aos titulares o regular exercício de todos os direitos previstos na lei (portabilidade, confirmação do tratamento, cópia dos dados, anonimização...); (ii) garantir que o acesso aos dados pessoais é conferido apenas àqueles colaboradores/terceirizados que devam ter acesso; (iii) adequar corretamente as hipóteses legais de tratamento (às vezes, partir para obter o consentimento pode não ser a melhor alternativa); (iv) garantir a segurança dos dados pessoais durante todo o ciclo de vida, gerando trilhas auditáveis; e (v) mudar a cultura, conscientizar e treinar colaboradores e terceirizados.

Fato é que, quando se fala em proteção de dados pessoais, não há como se afastar da temática atinente à segurança, incluindo a da informação. Já no artigo 1º da lei 8.935/94[19], que regulamenta o artigo 226 da CF/88, observa-se que os serviços notariais e de registro destinam-se, dentre outros pontos, a conferir segurança aos atos jurídicos.

Ao falar em segurança, o legislador não se limita à segurança jurídica, abarcando também a segurança físico-lógica das informações disponibilizadas ao notário e ao registrador, sendo dever de tais profissionais guardarem em locais seguros os livros, papéis e documentos de sua serventia; guardar sigilo sobre a documentação e os assuntos de natureza reservada que tenham conhecimento em razão do exercício da função (artigo 30, I e VI da lei 8.935/94).

De mais a mais, a lei 8.935/94 “Lei dos Notários e Registradores”, no artigo 42, exige que os papéis referentes aos serviços dos notários e dos oficiais de registro sejam “arquivados mediante utilização de processos que facilitem as buscas” e, lá no artigo 46, dispõe que “os livros, fichas, documentos, papéis, microfilmes e sistemas de computação deverão permanecer sempre sob a guarda e responsabilidade do titular de serviço notarial ou de registro, que zelará por sua ordem, segurança e conservação”.

Como se vê, bem antes da LGPD, a legislação setorial já continha direcionamentos quanto à necessidade de garantia da tríade base da segurança da informação, a “CID”: Confidencialidade, Integridade e Disponibilidade das informações.

Deverá ser realizado para o atendimento de sua finalidade pública, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

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

seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.
E as exceções ao consentimento previstas na LAI? Subsistem diante da nova Lei? - Subsiste a necessidade de cumprir a LAI (art. 23, §2º).

A Administração Pública não está sujeita às multas previstas nos incisos II e III. O regime sancionatório da LGPD não afasta o previsto na LAI.

A LGPD e a LAI possuem concepção semelhante sobre o que é dado pessoal. E as duas leis põem a salvo as informações pessoais dos titulares de dados pessoais no tocante à intimidade, à vida privada, à honra e à imagem - sendo elas restritas aos titulares e aos agentes de tratamento dos dados pessoais.

As tutelas dizem respeito à pretensão do indivíduo de não ser foco de observação de terceiros, de não ter os seus assuntos, informações pessoais e características expostas a terceiros ou ao público em geral.

Observa-se que ambas as legislações visam resguardar a informação pessoal, os que as diferem é quanto ao processo de tratamento no ciclo de vida dos dados ante as políticas de privacidade e proteção, assim como suas bases legais e princípios autorizadores.

As entidades e os órgãos públicos que fizerem tratamento de dados em desconformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD poderão ser penalizados com:

Advertência, com indicação de prazo para adoção de medidas corretivas;
Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
Bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e
Eliminação dos dados pessoais a que se refere a infração.
Além disso, os responsáveis poderão ser sancionados com as penas do Estatuto do Servidor Público, da Lei de Acesso à Informação (LAI) e da Lei de Improbidade Administrativa.

Observa-se que não existe uma superioridade de uma lei sobre a outra, mas particularidade em ambas: uma em garantir o acesso à informação; em regra; e a outra em assegurar a privacidade dos dados pessoais.

É notório que ambas (LGPD e LAI) buscam resguardar a informação pessoal de terceiros não autorizados, porém apenas a LGPD transfunde na preocupação em ter análise de impacto de privacidade documentada, políticas de privacidade e proteção documentada, políticas de respostas a incidentes.

Desta forma, nota-se que as leis, apesar de suas peculiaridades, mais contribuem para a proteção de dados pessoais comuns e especiais do que as repelem.

A LAI não tem no seu bojo previsão de pena pecuniária diante dos entes públicos da administração pública direta e indireta, porém os servidores podem responder perante a Lei de Improbidade Administrativa[20], assim como responder a um possível PAD (Processo Administrativo); o caso concreto determinará tais ocorrências.

Entende-se quando da aplicação da LGPD, ante às instituições públicas, também será passível de aplicação da Lei de Improbidade Administrativa com instauração de PAD aos servidores públicos. Destarte, tanto a LAI quanto a LGPD estão tendo como pano de fundo no ordenamento jurídico, a qual todos os agentes, servidores e empregados públicos devem ter como elemento norteador.

2.2 – Do compartilhamento de dados pelo poder Público

Sobre o compartilhamento de dados, a LGPD determina no art. 23 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 serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, como previsto no art. 26 da LGPD.

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

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

II- (..)

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

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

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

Já o art. 27 da LGPD trata sobre o procedimento formal da disponibilização de dados a terceiros:

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei [titular dos dados deve ser informado sobre a finalidade e procedimentos para tratamento dos dados]; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Como já decidido pelo próprio Supremo Tribunal Federal e indubitável leitura do caput do art. 26 da LGPD, é permitido o uso compartilhado de dados pelo Poder Público, desde que tenha por objetivo atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6° da lei.

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

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

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

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

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

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

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

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

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

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

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

Originalmente, o Poder Público apenas poderia compartilhar dados com entidades privadas em caso de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado; e nos casos em que os dados forem acessíveis publicamente.

Com a edição da Medida Provisória 869/18, o Poder Público também poderá compartilhar dados com entidades privadas se for indicado um encarregado; quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados.

No mais, é importante destacar que a LGPD tornou obrigatória a observância dos princípios Privacy By Design e Privacy By Default, pelos quais as entidades devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução.

Embora um dado pessoal tornado público (pelo próprio titular ou terceiros, inclusive pelo Estado) siga sendo um dado pessoal protegido pela LGPD, a nova redação do artigo 7º, §7º, deixa claro que tal informação poderá ser utilizada para novas finalidades (diferentes daquelas pelas quais o dado se fez público), desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD. Isso significa que, embora claramente seja possível utilizar um dado de acesso público para novas finalidades, será necessário que a empresa realize um teste de proporcionalidade e balanceamento de suas intenções, para que se avalie se estão de acordo com os requisitos trazidos por esse dispositivo legal, quais sejam: (i) propósito legítimo e específico, (ii) preservação dos direitos dos titulares e (ii) fundamentos e princípios da LGPD.

Vale lembrar que, enquanto a LGPD “original” apresentava vedação genérica em relação ao compartilhamento de dados de saúde para finalidades econômicas (com exceção apenas para hipóteses de portabilidade de dados solicitada pelo titular ou de consentimento - sendo que essa última, em nosso entendimento, ainda pode ser apoiada na própria base legal do consentimento específico e destacado para tratamento de dados sensíveis), a MP pretendia ampliar a autorização legal para compartilhamentos dessa natureza sempre e quando

fossem necessários para “adequada prestação de serviços de saúde suplementar”, expressão genérica e ampla que acabou não vingando na versão final da Lei, como visto acima.

Caso venha a haver alguma alteração na motivação do uso dos dados ou na finalidade do repasse para outras organizações, deverá ser realizado um novo pedido de autorização para o usuário.

A Autoridade Nacional de Proteção de Dados – ANPD poderá solicitar a elaboração de relatório de impacto à proteção de dados pessoais aos órgãos do Poder Público.

A ANPD poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

A ANPD estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

O encarregado, também conhecido por DPO (Data Protection Officer) é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Com a nova redação dada pela Lei nº 13.853, de 2019, o encarregado poderá ser pessoa natural (pessoa física) ou pessoa jurídica. (art. Art. 5º, inciso VIII).

Se o órgão do Poder Público compartilha dados pessoais constantes de sua base de dados com entidades privadas deverá obrigatoriamente indicar um encarregado (Data Protection Officer - DPO).

Pesquisadores concluíram que o poder público não vem adotando boas práticas de segurança e proteção de dados pessoais no desenvolvimento desses aplicativos, uma vez que adotam um tipo de permissão abrangente e não esclarecem para qual finalidade específica deve ser concedida determinada permissão ou ainda qual a política pública que está vinculada à coleta daquele dado ou ainda a base legal que permite tal procedimento. Esse modo de operação contraria as melhores práticas de segurança da informação que orientam que seja utilizado o modelo de obtenção de permissão específica, além disso, contrariando também os princípios expressos no artigo 6º da LGPD especialmente no que diz respeito à finalidade, inciso I e minimização da coleta, inciso III.

Conclusão

A finalidade é o principal princípio que embasa a LGPD nesse ponto, pois todo e qualquer compartilhamento de dados pessoais deve ser feito com fulcro na realização do fim que justificou a coleta do dado e ainda que foi informado à parte. Naturalmente, a finalidade deve preceder a coleta de dados e a ela fica vinculada para quaisquer atividades. A partir

dela é que se compreende a racionalidade que presidiu o envio de dados. Logo, é ela o critério norteador de qualquer aplicação.

É preciso compreender que o compartilhamento de dados deve ser verificado à luz das Políticas Públicas e finalidades institucionais dos receptores do envio de dados pessoais, com vistas ao cumprimento da LGPD.

A LGPD é bastante criteriosa ao se referir aos órgãos notariais e de registro, determinando de forma restritiva a necessidade de “fornecer acesso a dados por meio eletrônico” (art. 23, parágrafo 5º, LGPD). O dispositivo restringe as possibilidades quanto ao compartilhamento ou envio de dados e ratifica dispositivo anterior, que já mencionava que os serviços de registros públicos deveriam apenas disponibilizar ao Poder Judiciário e ao Poder Executivo federal, por meio eletrônico e sem ônus, o acesso às informações (art. 41, lei 11.977/09).

Resta claro que além da privacidade, a LGPD busca resguardar o compartilhamento ou acesso de dados e vinculá-lo às suas finalidades (art. 6º, incs. I, II e III, LGPD), evitando desvios e oportunismos no trato de dados pessoais, preservando as atribuições registrais e engrandecendo tal atribuição.

A responsabilização administrativa para os órgãos públicos e entidades de Registro Empresarial (Juntas Comerciais) não implica em multa (art. 52, parágrafo 3º LGPD), mas as sanções como bloqueio dos dados pessoais podem causar grande impacto na atuação pública.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração.

De acordo com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)[21], até o final de 2019, já haviam ocorrido mais de 9 mil incidentes de vazamentos de informações provenientes de órgãos ou entidades públicas. O que demonstra que o setor público assim como o privado precisam estar preparados para lidarem com o vazamento de informações.

Fatos que envolvam órgãos públicos, pela LGPD, não estarão sujeitos às sanções de multas, apenas a advertências e a eliminação de dados. Entretanto, isso não significa que servidores públicos envolvidos nos casos não sejam punidos ou penalizados.

Para o setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social disposto no ordenamento jurídico pátrio, já que conhecer seus cidadãos é, para o Estado, um pré-requisito para o próprio exercício de desempenho de suas finalidades públicas.

Concluindo, faz-se necessário encontrar um ponto de equilíbrio entre os direitos existentes no que toca à coleta de dados massivos dos usuários dos serviços públicos, realizando um juízo de ponderação entre a autonomia da vontade e a liberdade de contratar, traduzida pelo princípio da livre iniciativa (art. 1º, IV da CF. c/c art. 2º, VI da LGPD) e o direito à privacidade e à proteção de dados pessoais, cumprindo a Lei Geral de Proteção de Dados um relevantíssimo papel neste sentido.

Referências Bibliográficas

AMARAL, Luiz Fernando de Camargo Prodente do. Desafios da LGPD em Relação à Implementação pelo Poder Público. In: BLUM, Renato Opice (Coord.). Proteção de Dados. Desafios e Soluções na Adequação à Lei. Rio de Janeiro: Forense, 2020, p. 84.

BIONI, Bruno R. Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BODIN DE MORAES, Maria Celina. Danos à pessoa humana: uma leitura civilconstitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasíl. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasíl. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3

DAL POZZO, Augusto Neves, MARTINS, Ricardo Marcondes. LGPD e Administração Pública - 1ª Ed. Rt - Revista dos Tribunais. 2020

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006. p. 11-12

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SETOR PÚBLICO Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas. Relatório do Instituto de Tecnologia e Sociedade (ITS). Disponível em: https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf

MEINBERG, Fred. Consentimento versus Legítimo Interesse. Disponível em: https://fredmeinberg.com.br/2019/04/17/consentimento-versus-legitimo-interesse/

MEINBERG, Fred. Fred-Meinberg-E-Book-LGPD-no-poder-publico-e-cartorios. Disponível em: https://fredmeinberg.com.br/e-book-l-g-p-d-governo/

Migalhas. LGPD e setor público: aspectos gerais e desafios. Angela Maria Rosso. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios

MULHOLAND, Caitlin et MATERA, Vinicius. O Tratamento de Dados Pessoais pelo Poder Público. In: MULHOLLAND, Caitlin (Coord). A LGPD e o Novo Marco Normativo no Brasil, Porto Alegre: Arquipélogo, 2020, p. 224

PIERI, José Eduardo de V.; BASTOS, Rodrigo Albero Caldeira; SCHVARTZMAN, Felipe . Dados pessoais ‘públicos’ são, de fato, públicos? Site JOTA Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados-pessoais-publicos-sao-de-fato-publicos-30062019

SILVA, Érica Barbosa; RIBEIRO, Izolda Andréa de Sylos; ASSUMPÇÃO, Letícia Franco Maculan. A lei geral de proteção de dados e o registro civil das pessoas naturais Site Migalhas. Disponível em: https://www.migalhas.com.br/depeso/315759/a-lei-geral-de-protecao-de-dados-e-o-registro-civil-das-pessoas-naturais

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>.

ZOMPERO, Rogério. O registro público de empresas mercantis e atividades afins. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5367, 12 mar. 2018. Disponível em: https://jus.com.br/artigos/64025. Acesso em: 15 ago. 2020.

Notas:

* Doutorando em Ciências Jurídicas - UCA (Univ. Católica da Argentina), Mestrado em Direito Empresarial Econômico - UCA (Univ. Católica da Argentina). Especialista com MBA em Direito do Consumidor e da Concorrência pela FGV/RJ. Membro da Comissão de Defesa do Consumidor e da Comissão da Proteção de Dados e Privacidade da OAB/RJ. Sócio do Escritório Terra Sarmento Rocha Advogados e Procurador Adjunto da Junta Comercial do Estado do Rio de Janeiro – JUCERJA.

[2] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 10 de agosto de 2020.

[3] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm Acesso em: 10 de agosto de 2020.

[4] Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em: 10 de agosto de 2020.

[5] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 10 de agosto de 2020.

[6] LGPD - Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

*II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)

*OBS.: Com a não aprovação deste item da MP 959, voltou a valer a redação anterior do inciso II

[7] Decreto nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

[8] Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Compartilhamento-de-informacoes-de-banco-de-dados-exige-notificacao-previa-ao-consumidor.aspx Acesso em 10 de agosto de 2020.

[9] Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm#art5v Acesso em 10 de agosto de 2020.

[10] MENDES, Laura Schertel. Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020

[11] ADIs n. 6387, 6388, 6389, 6393, 6390.

[12] Desde o início de fevereiro de 2020, a Organização Mundial da Saúde (OMS) passou a chamar oficialmente a doença causada pelo novo coronavírus de Covid-19. COVID significa COrona VIrus Disease (Doença do Coronavírus), enquanto “19” se refere a 2019, quando os primeiros casos em Wuhan, na China, foram divulgados publicamente pelo governo chinês no final de dezembro. A denominação é importante para evitar casos de xenofobia e preconceito, além de confusões com outras doenças. Disponível em: https://portal.fiocruz.br/pergunta/por-que-doenca-causada-pelo-novo-virus-recebeu-o-nome-de-covid-19 Acesso em 10 de agosto de 2020

[13] Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1

[14] Órgão central de um sistema que reúne 38 integrantes – o Sistema Brasileiro de Inteligência (Sisbin) –, a ABIN tem por missão assegurar que o Executivo Federal tenha acesso a conhecimentos relativos à segurança do Estado e da sociedade, como os que envolvem defesa externa, relações exteriores, segurança interna, desenvolvimento socioeconômico e desenvolvimento científico-tecnológico. Disponível em: http://www.abin.gov.br/institucional/a-abin/ Acesso em 10 de agosto de 2020.

[15] Disponível em:https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757> Acesso em 10 de agosto de 2020

[16] Disponível em: https://gdpr-info.eu/

[17] LAI – Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em 10 de agosto de 2020.

[18] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>.

[19] Lei dos Notários e Registradores. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8935.htm Acesso em 10 de agosto de 2020.

[20] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8429.htm Acesso em 10 de agosto de 2020

[21] O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) faz parte do Departamento de Segurança de Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Disponível em https://www.ctir.gov.br/alertas/

Palavras Chaves
Dados pessoais; tratamento de dados; poder público; bases legais.