PROCESSO Nº: 33910.029786/2019-51

NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES

Interessado:

DIRETORIA DE DESENVOLVIMENTO SETORIAL

Registro ANS: DIDES

1. INTRODUÇÃO

A Agência Nacional de Saúde Suplementar (ANS) vem implementando medidas e estratégias de gestão da informação orientadas pelos princípios, pelas diretrizes e pelos preceitos estabelecidos pelos principais marcos legais promulgados nos últimos anos que tratam do tema.

Dentre os marcos legais relativos ao tema, destaca-se, por exemplo, a Lei da Transparência (LC 131/2009); a Lei de Acesso a Informação (Lei nº 12.527/2011), que regulamentou o direito constitucional de acesso às informações públicas, e o Decreto n.º 8.777, de 2016, que dispõe sobre a Política de Dados Abertos.

No último ano, foi promulgada a Lei Geral de Proteção de Dados Pessoais(Lei 13.709/2018), que estabelece padrões, regras e princípios para o tratamento de dados pessoais, a qual, após alteração promovida pela nº 13.853, de 09 de julho de 2019, entrará em vigor em agosto de 2020.

Tendo como principais objetivos a proteção dos direitos fundamentais de liberdade, privacidade e o desenvolvimento da personalidade da pessoa natural, a lei em questão acaba por consolidar determinados princípios constitucionais e obrigações legais esparsas afeitos ao Tratamento de Dados Pessoais de Pessoas Naturais na legislação brasileira.

Avalia-se que a entrada em vigor da LGPD trará implicações tanto para a ANS quanto para o setor regulado, tendo em vista que alguns sistemas estruturantes da saúde suplementar, bem como algumas obrigações de envio de informações por parte do setor regulado, que transacionam dados pessoais, precisarão ser adequadas às exigências da lei.

2. PROTEÇÃO DE DADOS PESSOAIS NO MUNDO

O Regulamento Geral de Proteção de Dados (GPRD), Regulamento (UE) 2016/6791 foi aprovado em 15 de abril de 2016 e, após um período de transição de dois anos, entrou em vigor em 25 de maio de 2018. Este regulamento concretiza e desenvolve o direito fundamental das pessoas físicas à proteção de dados de caráter pessoal que lhes digam respeito.

Anteriormente ao GPRD, cerca de 120 países já possuíam leis gerais de proteção de dados pessoais. No âmbito dos países membros da OECD, foram estabelecidas diretivas (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), que entraram em

aplicação em 23/11/1980, no sentido de que os Estados-membros deveriam prover legislação interna para proteção da privacidade e dos direitos individuais no gerenciamento de dados pessoais. Essa legislação deveria se aplicar aos setores públicos e privados, com a observância de limites à obtenção de dados pessoais, que somente poderia ser feita de forma legal e justa, de preferência com o consentimento do indivíduo. Os dados pessoais obtidos deveriam ser relevantes para os propósitos a que se destinam e ser mantidos precisos, completos e atualizados.

Os modelos de Autoridade de Proteção de Dados implementados pelos Estados-membros da União Europeia foram analisados pela Agência dos Direitos Fundamentais da UE para destacar as melhores práticas e os desafios enfrentados no âmbito do sistema europeu. Três pontos considerados como particularmente relevantes são os elementos principais a serem considerados no momento da criação de uma autoridade: (i) sua natureza jurídica de direito público; (ii) sua independência e (iii) sua autonomia orçamentária.

De acordo com Paixão (2018), na América Latina, a Argentina é o país que tem leis de proteção de dados pessoais em vigor desde 1994. Porém, com a entrada em vigor da GDPR na EU, há tendência de que esses regulamentos atuais sejam adequados. O México aprovou em 2010 a Lei Federal Mexicana de Proteção de Dados Pessoais em Poder de Particulares. Há ainda outros países que ainda que não tenham elaborado legislação abrangente de proteção de dados pessoais, possuem dispositivos que regulamentam em parte a proteção de dados, como Colômbia, Chile, Peru e Costa Rica.

A LGPD brasileira demonstra a preocupação do legislador com questões e princípios de transparência, especialmente ao exigir dos controladores e operadores informações claras e transparentes ao titular dos dados pessoais em relação às finalidades de uso e tratamento dos seus respetivos dados.

Claramente inspirada na regulação europeia relativa aos dados pessoais, a Lei 13.709/2018 aspira a conciliação entre a proteção da pessoa, o interesse público e o incentivo ao desenvolvimento econômico e tecnológico, vinculados, em nossas sociedades, à circulação e ao uso da informação. O que à primeira vista poderia então ser encarado como um conflito de normas através da dicotomia transparência vs. privacidade, na prática, pode ser interpretado lato sensu como complementar.

3. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL ANTES DA LGPD

O ordenamento jurídico brasileiro, ao tratar da proteção do direito à privacidade, tradicionalmente dava mais ênfase ao aspecto clássico de liberdade negativa.

A Constituição da República Federativa do Brasil, de 1988, previu a intimidade e a vida privada como direitos fundamentais, conforme disposto nos incisos X, XI, XII e LX de seu artigo 5°. Esses dispositivos trataram da privacidade como “direito de estar só”, a qual foi protegida pela inviolabilidade do domicílio, sigilo telefônico, de correspondência, de comunicações telegráficas e de dados.

A própria Constituição Federal reconheceu o caráter relativo do direito à privacidade e admitiu sua limitação frente a outros interesses de porte constitucional, como as restrições ao sigilo de correspondência e ao sigilo de comunicação telegráfica e telefônica que podem ser determinadas para a proteção do interesse público no caso de estado de defesa ou de estado de sítio, conforme disposto no artigo 136, § 1°, inciso I, alíneas “b” e “c”, e no artigo 139, inciso III da Magna Carta.

Essa faceta do direito à privacidade foi reforçada pelo Código Civil de 2002, que dispôs sobre a privacidade no capítulo que trata dos direitos da personalidade. A privacidade foi tratada tão somente no seu aspecto de liberdade negativa pelo artigo 21, admitidas exceções ao direito de inviolabilidade, conforme o artigo 20 desse Código.

Os artigos 347, 363 e 406 do Código de Processo Civil protegeram indiretamente do direito à privacidade ao assegurarem o direito da parte ou de terceiro de não depor sobre fatos, ou de

exibir coisas que revelem fatos “a cujo respeito, por estado ou profissão, deva guardar sigilo”.

Também protegeram o direito à privacidade em seu aspecto de liberdade negativa os tipos penais de “violação de correspondência”, “violação de comunicação telegráfica, radioelétrica ou telefônica”, “divulgação de segredo”, “violação do segredo profissional”, “invasão de dispositivo informático” e “violação de sigilo funcional” (arts. 151, 153, 154, 154-A e 324). Previstos no Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940).

Mas a Constituição não se limitou à noção tradicional de privacidade. O inciso XXXIII, a alínea “b” do inciso XXXIV e o inciso LXXII do artigo 5º da Constituição Federal, ao disporem sobre o direito do indivíduo de acessar e retificar suas informações pessoais em posse de entidades governamentais ou de caráter público, indicaram que foi adotada a concepção de privacidade como “liberdade informacional”, assegurando o controle do indivíduo sobre suas próprias informações.

A faceta de liberdade informacional ganhou destaque nas disposições do Código de Defesa do Consumidor, de 1993, sobre os direitos dos consumidores em face de bancos de dados com informações pessoais. Estão previstos no artigo 43 direitos do consumidor:

a) de acesso a suas informações pessoais existentes nesses registros;

b) à objetividade, clareza, veracidade e inteligibilidade dessas informações;

c) à ciência da abertura de registro com suas informações pessoais;

d) à correção de informações inexatas que tenham sido registradas.

O Decreto nº 4.553, de 2002, alterado pelo Decreto nº 5.301, de 2004, e revogado pelo Decreto nº 7.845, de 14 de novembro de 2012, dispunha sobre “a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal”.

Tal decreto impunha medidas especiais de segurança e limitações ao conhecimento de informações sigilosas que se aplicam à sua “produção, manuseio, consulta, transmissão, manutenção e guarda”. Apesar de esse texto se destinar claramente à proteção da segurança da sociedade e do Estado, ele também tratava, ainda que de forma bastante superficial, da privacidade de informações pessoais, pois incluía entre os dados e informações sigilosos “aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas”.

Além da limitação e controle de acesso às informações sigilosos, bem como outras medidas especiais de segurança relativas ao manuseio, à consulta, à transmissão, à manutenção e à guarda dessas informações, esse Decreto possuía previsões específicas de proteção à privacidade, como o direito do cidadão de acessar as informações sigilosas que digam respeito à sua pessoa, bem como a exigência, para liberação de documentos que contenham informações pessoais, de autorização prévia do titular ou de seus herdeiros.

Em 2011 foi promulgada a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011), regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012, a qual tem como claro objetivo facilitar o acesso dos cidadãos aos documentos e às informações controlados por órgãos e entidades da administração pública direta, indireta e fundacional, estabelecendo a publicidade e a transparência como regra e o sigilo como exceção.

Em relação às informações pessoais, foram tratadas como sigilosas apenas as sensíveis, ou seja, aquelas referentes à intimidade, vida privada, honra e imagem. Além das exceções a esse sigilo já previstas no Decreto 4.553 (titular, agentes públicos e consentimento), também dispensou o consentimento do titular para acessar informações pessoais sensíveis na tutela da saúde, na realização de estudos e pesquisas científicas, no cumprimento de ordem judicial, na defesa de direitos humanos e na proteção de interesse público geral preponderante. Destaque-se que o art. 31 dessa Lei reforçou um pouco mais o direito à liberdade informacional, criando um dever de transparência no tratamento das informações pessoais, apesar de não especificar como deve ser exercitada essa transparência.

4. PROTEÇÃO DE DADOS PESSOAIS NA LGPD

A LGPD, aprovada em 2018, e tendo como paradigma o Regulamento Geral sobre a Proteção de Dados da União Européia (GDPR), afirmou inequivocamente o direito à privacidade como liberdade informacional, assegurando o que o Tribunal Constitucional Federal alemão chamou de *Informatinelle Selbstestimmung*, ou seja, a autodeterminação em matéria de informação, que conjuga o aspecto negativo ao domínio ou controle pelo indivíduo sobre os *inputs* e *outputs* de informação dos quais é titular.

Os direitos dos titulares de dados pessoais não apenas foram declarados, mas também foram assegurados:

a) pela previsão de restrições no tratamento de dados pessoais e de imposição aos agentes no tratamento de dados pessoais de requisitos de segurança, acesso e controle;

b) pela criação de uma estrutura de governança e *accountability* com definição das responsabilidades e obrigações de empresas, órgãos e entidades públicas e autoridades regulatórias quanto à transparência, ao monitoramento, à prestação de contas, gestão de risco e garantia dos direitos dos titulares de dados pessoais.

4.1. Alcance da norma

A LGPD se limita a regular o tratamento de dados pessoais:

a) de pessoas naturais (art. 5º, I), de modo que ela não cria nenhuma proteção adicional aos dados de pessoas jurídicas, tampouco de pessoas falecidas.

b) realizados no território brasileiro ou no exterior, se os dados pessoais forem coletados no Brasil, se eles se relacionarem a indivíduos localizados no território brasileiro ou se o tratamento tiver por objetivo a oferta de produtos e/ou serviços o público brasileiro (art. 3º).

São expressamente excluídos do âmbito de aplicação da norma as hipóteses de tratamentos listadas no art. 4º, das quais é relevante para a análise desta Nota a exceção referente às finalidades acadêmicas, a qual será detalhada mais adiante.

Merece destaque a grande abrangência dada ao conceito de tratamento de dados, que considera irrelevante o meio e/ou forma de tratamento dos dados, contemplando uma grande leque de atividades (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração), e alcançando tanto meios digitais como não digitais.

4.2. Fundamentos e princípios da LGPD

Os fundamentos da LGPD estão listados em seu artigo 2º. Todos eles remetem a interesses constitucionais que são envolvidos no tratamento de dados pessoais, alguns deles conflitantes, como a proteção à privacidade e o direito à informação.

Esses fundamentos são desdobrados em princípios (finalidade, adequação, necessidade, livre acesso aos dados por parte dos titulares, qualidade dos dados, transparência e não discriminação) no art. 6º da LGPD, claramente inspirados na GPRD. Esses princípios nada mais são do que diretrizes que devem ser consideradas no tratamento de dados pessoais e, consequentemente, na interpretação da LGPD.

A LGPD oferece uma solução legislativa de ponderação de interesses constitucionais, numa tentativa de dar maior segurança jurídica à proteção de dados pessoais.

Ressalve-se que, como a questão envolve direitos fundamentais, o regramento da LGPD

orienta mas não engessa a solução da colisão, a qual não pode ser arbitrada de forma abstrata e definitiva, sem considerar o caso concreto.

4.3. Dados pessoais e dados pessoais sensíveis

O art. 5º, I da LGPD considera dado pessoal a "informação relacionada a pessoa natural identificada ou identificável". Ou seja, para ser relevante à privacidade, a informação precisa ser pessoal, nominativa, ou seja, ela deve ser coletada de forma individual e não anônima. O titular dessa informação deve ser identificado, ou ao menos identificável. Dados não personalizados, seja pela agregação em grupos ou categorias, ou, quando individualizados, pelo anonimato, destinados exclusivamente para fins estatísticos, não afetam a esfera de intimidade.

A inexistência de identificadores comuns em informações individuais como nome, endereço, número de identidade e data de nascimento pode não ser suficiente para afastar seu caráter nominativo. Isso porque podem existir outros dados que, apesar de não serem identificadores por si mesmos, quando combinados com outros podem possibilitar a identificação do titular da informação. Por exemplo, a informação da profissão de um indivíduo não é suficiente, por si só, para identificá-lo. Contudo, se combinada com o número do CEP de sua residência e sua idade, talvez seja possível revelar sua identidade, ou ao menos limitar bastante o universo investigado.

Mas o simples fato de ser nominativa não torna a informação sensível à intimidade. Conforme Tércio Sampaio Ferreira Júnior,

> "Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc. -, condicionam o próprio intercâmbio em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a inviolabilidade da privacidade pela proteção desses dados em si, pelo sigilo, não faz sentido."[1]

Além disso, a LGPD protege com mais rigor os dados pessoais sensíveis, os quais se referem a "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". Trata-se de informações que interessam tão somente às pessoas das relações privadas ou íntimas do indivíduo, ou, em alguns casos, exclusivamente ao próprio indivíduo. Como são informações próprias da intimidade, são consideradas sensíveis, motivo pelo qual merecem proteção jurídica.

O tratamento de dados pessoais sensíveis que viole as regras de proteção à privacidade pode provocar danos materiais e morais ao seu titular. Em matéria de saúde, por exemplo, pelo conhecimento de certas doenças é possível, por exemplo, inferir sobre a sexualidade de um paciente. Essa inferência, acertada ou não, pode afetar suas relações familiares, seus relacionamentos íntimos e até mesmo sua vida profissional, especialmente no caso de pessoas públicas.

No campo do trabalho, o conhecimento do empregador sobre o estado de saúde do empregado confere subsídios ao primeiro para o controle de custos dos recursos humanos. Identificados empregados doentes ou com hábitos prejudiciais à saúde, podem os empregadores desenvolver programas de promoção e proteção à saúde para melhorar a qualidade de vida de seus funcionários e, consequentemente, reduzir o índice de absenteísmo da mão de obra. Por outro lado, também é possível que essas informações sejam utilizadas de forma abusiva na gestão dos recursos humanos, seja pela negativa da contratação de mulheres grávidas e de candidatos cujo histórico médico aponte risco de absenteísmo, seja pela demissão de funcionários de maior risco de morbidade.

Também há doenças estigmatizantes que submetem seus portadores à repulsa da sociedade como AIDS, a tuberculose e a hanseníase. Os casos citados por Anne Wells Branscomb ilustram como as vidas de pessoas infectadas pelo HIV podem ser devastadas pela revelação pública de suas condições.

Como se pode notar, a exposição de detalhes sobre a condição ou o tratamento de um

paciente pode ter impactos na vida social e profissional do paciente mais graves do que os males da própria doença. Por esse motivo, toda informação pessoal sobre saúde é classificada como informação sensível, merecendo proteção especial.

Apesar de didática, a distinção de dados pessoais sensíveis dos não sensíveis está cada vez mais menos clara em razão dos avanços na tecnologia de comunicação e informação. A coleta massiva de dados pessoais e os grandes avanços no processamento, cruzamento e análise de grandes conjuntos de dados têm permitido a inferência de informações pessoais sensíveis a partir de dados aparentemente não relacionados. O histórico de navegação e de pesquisas na Internet e curtidas em publicações nas redes sociais, por exemplo, podem indicar se uma mulher está grávida ou se uma pessoa está doente.

Possivelmente por esse motivo a LGPD protegeu qualquer tipo de dado pessoal, mesmo que não seja sensível *prima facie*.

4.4. Atores da Proteção de Dados Pessoais

A LGPD, ao tratar de direitos, obrigações, responsabilidades e atribuições na proteção de dados pessoais, menciona os seguintes atores:

a) titular - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

b) agentes de tratamento - o controlador e o operador;

c) controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

d) operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

e) encarregado - pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

f) órgão de pesquisa - órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

g) autoridade nacional - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

4.5. Hipóteses de tratamento de dados pessoais

A regra geral é a de vedação do tratamento de dados pessoais sem o expresso consentimento do titular ou de seu responsável legal, no caso de incapaz (art. 7º, I, art. 11, I e art. 14). Nisso, ela foi mais severa que os regramentos anteriores, pois estendeu essa vedação a toda e qualquer informação pessoal, não apenas a informações pessoais sensíveis.

A LGPD disciplinou com rigor à formalização do consentimento para evitar erro e vício da manifestação de vontade (art. 8º), principalmente no caso de menores de idade (art. 14, §1º).

a) hipóteses de dispensa do consentimento prévio

As hipóteses de dispensa do consentimento prévio para o tratamento de dados pessoais estão previstas no art. 7º e no art. 11º, II da LGPD. Dentre elas, a mais relevante para a ANS é a referente aos “dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" (art. 7º, III, e art. 11, II, “b”).

O artigo 23 da lei, por sua vez, estabelece os parâmetros para o tratamento de dados

pessoais pelo poder público: deve ser realizado para uma finalidade pública, norteada pelo interesse público, e com o objetivo de executar suas competências legais ou atribuições legais do serviço público. Isso abrange quase a totalidade dos tratamentos de dados pessoais pela ANS, incluindo os referentes:

- aos cadastros de beneficiários do Sistema de Informações de Beneficiários (SIB);
- aos dados assistenciais da Troca de Informações de Saúde Suplementar;
- aos dados assistenciais dos atendimentos realizados pelo SUS a beneficiários de planos privados de assistência à saúde tratados, bem como as informações e documentos apresentados pelas operadoras na defesa das cobranças dos processos de ressarcimento ao SUS;
- às informações e documentos utilizados na instrução e defesa em processos administrativos sancionadores por infrações à normas da saúde suplementar;
- às informações e documentos utilizados na instrução e defesa em processos de apuração de fraude em declaração de saúde para fins de rescisão unilateral de contrato de plano privado de assistência à saúde.

Essa hipótese é complementada pela exceção prevista no art. 7º, II, e art. 11, II, "a", que autoriza o tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador. Isso permite, por exemplo, que as operadoras de planos privados de assistência à saúde enviem para a ANS dados pessoais de seus beneficiários, o que contempla:

- os cadastros de beneficiários do Sistema de Informações de Beneficiários (SIB);
- os dados assistenciais da Troca de Informações de Saúde Suplementar.

Também relevante para os processos administrativos da ANS é a dispensa do consentimento do titular no tratamento de dados pessoais, inclusive sensíveis[2], para o "exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral" (art. 7º, VI e art. 11, II, "d"). Isso autoriza esta Agência e as entidades reguladas a trocarem dados pessoais, inclusive documentos, na instrução e defesa em processos administrativos referentes a:

- cobrança de ressarcimento ao SUS;
- apuração de infrações às normas da saúde suplementar;
- apuração de fraude em declaração de saúde para fins de rescisão unilateral de contrato de plano privado de assistência à saúde.

Sobre isso compete apontar a vedação do art. 21 à utilização em prejuízo do titular de dados pessoais coletados no exercício regular de seus direitos. Assim, não podem ser utilizados, por exemplo, dados referentes a reclamações administrativas e ações judiciais regularmente movidas pelo consumidor para criar qualquer tipo de lista restritiva, negar acesso a produtos e serviços, ou agravar as condições de contratação ou motivar a rescisão ou não renovação do contrato.

Observe-se que o compartilhamento de bases de dados entre entidades e órgãos públicos sem o consentimento do titular, desde que observada a finalidade pública, não apenas é admitida pelo art. 7º e art. 11, II, como também é estimulada pelos arts. 25 e 26. Essa hipótese cobre, por exemplo:

- o compartilhamento da Secretaria da Fazenda Nacional com a ANS da base de dados do Cadastro de Pessoas Físicas para fins de enriquecimento e melhoria da qualidade dos dados dos cadastros de beneficiários;
- o compartilhamento do DATASUS com a ANS das bases de dados do Sistema de Informações Hospitalares (SIH) e do Sistema de Informações Ambulatoriais (SAI) para processamento do ressarcimento ao SUS, e do Cartão Nacional de Saúde (CNS), para enriquecimento e melhoria da qualidade dos cadastros de beneficiários;

- o compartilhamento da ANS com o DATASUS do Conjunto Mínimo de Dados (CMD) referentes aos contatos assistenciais na saúde suplementar.

Outra exceção ao consentimento prévio, prevista no artigo 7º, IV, no artigo 11º, II, "c", é a realização de estudos por órgãos de pesquisa. A Lei não inclui nessa hipótese as entidades privadas de pesquisa, de maneira que é prudente autorizar a disponibilização desses dados apenas para órgãos e entidades públicos de pesquisa, definidos no artigo 5º, VIII. Além disso, esses dispositivos exigem, sempre que possível, a anonimização dos dados pessoais.

Também merece destaque a dispensa de consentimento do titular no caso de tratamento de dados pessoais para tutela à saúde (artigo 7º, VIII e artigo 11º, II, "f"), desde que "exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

A expressão "serviços de saúde" foi incluída por alteração feita pela Lei nº 13.853, de 2019, claramente contemplando gestores públicos e privados de saúde, como as operadoras de planos privados de assistência à saúde, não apenas no atendimento assistencial, mas também na gestão do cuidado.

Já a expressão "autoridade sanitária" indica que a exceção não se limita à tutela da saúde individual, alcançando também a saúde pública. Apesar de não haver exigência expressa de regulamentação desses dispositivos, para reduzir a insegurança jurídica quanto à matéria, é necessário detalhamento maior das hipóteses de subsunção e da forma e das condições para tratamento de dados na tutela à saúde.

É possível, portanto, vislumbrar que são admitidos os seguintes tratamentos de dados sem o consentimento do titular:

- compartilhamento de registros de saúde com os médicos assistentes e outros prestadores de serviços de saúde para melhorar o cuidado e o resultado em saúde para o paciente;
- utilização de informações de saúde por gestores de sistemas de saúde públicos ou privados para a condução de programas de promoção de saúde e de prevenção de doenças, bem como para o direcionamento dos pacientes para prestadores mais adequados para seus quadros;
- comunicação à autoridade sanitária de suspeita ou confirmação de doença ou agravo e eventos de saúde pública, como acidentes de trabalho, doenças infecto-contagiosas, violência doméstica etc;
- utilização de informações pessoais de saúde pela ANS para subsidiar a formulação de políticas públicas de melhoria do modelo assistencial, bem como para servir de insumo para o monitoramento técnico-assistencial das operadoras, de modo a permitir que a Agência identifique anomalias e intervenha para assegurar a continuidade e a qualidade do cuidado.

Cabe atentar para o inciso IX do art. 7º, o qual dispensa o consentimento do titular "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Trata-se de exceção "guarda-chuva", que abarca todas as demais hipóteses não previstas expressamente na LGPD, de modo que o rol do art. 7º é meramente exemplificativo.

b) hipóteses de tratamento dados pessoais sensíveis

As hipóteses de tratamento de dados pessoais sensíveis estão previstas no art. 11 da LGPD. Apesar de quase todas serem idênticas ao rol do art. 7º, referente aos dados pessoais não sensíveis, há uma diferença marcante – os dados pessoais sensíveis não se enquadram "guarda-chuva" do art. 7º, IX, de maneira que se pode entender que o art. 11 é taxativo, não admitindo outras exceções além daquelas expressamente relacionadas.

Dos dados pessoais sensíveis, a LGPD é ainda mais rigorosa em relação aos dados pessoais de saúde, proibindo, no art. 11, §4º, seu uso e compartilhamento com objetivo de obter

vantagem econômica. Esse dispositivo é reforçado pelo art. 11, §5º, o qual veda expressamente o emprego de dados pessoais de saúde por operadoras de planos privados de assistência à saúde para a práticas discriminatórias de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Por outro lado, pode-se observar no §4º do art. 11 o cuidado em não inviabilizar o mercado de atenção à saúde. Esse dispositivo ressalvou da vedação os casos de prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, para permitir a portabilidade dos dados quando solicitada pelo titular e para as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de assistência à saúde.

Destaque-se que quase a totalidade dos tratamentos de dados pessoais pela ANS (SIB, TISS, Ressarcimento ao SUS, processos sancionadores, processos de apuração de fraude em declarações de saúde e outros) contêm dados sensíveis que, embora dispensados de consentimento prévio, exigem requisitos adicionais de ética e segurança previstos no artigo 13, como a vedação da revelação de dados pessoais na divulgação dos resultados, do compartilhamento dos dados com terceiros, do tratamento dos dados pessoais fora do ambiente controlado e seguro do órgão ou para finalidades que não a realização de estudos e pesquisas. Esses requisitos, por sua vez, deverão ser regulamentados pela ANPD e pelas autoridades da área de saúde e sanitárias (artigo 13, §3º), dentre as quais se inclui a ANS.

4.6. **Direitos do titular**

Além do direito do titular à liberdade negativa de não tratamento de seus dados pessoais sem seu expresso consentimento, a LGPD não apenas reafirmou e ampliou direitos já previstos no Código de Defesa do Consumidor (acesso e correção de informações pessoais em bancos de dados de fornecedores) e na Constituição Federal (*habeas data*), bem como previu proteções adicionais.

O titular tem o direito de acessar informações sobre o tratamento de seus dados, disponibilizadas de forma clara, adequada e ostensiva, como a finalidade específica do tratamento, a forma e a duração do tratamento, a identificação do controlador, as informações de contato do controlador, as informações acerca do uso compartilhado de dados pelo controlador e a finalidade, as responsabilidades dos agentes que realizarão o tratamento, os direitos do titular e os meios para exercício de seus direitos (art. 9º).

O titular também tem direito de obter do controlador, mediante requisição:

a) a revogação do consentimento do tratamento de dados, por procedimento gratuito e facilitado (art. 8º, §§ 5º e 6º, e art. 18, IX);

b) a confirmação da existência de tratamento (art. 18, I) no prazo de 15 dias (art. 19, II);

c) o acesso aos dados (art. 18, II) em meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa (art. 19, §2º);

d) a correção de dados incompletos, inexatos ou desatualizados (art. 18, III);

e) a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV);

f) a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (art. 18, V);

g) a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 (art. 18, VI);

h) a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);

i) a informação sobre a possibilidade de não fornecer consentimento e sobre as

consequências da negativa (art. 18, VII);

j) solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

4.7. **Obrigações e responsabilidades dos agentes de tratamento de dados**

A LGPD criou diversos deveres, obrigações e responsabilidades para os agentes de tratamento de dados.

Os deveres e das obrigações mais básicos do controlador correspondem aos direitos e garantias dos titulares dos dados pessoais. Assim, o controlador deve:

a) dar publicidade às informações sobre tratamento de dados previstas no art. 9º e no art. 14, §2º;

b) disponibilizar meios de receber, processar e atender às requisições dos titulares de dados pessoais tratadas no art. 18.

Além dessas, o controlador tem o dever de:

a) indicar o encarregado pelo tratamento de dados pessoais (art. 41, *caput*);

b) divulgar publicamente a identidade e as informações de contato do encarregado (art. 41, §1º)

c) juntamente com o operador, manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (art. 37);

d) quando solicitado pela ANPD, elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (art. 38);

e) fornecer ao operador instruções sobre o tratamento de dados, observando as normas sobre a matéria (art. 39);

f) juntamente com o operador, adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 46), mesmo após o término do tratamento (art. 47), inclusive adotando sistemas conformados aos requisito de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares;

g) juntamente com o operador e com qualquer pessoa que intervenha em qualquer fase do tratamento, garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o término do tratamento (art. 47);

h) conjuntamente com o operador, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (art. 50);

i) no caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, comunicar a ocorrência do incidente à ANPD e ao titular e adotar as providências determinadas pela ANPD (art. 48).

Adicionalmente às obrigações já mencionadas acima, o operador tem o dever de realizar o tratamento segundo as instruções fornecidas pelo controlador (art. 39).

Em relação ao dever de reparar dano causado no exercício de atividade de tratamento de dados pessoais em violação à legislação de proteção de dados pessoais:

a) o operador é responsável solidário sempre que descumprir a legislação de proteção de dados ou quando não observar instruções lícitas do controlador (art. 42, § 1º, I);

b) os controladores são responsáveis quando diretamente envolvidos no tratamento de dados (art. 42, § 1º, II).

A responsabilidade do agente de tratamento somente é afastada quando provado:

a) que não realizaram o tratamento de dados pessoais (art. 43, I);

b) que não houve violação à legislação de proteção de dados (art. 43, II); ou

c) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (art. 43, III).

Pessoas jurídicas de direito público têm obrigações em comum com os demais agentes de tratamento, como de dar publicidade às atividades de tratamento de dados (art. 23, I) e nomear encarregado (art. 23, III).

Há, contudo, alguns deveres e obrigações específicos das entidades e órgãos públicos, como:

a) no atendimento das requisições dos titulares de dados pessoais, o observar os procedimentos e prazos previstos em legislação específica (art. 23, § 3º), em especial na Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

b) manter os dados pessoais 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);

c) comunicar à ANPD contratos e convênios celebrados com entidades privadas que envolvam a transferência de dados pessoais constantes de suas bases de dados (art. 26, § 2º);

d) informar à ANPD e ao titular a comunicação ou o uso compartilhado de dados pessoais, ressalvadas as exceções previstas na LGPD (art. 27);

e) atender às solicitações da ANPD de realização de operações de tratamento de dados pessoais, de informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado;

f) cumprir as medidas determinadas pela ANPD para fazer cessar a violação à LGPD (art. 31).

4.8. **O papel da ANPD e demais autoridades reguladoras**

A LGPD concede à ANPD atribuições de regulamentação da LGPD (art. 11, §3º, art. 12, §3º, art. 13, §3º, art. 18, *caput*, V, art. 19, §§3º e 4º, art. 23, §1º, art. 27, par. Único, art. 30, art. 35, art. 40, art. 41, §3º, art. 46, §1º, art. 53), orientação e fomento (art. 4º, §3º, art. 29, art. 32, art. 33, par. único, art. 50, §3º, art. 51), monitoramento e fiscalização (art. 4º, §2º, art. 10, §3º, art. 15, IV, art. 18, § 1º, art. 20, §2º, art. 26, § 2º, art. 27, art. 29, art. 31, art. 32, art. 33, V, art. 34, art. 35, §§2º, 3º e 4º, art. 36, art. 38, art. 48, art. 52).

A Lei traz como uma das competências da ANPD, “articular-se com as autoridades

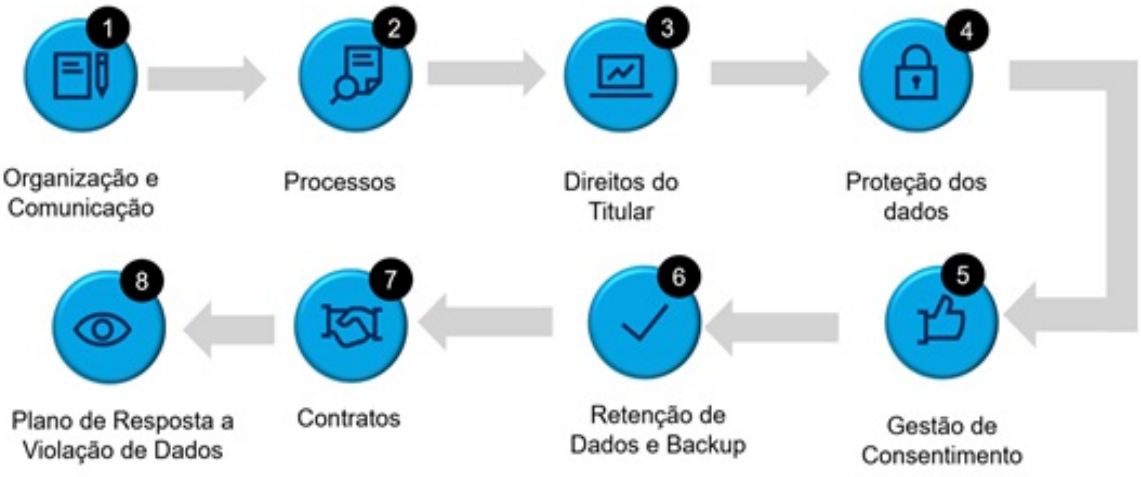
reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;" (artigo 55°-J, XXIII). Os parágrafos 3° e 4° desse mesmo artigo tratam do relacionamento entre a ANPD e os órgãos e entidades reguladores setoriais, sem estabelecer preponderância entre eles. Esses dispositivos indicam que, nas matérias em que houver sobreposição de atribuições, a ANPD deverá atuar de forma colaborativa com os demais atores reguladores. Assim, os eventuais conflitos de competência devem ser resolvidos por meio de comunicação, coordenação e cooperação.

5. ADEQUAÇÃO DA ANS E DA REGULAÇÃO DA SAÚDE SUPLEMENTAR À LGPD

5.1. Requisitos para aplicação da LGPD na saúde suplementar

Para que as instituições estejam aptas ao cumprimento da LGPD, a partir de sua vigência em agosto de 2020, são necessários requisitos de ordem organizacional e tecnológicos.

A figura abaixo ilustra o passo-a-passo da implementação do Plano de Ação desenhado pelo *Gartner*:



Fonte: © 2019 Gartner, Inc. and/or its affiliates. All rights reserved.

As etapas apresentadas na figura são descritas a seguir:

1. ***Organização e Comunicação***
   - *Nomear o Oficial de Proteção de Dados (DPO).*
   - *Identificar as funções da própria organização e dos parceiros: Controladores de Dados / Processadores de dados.*
   - *Estabelecimento de padrões mínimos para um Projeto de Governança da Informação e Proteção de Dados.*
   - *Divulgação em veículos de fácil acesso a finalidade, práticas de execução e previsão de tratamento de dados públicos. Indicação de Encarregado da função para tal.*
   - *Criar novo aviso de privacidade e publicar (externamente).*
   - *Criar nova Política de Privacidade e publique (internamente).*
2. ***Processos***
   - *Mapeamento dos processos de trabalho que envolvam tratamento de dados pessoais e dados pessoais sensíveis, identificando o fluxo desses dados, a tecnologia utilizada, onde são armazenados e as pessoas envolvidas.*
   - *Identificar quais dados pessoais são processados em qual processo de negócios.*
   - *Motivar processos de dados pessoais ("propósito de processamento") para cada processo de negócios.*

- *Criar ou alterar o processo de avaliação de impacto da privacidade.*
- *Criar ou alterar o processo de avaliação de risco.*
- *Realizar avaliações de risco e privacidade para identificar lacunas iniciais*
- *Determinar e documentar fundamentos legais para processamento.*
- *Criar rotina para caso a autoridade nacional faça requisição de relatório. O controlador deverá inserir no, no mínimo, as seguintes informações:*
  - *Descrição dos tipos de dados coletados;*
  - *Metodologia utilizada para a coleta de dados;*
  - *Metodologia utilizada para garantir a segurança das informações;*
  - *Análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.*

3. ***Direitos do Titular***
   - *Definição de mecanismos e garantias de Compliance com princípios e direitos do titular, conforme previsto em Lei.*
   - *Desenvolver Plano de Contingência em caso de incidente envolvendo dados pessoais que possa implicar em risco ou danos relevantes aos titulares.*
   - *Definir fluxo institucional e regramento interno para confirmação ou providências para o acesso e retificação de dados pessoais, mediante requisição do titular, em formato simplificado ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até 15 (quinze) dias.*
   - *Criar portal de autoatendimento onde os sujeitos de dados podem executar ações para executar seus direitos.*
   - *Garantir que os detalhes de contato do DPO estejam disponíveis para todos os assuntos de dados.*
4. ***Proteção dos Dados***
   - *Rever o armazenamento atual de dados pessoais.*
   - *Remover quaisquer dados pessoais que não atendam aos critérios de finalidade de processamento (incluindo Backups).*
   - *Registrar as assinaturas dos proprietários do processo de negócios, indicando que seu processo é totalmente compatível.*
   - *Realizar uma avaliação de risco se apropriado.*
   - *Indicar Encarregado pelo tratamento dos dados pessoais, divulgando publicamente, de forma clara e objetiva, preferencialmente no seu sítio eletrônico, a identidade da pessoa e suas informações de contato. Em linhas gerais, as atividades do encarregado consistem em:*
     - *Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*
     - *Receber comunicações da autoridade nacional e adotar providências;*
     - *Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;*
     - *Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares emitidas pela autoridade nacional de proteção de dados;*
     - *Criar rotinas de registro das operações de tratamento de dados pessoais que realize, podendo a autoridade nacional determinar que seja elaborado relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações.*
5. ***Gestão de Consentimento***
   - *Identificar todos os pontos de contato em que o consentimento dos dados é obtido.*
   - *Identificar processos para os quais é necessário o consentimento.*

- *Identificar controladores de dados e processadores envolvidos com dados para os quais é necessário o consentimento.*
- *Revisar o gerenciamento de consentimento – se existente - no site e adaptar a LGPD.*
- *Revisar a gestão de consentimento existente em formulários em papel e adaptar a LGPD.*
- *Criar repositório para gerenciamento de consentimento para garantir que o ônus da prova possa ser facilitado.*

6. ***Retenção de Dados e Backup***
   - *Revisar os requisitos de retenção de dados existentes.*
   - *Revisar os processos de backup existentes.*
   - *Alterar as políticas de retenção de dados e os processos de backup.*
   - *Remover todos os dados pessoais existentes em backups existentes.*
7. ***Contratos***
   - *Criar acordos controlador-processador onde ainda não estão em vigor.*
   - *Atualizar os acordos do controlador-processador: uso intencional e requisitos de segurança.*
   - *Atualizar outros acordos existentes, quando aplicável.*
   - *Atualizar o processo de aquisição: critérios de seleção para novos serviços.*
   - *Atualizar o processo de aquisição: novos requisitos incluídos em novos contratos.*
8. ***Plano de Resposta a Violação de Dados***
   - *O controlador responde solidariamente com o operador se, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à LGPD.*

No próximo item faz-se a sugestão de planos de ação com base no modelo acima descrito, porém adaptado às particularidades institucionais da ANS.

5.2. Proposta para implementar os requisitos da LGPD na ANS

Na hipótese de a ANS ser enquadrada como Controlador, identifica-se uma série de obrigações trazidas pela Lei, em especial a observância dos princípios gerais (art. 6º) e a garantia de direitos do titular.

Com base na metodologia proposta pelo *Gartner*, observa-se que uma grande parte das ações a serem implementadas não competem à GEPIN. Todavia, como o debate sobre os impactos da LGPD tem ocorrido no âmbito da DIDES, foi elaborada proposta de Planos de Ação para implementar a LGPD na instituição, que seguem anexos a esta nota.

A proposta dos Planos de Ação considera a abrangência da lei e o possível impacto em diversas unidades da ANS, bem como no setor regulado. Por esta razão, são propostos dois Planos de Ação 1) dos impactos da LGPD na dimensão institucional (14820595); 2) dos impactos da LGPD nas obrigações do regulado (14820660);

O Plano de Ação da dimensão institucional teve como base o modelo do*Gartner*, porém, adaptado às particularidades institucionais da ANS e mais sintético - o que permite melhor acompanhamento – e tem o objetivo de estabelecer etapas e responsabilidades para implantação dos requisitos da LGPD para que a ANS esteja apta a cumprir a lei a partir da data de sua vigência (agosto 2020).

O Plano de Ação para as obrigações do regulado tem o objetivo de promover as adequações necessárias das regras de envio de informações obrigatórias para a ANS para atender aos requisitos da LGPD.

Importante destacar que os prazos e responsabilidades sugeridos são hipotéticos e necessitam da discussão com os órgãos técnicos competentes, tanto no que diz respeito aos prazos e

responsabilidades, quanto nas etapas descritas.

Para garantir que as ações sejam sinérgicas, é importante que as responsabilidades que foram atribuídas a instâncias colegiadas como CT e SGODITI tenham uma coordenação única que, propõe-se, seja de competência do Oficial de Proteção de Dados (DPO) [3].

5.3. Encaminhamentos propostos

Conforme demonstrado, há uma série de requisitos, definições e providências que necessitam ser tomadas antes da entrada da lei em vigência. Considerando grande parte das ações e medidas a serem adotadas estão além das competências da GEPIN isoladamente, sugere-se:

a) submeter à análise jurídica, da Procuradoria Federal junto à ANS, os entendimentos firmados nesta nota, especialmente quanto ao enquadramento da Agência como agente de tratamento (Controlador);

b) articular-se com a Casa Civil da Presidência da República para identificar previamente as competências que serão atribuídas à Autoridade Nacional de Proteção de Dados (ANPD) no que tange ao alinhamento de suas competências e ações a serem implementadas em conjunto com a ANS, no âmbito do Setor de Saúde Suplementar;

c) por analogia, nomear para a função de Oficial de Proteção de Dados (DPO) a mesma autoridade que cumpre a responsabilidade definida no art. 40 da Lei 12.527/2011 (LAI) e estendida para a Política de Dados Abertos;

d) considerando as competências regimentais da GGATP/PRESI, estabelecer esta unidade como responsável pelo processo de implementação da LGPD na ANS com finalidade de coordenar as ações nas múltiplas diretorias e:

e) pautar discussão no SGODITI para alinhamento técnico dos Planos de Ação, especialmente, as etapas e prazos descritos;

f) pautar para deliberação no CT o cronograma e as responsabilidades pela coordenação e execução do Projeto de Implementação da LGPD;

g) coordenar e monitorar o projeto de implementação da LGPD.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BRANSCOMB, Anne Wells. Who Owns Information: from privacy to public access, USA: BasicBooks, 1994.

CARVALHO, Luiz et al. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. In: **Anais do VII Workshop de Transparência em Sistemas**. SBC, 2019. p. 21-30.

CORRÊA, Adriana Espíndola. Lei de Proteção de Dados e a identificação nacional: há antinomias. **Revista Consultor Jurídico. Disponível em https://www. conjur. com. br/2019-fev-18/direito-civil-atual-lei-protecao-dados-identificacao-nacional-antinomias# sdfootnote2sym. Acesso em: Em**, v. 18, 2019.

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho de 27 de abril de 2016.

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

DUARTE, Natália Bento Mendes. **Proteção de dados pessoais na área da saúde no Brasil**. 2018.

FERRAZ JR., Tercio Sampaio. Direito constitucional: liberdade de fumar, privacidade, Estado, direitos

humanos e outros temas. Barueri: Manole, 2007.FONTES JR., João Bosco Araújo. Liberdades Fundamentais e Segurança Pública – Do Direito à Imagem ao Direito à Intimidade: a garantia constitucional do efetivo estado de inocência. Rio de Janeiro: Lúmen Juris Editora, 2006.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

LEI Nº 13.853, DE 08 DE JULHO DE 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018.

NETTO, Clovis Armando Alvarenga et al. A Janela de Johari como ferramenta de análise da privacidade de dados pessoais. **Ciência da Informação**, v. 48, n. 1, 2019.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (1980), version revised http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf 2013.

PAIXÃO, Pedro. Proteção de dados na América Latina. In: https://cio.com.br/protecao-de-dados-na-america-latina/ de 10 de julho de 2018.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) de 27 de abril de 2016.

SAMPAIO, José Adércio Leite. O direito à intimidade e à vida privada – uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte, Belo Horizonte, Del Rey, 1998.

VIGNOLI, Richele Grenge; VECHIATO, Fernando Luiz. Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação. 2019.

[1] Direito Constitucional – Liberdade de fumar, Privacidade, Estado, Direitos Humanos e outros temas, p. 174.

[2] Será abordado no próximo item a caracterização de "dados pessoais sensíveis" e as vedações relacionadas ao tratamento deste tipo de dado

[3] O Oficial de Proteção de Dados (DPO - *Data Protection Officer*) na instituição, terá como principal atividade o monitoramento e disseminação das boas práticas em relação à proteção de dados pessoais perante funcionários e contratados no âmbito da empresa, assim como será a interface com a Autoridade Nacional de Proteção de Dados (ANPD), criada em dezembro/2018.

Documento assinado eletronicamente por **MIRELLA JORDAO AMORIM**, **Especialista em Regulação de Saúde Suplementar**, em 21/11/2019, às 16:30, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **FREDERICO YASUO NORITOMI**, **Coordenador(a) de Análise e Informações Estratégicas**, em 21/11/2019, às 16:41, conforme horário oficial de

Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Celina Maria Ferro De Oliveira**, **Gerente de Padronização, Interoperabilidade e Análise de Informação**, em 21/11/2019, às 16:55, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Cristiano Dos Reis Moura**, **Especialista em Regulação de Saúde Suplementar**, em 21/11/2019, às 17:05, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **RODRIGO RODRIGUES DE AGUIAR**, **Diretor(a) de Desenvolvimento Setorial**, em 21/11/2019, às 17:25, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **DANIEL MEIRELLES FERNANDES PEREIRA**, **Diretor(a)-Adjunto(a) da DIDES**, em 21/11/2019, às 17:25, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539/2015.

A autenticidade deste documento pode ser conferida no site https://www.ans.gov.br/sei/autenticidade, informando o código verificador **14815937** e o código CRC **E9E6CCE0**.

Referência: Processo nº 33910.029786/2019-51 SEI nº 14815937