PROTEÇÃO DE DADOS DE SAÚDE: GOVERNANÇA E BOAS PRÁTICAS NA LGPD À LUZ DAS NORMAS DA ANPD (2024) EM CONTRAPONTO A NORMATIVA EUROPEIA (GDPR)

HEALTH DATA PROTECTION: GOVERNANCE AND GOOD PRACTICES IN THE LGPD IN LIGHT OF ANPD REGULATIONS (2024) AS A CONTRAST TO EUROPEAN REGULATIONS (GDPR)

Carlos Alexandre Lorga[321]

Caroline Alessandra Taborda dos Santos Dallegrave[322]

[321] Doutorando em Direito, Universidade de Coimbra, Portugal, Mestre em Direito, Unicuritiba, Pós-graduado em Direito Civil e Empresarial, PUC-PR. Pós-graduado em Direito Socioambiental, PUC-PR. Advogado sócio da Lorga Sociedade de Advogados, Curitiba, Paraná, Brasil.

[322] Mestre em Direito Empresarial e Cidadania pelo Unicuritiba. Pós-Graduada em Direito Aplicado pelo EMAP/PR. Especialista em Direito Administrativo pelo Instituto de Direito Romeu Felipe Bacellar, Mediadora Extrajudicial pelo ABRAME, Advogada sócia do Taborda Advocacia.

A Lei Geral de Proteção de Dados dedica uma parte da norma às boas práticas e governança. Induz que controladores e operadores responsáveis na cadeia de tratamento de dados implementem um programa de governança em privacidade. A forma de executar tais tarefas vem sendo regulamentada pela Autoridade Nacional de Proteção de Dados Pessoas, por meio de Resoluções. A proposta de abordar o tema é avaliar aspectos desta ferramenta (programa de governança em privacidade) no tratamento de dados de saúde. O leitor poderá refletir sobre a utilidade, segurança e prevenção visando o alinhamento dos princípios da norma para a proteção de dados de saúde, assim como as recentes regulamentações pela ANPF e compará-los com o tratamento dado pelo Regulamento Geral de Proteção de Dados na União Europeia em alguns aspectos.

PALAVRAS-CHAVE:LGPD. Dados sensíveis. Saúde. Governança. ANPD.

The General Data Protection Law dedicates a part of the standard to good practices and governance. It requires controllers and operators responsible for the data processing chain to implement a privacy governance program. The way to perform such tasks has been regulated by the National Data Protection Authority, through Resolutions. The purpose of addressing the topic is to evaluate aspects of this tool (privacy governance program) in the processing of health data. The reader will be able to reflect on the usefulness, security and prevention aiming at aligning the principles of the standard for the protection of health data, as well as the recent regulations by the ANPF and compare them with the treatment given by the General Data Protection Regulation in the European Union in some aspects.

KEYWORDS: LGPD; Sensitive data; Health; Governance;. ANPD

INTRODUÇÃO

A proteção de dados pessoais tem natureza de direito fundamental. Esta é a dimensão estabelecida na Europa. A Carta Europeia de Direitos Fundamentais (CEDF) dedicou o art. 8º a este tema. O Tribunal de Justiça da União Europeia ressalta a proteção de dados com esta magnitude. Os potenciais usos dos dados pessoais pauta a tutela legal inerente ao seu tratamento[323]

As normas sobre o tema, em comum, apontam para que os dados pessoais devem ter um *tratamento leal*, com *fins específicos*, e *consentimento da pessoa* ou *na forma prescrita em lei*. Às pessoas é garantido o acesso aos seus

323 Pereira, Alexandre L. Dias. 2018. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29, 51-70. Com grande propriedade o Autor afirma que : "Na jurisprudência afirma-se a proteção dos dados pessoais como projeção do direito fundamental à "autodeterminação informacional"(7)(Acórdão do Supremo Tribunal de Justiça, Acórdão de 16 de outubro de 2014, proc. 679/05. Todavia, o regime dos dados pessoais é marcado igualmente por exigências de bom funcionamento do mercado interno. Com efeito, a Diretiva 95/46 afirma a liberdade de circulação de dados como ferramenta das quatro liberdades do mercado interno (pessoas, mercadorias, serviços e capitais), respeitando os direitos fundamentais das pessoas segundo o princípio do "elevado nível de proteção"".

dados colhidos e de exigir a retificação se preciso. Também preveem as normas a existência de uma autoridade independente investida na competência de fiscalização no cumprimento das obrigações legais, zelando pelo tratamento de dados pessoais ocorra conforme o alcance da garantia fundamental, sob pena de imposição de sanções.

Na Constituição da República de Portugal (CRP) o art. 35º dedica-se à proteção de dados no campo dos Direitos, Liberdades e Garantias Pessoais. Tal qual a Carta Europeia (CEDF) a Constituição Portuguesa contempla semelhantes pressupostos para a proteção do direito fundamental da proteção de dados. Há explícita preocupação na CRP na utilização da informática[324].

A Lei nº 58/2019, no papel de amoldar a proteção dos dados pessoais aos ditames da Constituição e ao Regulamento Geral de Proteção de Dados UE é o marco legal português equivalente ao novel marco legal brasileiro neste tema.

Apenas com a Emenda Constitucional 115/2022 é que a Constituição da República Federativa do Brasil (CRFB) passou a contemplar de forma expressa a *proteção de dados* entre os direitos e garantias fundamentais. No entanto, tal fato não a diminuía, visto o entendimento, até então de que esta garantia fundamental era inerente a *intimidade privada* e da *inviolabilidade de dados* prevista nos incisos X e XII do art. 5º. E foi derivada destas duas garantias da CRFB que a proteção de dados era detalhada em norma infraconstitucional, a Lei Geral de Proteção de Dados, até que com a Emenda 115/2022 foi incluída no inc. LXXIX, do art. 5º da CRFB e passou a ser expressamente reconhecida como tal, não deixando mais brechas para possíveis interpretações.

A Lei nº 13.709/2018, alterada pela Lei nº 13.853/2019 entrou em vigor de forma fracionada, sendo que os artigos que tratavam da criação da Autoridade Nacional de Proteção de dados passaram a vigorar em 28/12/2018, os demais artigos, com exceção dos que tratavam das sanções administrativas, passaram a vigorar em 18 de setembro de 2020 e, a os artigos que tratavam das sanções administrativas entraram em vigor em 1º de agosto de 2021[325].

Em se tratando de *boas práticas* e *governança*, foi a partir de 2024 que a Autoridade Nacional de Proteção de Dados (ANPD) editou normas importantes sobre o tema. A Resolução CD/ANPD nº 15/2024 dispõe sobre o regulamento de comunicação de incidentes de segurança com

324 Art. 35º. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis

325 https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd Acesso em 06 abril 2025.

dados pessoais, trazendo critérios objetivos, como o risco ou dano relevante aos titulares, o volume de dados afetados e o tempo de exposição. Essa resolução exige, por exemplo, que a comunicação ao titular e à ANPD seja feita em até três dias úteis da ciência do incidente, com detalhamento do ocorrido e medidas adotadas.

Já a Resolução CD/ANPD nº 18/2024 trata do regulamento de transferência internacional de dados pessoais, permitindo a adoção de cláusulas-padrão contratuais aprovadas pela ANPD, além de instrumentos jurídicos específicos, como cláusulas aditivas e regras corporativas globais *(binding corporate rules*), com especial importância para prestadores de serviços de saúde que operam com tecnologia estrangeira.

A Resolução CD/ANPD nº 19/2024, por sua vez, disciplina o modelo de programa de governança em privacidade, detalhando seus requisitos obrigatórios, como a adoção de políticas internas, a indicação de encarregado, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), o compromisso com o princípio da responsabilidade e prestação de contas e a demonstração de boas práticas.

O tratamento de dados de saúde exige cautelas adicionais e conformidade com o artigo 11 da LGPD, que impõe condições específicas para a coleta e utilização desses dados, exigindo consentimento livre, informado e destacado, ou enquadramento em hipóteses legais específicas como tutela da saúde ou cumprimento de obrigação legal.

Nesse contexto, torna-se indispensável a adoção de programas de governança estruturados conforme as novas diretrizes da ANPD, garantindo mecanismos de segurança, mitigação de riscos e responsabilização. Protocolos específicos em unidades de saúde, controle de acesso, anonimização, níveis de classificação e certificações são exemplos práticos de medidas que devem compor esse programa.

A construção de um ambiente normativo robusto para dados de saúde reforça o direito à intimidade e à autodeterminação informativa dos cidadãos, promovendo segurança jurídica às instituições de saúde e conformidade com os padrões internacionais.

Tais regras abrangeriam as condições de organização, o regime de funcionamento, os procedimentos, reclamações e petições dos titulares de dados, normas de segurança, padrões técnicos, obrigações específicas aos envolvidos no tratamento de dados, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e demais aspectos do tratamento de dados pessoais.

Pretende o presente estudo avaliar peculiaridades específicas inerente a implementação de regras de *boas práticas* e de *governança* no tratamento de dados de saúde, segundo o enfoque dos princípios trazidos na LGPD e das normas da ANPD, trazendo destaques parametrizados pelo Regulamento Geral de Proteção de Dados da União Europeia.

1 ASPECTOS GERAIS DAS NORMAS SOBRE PROTEÇÃO DE DADOS E TRATAMENTO.

As normas legais no campo da proteção de dados trazem, dentre outras similaridades, a obrigação do tratamento *lícito*, *leal* e *transparente*, com *fins específicos*, *adequados* e *exatos*, obtidos com *consentimento* (especialmente em dados de saúde), com *segurança*, e outros *princípios* e *subprincípios derivados*.

Alexandre Sousa Pinheiro[326] entende que os *fins específicos* devem compatibilizar-se as várias funções da proteção de dados. Esta compatibilização, a nosso ver, tem importante função de proteção:

"*O princípio da finalidade desempenha várias funções dentro do direito da proteção de dados. Por um lado garante que a recolha de informação não é "cega" às suas consequências. Ou seja, os tratamentos de dados pessoais só podem verificar-se quando uma situação ou um conjunto de situações fáticas o justificar. (...) Dentro de um determinado tratamento de dados, a recolha deve limitar-se aos elementos necessários para a prossecução da finalidade, verificando-se uma verdadeira economia de dados. Quanto a nós, o princípio da finalidade desempenha um forte elemento fiscalizador da legitimidade do tratamento".*

Conectada à finalidade da coleta e tratamento de dados o *consentimento* mereceu especial atenção na medida em que está intrínseco ao direito personalíssimo à *intimidade privada*.

O *consentimento* (art. 4º, nº 11 GDPR) consiste em "*uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*.

Na LGPD (art. 5º, XII) a norma brasileira se mostra mais sintética, porém, equivalente. Confere ao *consentimento* como sendo uma "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*."

O item 32 das "Considerações" no GDPR[327] evidencia que o silêncio, opções pré-validadas ou a omissão não constituem uma forma de

326 Pinheiro, Alexandre Sousa. 1º semestre de 2018. "Apresentação do regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral de Proteção de Dados (GDPR)." Revista do Centro de Estudos Judiciários, 303-327. (Pinheiro 313)

327] (EUR-LEX, União Europeia) item (32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.

consentimento. Então, de fato, podemos destacar entre a norma brasileira e o regulamento europeu esta sensível diferença. O regulamento europeu mostra-se mais determinado no sentido de o *consentimento* ser específico, reforçando que o ato tem que ser inequívoco, exemplificando o seu alcance. Quanto a este ponto a norma brasileira deixa margem a interpretações a serem dirimidas quando da aplicação da norma, o que merece crítica, considerando a sensibilidade da *intimidade privada*.

Contudo, a Lei Brasileira traz em outras 36 oportunidades, dentro do texto legal, a forma de como este consentimento deve ser aplicado. E, de forma específica na área da saúde, tal consentimento não será exigido, desde que o tratamento do dado seja indispensável para: art.11, 'f'. *tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.*

André Gonçalo Dias Pereira[328] busca tratar a *intimidade privada* como:

"... *o controlo de informação sobre a vida privada. O interesse que visa proteger é o interesse em controlar a tomada de conhecimento, a divulgação ou simplesmente a circulação de informação sobre a vida privada – isto é, genericamente, sobre os factos, comunicações ou posições sobre ou próximos do indivíduo ou confidenciais ou reservados -, bem como o interesse na subtracção à atenção dos outros (anonimato lato sensu), ou interesse na solidão (na exclusão do acesso físico dos outros à pessoa)".*

O raciocínio aqui compartilhado reforça que o *consentimento* é um dos elementos indispensáveis no ato de disposição de vontade. A *intimidade privada* é indissociável do controle de informações do indivíduo. O status de garantia fundamental da proteção de dados não se alcança sem ato inequívoco e específico de manifestação livre de vontade e antecipada de informações suficientemente claras sobre a finalidade e alcance do tratamento de dados a ser executado. Ressalvadas as hipóteses que dispensam o consentimento, ante o sopesar dos princípios constitucionais e a própria proteção à vida, como são as hipóteses descritas no inc. II do art. 11 da LGPD.

Mais aspectos gerais comuns nas normas pesquisadas foram evidenciados no que diz respeito à privacidade inerente a proteção de dados. A privacidade e a proteção de dados, tem relação com outros valores fundamentais. A dignidade, a integridade e autonomia. Esta última como expressão do consentimento revela importante consideração no campo da proteção de dados, portanto, orbitando em torno da tutela

[328] Pereira, André Gonçalo Dias. Direitos dos Pacientes e Responsabilidade Médica. Coimbra: Coimbra Editora, 2015.(A. G. Pereira, Direitos dos Pacientes e Responsabilidade Médica 627)

dos direitos fundamentais da liberdade e da privacidade.

Nesta essência pujante de valores jurídicos mostra-se essencialmente relevante a discussão de um modelo de *boas práticas* e de *governança* em privacidade e tratamento de dados merecendo aprimoramento constante para a real utilidade da tutela da proteção de dados. E, nestes aspectos, é que as recentes normas regulamentarem da ANPD devem ser analisadas e aplicadas.

2 PROTEÇÃO DE DADOS

2.1. Dados

O dado é o estado inicial, ou podemos atribuir, é a informação sem tratamento, pois isoladamente não acresce conhecimento. No entanto, tratado ou não, os dados estão no domínio da categoria dos direitos da personalidade[329] compondo elemento extrapatrimonial intrínseco da pessoa individual, e dela, para o coletivo. O dado em si desdobra-se em informações com diversas finalidades, tais como, identificação pessoal, suas características, seu meio social, etc.

2.2. Conceito de Dados Pessoais para a Proteção de Dados

Vivemos em uma *sociedade da informação*[330]. A informação, por si, começa a ganhar sentido na coleta, armazenamento e, especialmente, quando do tratamento de dados, sem os quais, torna-se vazia e sem utilidade.

Em nossos tempos toma relevância no desenvolvimento da economia como reflexo da *(re)evolução social*, decorrendo, assim, a necessidade do estabelecimento de regras que visem a proteção do indivíduo e dos grupos, e essas regras devem afetar especialmente a quem seja responsável pelo tratamento de dados.

Bem por isso que os direitos da personalidade gozam de garantia fundamental. Surge desde antes do nascimento e se estendem mesmo após a morte. Constituem-se em objeto de direitos subjetivos. O ordenamento jurídico, nos mais variados diplomas, busca a proteção de interesses da personalidade. Objetivam a proteção e/ou a tentativa de tutelar afronta a este bem jurídico. A evolução humana, constituída como organismo, exige a tutela da personalidade, até como meio de sustentação da sociedade, ou melhor, até como parte dos pilares da pacificação social. A tutela geral da personalidade é percebida, por exemplo, no art. 70º do Código Civil

[329] Bioni, Bruno Ricardo. Proteção de Dados Pessoais: A função e os limites do consentimento. Rio de Janeiro: Editora Forense Ltda, 2019.(Bioni 59) Comentários sobre os direitos da personalidade: "Os direitos da personalidade são uma "noção inacabada" que deve ser cultivada, especialmente frente ao abordado manancial de dados produzidos pelas pessoas na sociedade da informação. Por meio dessa premissa, será possível identificar uma nova variante desta categoria jurídica para nela enquadrar a proteção de dados pessoais".

[330] Bioni, Bruno Ricardo. Proteção de Dados Pessoais: A função e os limites do consentimento. Rio de Janeiro: Editora Forense Ltda, 2019.(Bioni 3-12)

Português[331], e no art. 2º c/c art. 12 do Código Civil Brasileiro[332].

Os direitos da personalidade têm próxima relação com a noção de *dados pessoais*. Basta, para tanto, observar as definições desenvolvidas nas normas em estudo.

No Regulamento Geral de Proteção de Dados (GDPR) dados pessoais é definido como a:

"*informação relativa a uma pessoa singular identificada ou identificável"*. Ao dispor sobre pessoa singular identificável complementa que: "*é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular*".

A norma legal brasileira (LGPD), define *dado pessoal* em sentido equivalente ao regulamentado na União Europeia, porém, desdobra dados pessoais em mais uma espécie, os ***dados pessoais sensíveis*.** Define como sendo o:

"*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*".

Também há a categoria dos *dados anonimizados,* aqueles pelos quais não é possível identificar seu titular após realizada a *anonimização* e, que podem ser considerados dados pessoais se utilizados para a formação de perfil comportamental a pessoa natural, se identificada.

Em Portugal, visando a execução do Regulamento da União Europeia neste tema, a Lei nº 58/2019, dedica-se ao tratamento de *dados pessoais* e à livre circulação destes no âmbito nacional, portanto, a definição de *dados pessoais* é tal qual a disposta no GDPR, portanto, ratifica a definição por uma visão expansionista.

A definição tratada nos direciona para a *noção expansionista*, na medida em que estão relacionados à pessoa natural identificada ou identificável, bem como em relação a grupos, ampliando o leque de abordagem. Neste sentido ressalta o Tribunal de Justiça da União Europeia[333],

[331] Artigo 70.º (Tutela geral da personalidade)1. A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida.

[332] Art. 2º A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro.Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

[333] (Tribunal de Justiça da União Europeia reconheceu o direito dos cidadãos a serem "esquecidos" na internet, e o de pedirem à Google e outros motores de busca que suprimam as ligações às suas informações pessoais). Destacamos: 68. O Tribunal de Justiça já declarou que as disposições da Diretiva 95/46, na medida em que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos

dando a uniformidade da hermenêutica jurídica posicionando-se na amplitude da definição necessária para a garantia do direito fundamental à proteção de dados.

Parece-nos adequada a concepção expansionista por ser acertada à tutela da proteção de dados, enquanto direito fundamental da pessoa natural, com a salvaguarda das limitações que a lei expressamente disciplinar neste sentido, bem como a autodeterminação informacional que se exprime por meio do consentimento.

2.3. Dados de Saúde

Avançando a partir da noção de dados pessoais, segundo as normas citadas e partindo para os aspectos da proteção há certas especificidades na tutela da proteção de dados que merecem compreensão, com reflexo aos *dados sensíveis*.

É indiscutível o papel da saúde no desenvolvimento socioeconômico, não importando em qual perspectiva, seja na prevenção, na promoção, ou no cuidado, até porque a integralidade é personagem que agrega a linha de cuidados em saúde. Sobre saúde[334] este é um dos alicerces para o desenvolvimento socioeconômico sustentável. Não poderia ser diferente, a ponto de que as mais variadas questões da área da saúde no direito, consagrando a sua multidisciplinariedade, com evidência atualmente na tecnologia (telemedicina, inteligência artificial, sistemas de informática, etc.) veio merecer especiais destaques no cenário ético-jurídico em escala global.

A inovação (revolução) tecnológica está propagando os mais diversos debates jurídicos. Na proteção de dados de saúde ganha importante projeção. O tratamento de dados traz uma série de possíveis desdobramentos, que vão do mero compartilhamento de informações colhidas por meio de vários *inputs*, como por exemplo de dispositivos móveis (atividade cardíaca, peso, altura, índice de massa corporal, tipo sanguíneo, medidores de estresse, atividade física, etc.) até em nível de dados coletados por meio sistemas dedicados a serviços de saúde (exames, atendimentos de urgência/emergência, consultas, internamentos, procedimentos, telemedicina, etc.).

Estamos sob constante vigilância em tempos da sociedade da informação. Os meios digitais expõem o indivíduo a mais diversas abordagens. Boa parte no intuito de despertar interesse em *produtos*, em expor e explorar *comportamento* e toda a sorte de incentivos virtuais para induzir e

fundamentais que, segundo jurisprudência constante, são parte integrante dos princípios gerais de direito cujo respeito é assegurado pelo Tribunal de Justiça e que estão atualmente consagrados na Carta (v., designadamente, acórdãos Connolly/Comissão, C-274/99 P, EU:C:2001:127, n.° 37, e Österreichischer Rundfunk e o., EU:C:2003:294, n.° 68).

[334] Lorga, Carlos Alexandre. "SAÚDE E DESENVOLVIMENTO: A INFLUÊNCIA DA UNIVERSALIDADE E DA INTEGRALIDADE NO DESENVOLVIMENTO SUSTENTÁVEL." Saúde, CONASS - Conselho Nacional dos Secretários de Estado da. *Para entender a gestão do SUS*. Brasília: Conass, 2015. artigo nº 7.

indicar o adequado modelo social em várias perspectivas, induzindo condutas, em majoritária parte com finalidades comerciais.

Por isso mecanismos de proteção de dados devem ser efetivos, devem coibir abusos, e devem garantir o direito fundamental da pessoa individual, e especialmente, possa dissuadir o tratamento de informações predatória que satisfaça apenas fim comercial e não alinhado com parâmetros razoáveis de responsabilidade social.

André Gonçalo Dias Pereira expõe que:

"*Perante este quadro de desenvolvimento tecnológico e esta mutação das relações humanas e das relações humano-máquina, as reflexões ética e jurídica estão considerando várias questões: a proteção de dados e a privacidade, incluindo das informações genéticas, bem como o direito de manter uma interface humana em situações vulneráveis que surgem de doenças*".[335]

Os dados de saúde na legislação brasileira são classificados como *dados pessoais sensíveis* conforme o inciso II do art. 5º da LGPD. A referida norma define *dado pessoal sensível* como sendo:

"*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*".

Somente podem ser objeto de tratamento se houver consentimento, forma específica e destacada, e finalidades específicas. Nas hipóteses *sem* consentimento do titular dos dados de saúde somente poderá ocorrer o tratamento em situações indispensáveis, taxativamente como: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; *f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária*; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[335] Pereira, André Gonçalo Dias.—. "O MÉDICO-ROBÔ E OS DESAFIOS PARA O DIREITO DA SAÚDE: ENTRE O ALGORITMO E A EMPATIA." GAZETA DE MATEMÁTICA novembro de 2019: 32-36. p.33

A norma brasileira em relação aos dados de saúde tem tratamento específico dispondo que pode ocorrer para fins de tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, devendo ser observada as vedações constantes do §§ 4º e 5º do art. 11 da LGPD. Na realização de estudos em saúde pública o tratamento de dados deverá observar a regulamentação da autoridade nacional e das autoridades da área de saúde e sanitárias.

A jurisprudência nacional ainda é incipiente, mas já há precedentes administrativos que evidenciam a responsabilização de clínicas e hospitais por vazamento ou acesso indevido a dados sensíveis, especialmente quando não há comprovação de adoção de medidas técnicas mínimas, como criptografia, controle de acesso e políticas internas de confidencialidade.

Outro aspecto relevante é a obrigação de *anonimização* ou *pseudonimização* dos dados sempre que possível, conforme dispõe o §4º do artigo 11 da LGPD. Essa técnica reduz os riscos associados ao tratamento de dados sensíveis e é especialmente recomendada em projetos de pesquisa ou compartilhamento com terceiros.

As resoluções da ANPD também impõem deveres de capacitação continuada dos profissionais que atuam no tratamento de dados sensíveis de saúde, bem como a nomeação de encarregado (*Data Protection Officer - DPO*), responsável por orientar, fiscalizar e mediar a comunicação entre a instituição, os titulares dos dados e a autoridade reguladora, como será abordado no capítulo específico sobre governança.

O reconhecimento dos dados de saúde como dados sensíveis impõe um regime jurídico reforçado, com exigência de governança técnica e jurídica, transparência, documentação e responsabilização, em consonância com os princípios da LGPD e os padrões internacionais de proteção de dados pessoais.

No GDPR, em alusão ao item 35 das considerações do regulamento, os dados de saúde são todas as informações "*sobre a sua saúde física ou mental no passado, no presente ou no futuro*". Neste conjunto de informações estão as coletadas antes da prestação de serviços de saúde, ou durante essa prestação; qualquer número, símbolo ou sinal particular atribuído à pessoa para identifica-la para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames, inclusive a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, doença, deficiência, risco de doença, histórico clínico, tratamento clínico ou estado fisiológico ou biomédico, independentemente da fonte (médico ou outro profissional de saúde, um hospital, uma clínica, um dispositivo médico ou um teste de diagnóstico *in vitro*).

No mesmo sentido *lato* empregado na definição de dados pessoais os dados de saúde também recebem análogo entendimento.

Alexandre L. Dias Pereira[336] enfatiza que os dados de saúde devem ser interpretados em termos amplos.

Diante disso, a conformidade com a LGPD e com as normativas da ANPD demanda das instituições de saúde a estruturação de programas robustos de governança, com políticas formais, revisão periódica dos processos, monitoramento contínuo, mecanismos de auditoria e resposta a incidentes.

2.4. Tratamento de Dados no GDPR. Princípios e os equivalentes na LGPD.

Na União Europeia a proteção de dados pessoais tem status de direito fundamental. Como mencionado, os dados recolhidos devem ser manipulados com lealdade, com fins específicos e mediante consentimento ou por outro meio autorizado por lei. Não se restringe o acesso do indivíduo aos seus dados pessoais, nem tão pouco impedir a sua retificação. Uma autoridade estará investida do dever de fiscalização para os fins da efetividade da proteção de dados. Por se tratar de Regulamento[337] no âmbito da EU é norma impositiva para todos os Estados-Membros.

A Diretiva_95/46/CE[338] é o primeiro marco normativo para a tutela da proteção de dados na União Europeia[339]. Foi revogada pelo Regulamento 2016/679/CE que institui o Regulamento Geral de Proteção de Dados (GDPR) no âmbito dos Estados-Membros da UE.

A transposição da Diretiva 95/46/CE, muito embora tenha alcançado objetivos e princípios que se tornaram sólidos, experimentou dificuldades em termos de efetividade. Disparidades na execução e aplicação da Diretiva na transposição contribuíram para isso. Alexandre Sousa Pinheiro[340] reflete que a Diretiva não "*possa ser considerada como um texto paradigmaticamente unificador em matéria da proteção de dados no domínio da União Europeia*". No entanto, indiscutivelmente foi a Diretiva

[336] Pereira, Alexandre L. Dias. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." *Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29* 2018: 51-70 (A. L. Pereira 58). Comenta o Autor sobre o conceito interpretado pelo Grupo de Trabalho sobre proteção de dados: "*previsto no artigo 29.º da Dir. 95/47, desenvolveu a interpretação deste conceito recomendando que os dados de saúde deveriam abranger: (a) quaisquer dados pessoais estritamente relacionados com o estado de saúde da pessoa, tais como dados genéticos ou dados sobre o consumo de medicamentos, álcool e drogas e (b) quaisquer outros dados contidos nos ficheiros clínicos sobre o tratamento de um paciente, incluindo dados administrativos (número de segurança social, data de admissão no hospital, etc.), de modo a que qualquer dado que não seja relevante para o tratamento do paciente não seja inserido nos ficheiros médicos*".

[337] (EUR-LEX, União Europeia) Os regulamentos são atos legislativos definidos no artigo 288.o do Tratado sobre o Funcionamento da União Europeia (TFUE). Têm caráter geral, são obrigatórios em todos os seus elementos e diretamente aplicáveis em todos os países da União Europeia (UE).

[338] (EUR-LEX, União Europeia) A diretiva faz parte do direito derivado da UE. É, por conseguinte, adotada pelas instituições da UE com base nos tratados fundadores. Uma vez adotada a nível da UE, a diretiva é incorporada — ou transposta — pelos países da UE, passando a vigorar como lei nesses países.

[339] Afirma Alexandre L. Dias Pereira que a lei de 30 de setembro de 1970, da Land Hesse, da República Federal da Alemanha, seria a primeira lei de proteção de dados pessoais

[340] Pinheiro, Alexandre Sousa. "Apresentação do regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral de Proteção de Dados (RGPD)." Revista do Centro de Estudos Judiciários 1º semestre de 2018: 303-327.(Pinheiro 306)

impulsionadora de debates ético-jurídicos, evoluindo, certamente, para o Regulamento.

Da Diretiva 95/46/CE para o GDPR foram ampliados os conceitos empregados na proteção de dados. Um processo natural evolutivo próprio de uma norma a suplantar outra. O GDPR contém 26 definições, o que a torna uma norma com características muito próprias.

Uma das características do GDPR diz respeito ao modelo de supervisão e o papel das autoridades nacionais no controle da proteção de dados[341] de forma a lhes atribuir competências de investigação, de correção e sanção, poderes consultivos e de autorização. Há a figura do *encarregado de proteção de dados* que deve ter *domínio do Direito e das práticas de proteção de dados*" (art. 38º, nº 5), vinculado ao sigilo e confidencialidade de suas funções.

Aborda o art. 5º do GDPR os princípios[342] relativos aos tratamentos de dados pessoais:

(i) Princípio da licitude, lealdade e transparência;

(ii) Princípio da finalidade;

(iii) Princípio da minimização dos dados;

(iv) Princípio da exatidão;

(v) Princípio da limitação da conservação;

(vi) Princípio da integridade e confidencialidade;

A respeito da aplicação dos princípios supracitados o GDPR atribui ao responsável pelo tratamento de dados o cumprimento e comprovação. Impõe um modelo proativo de atuação focado na responsabilização dos sujeitos, caso a regulamentação seja ofendida, o que se torna possível de verificação na medida em que há a obrigatoriedade de *registros das atividades de tratamento*.

Em matéria de sanções a GDPR, orienta ter em conta em relação a conduta, a sua natureza, gravidade e duração da infração, o caráter doloso, as medidas tomadas para atenuar os danos, o grau de responsabilidade, a reincidência, e a via pela qual a infração chegou a conhecimento da autoridade de controle, o cumprimento das medidas ordenadas em face do responsável pelo tratamento dos dados ou o subcontratante, o

---

[341] Pinheiro, Alexandre Sousa. Ob. Citada p. 322, no que diz respeito aos poderes das autoridades nacionais no controle da proteção de dados, minimamente, constituem-se em: "*Os poderes estão divididos entre poderes de investigação (nº1, do artigo 58º), poderes de correção (nº 2, do artigo 58º) e poderes consultivos e de autorização (nº 3, do artigo 58º)".*

[342] Pereira, Alexandre L. Dias. 2018. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." *Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29*, 51-70. Sobre os princípios segundo GDPR: "O tratamento de dados pessoais obedece a um conjunto de princípios fundamentais, designadamente a transparência, a finalidade, e a qualidade dos dados (licitude e lealdade; adequação, pertinência e proporcionalidade; exatidão e atualização). A licitude do tratamento significa que tratamento de dados pessoais será lícito se houver (1) consentimento do titular dos dados; (2) execução de contrato ou diligências prévias à sua formação ou declaração de vontade negocial do titular de dados; (3) cumprimento de obrigação legal a cargo responsável do tratamento; (4) proteção de interesses vitais do titular dos dados, se este estiver incapaz de consentir; (5) execução de missão de interesse público ou exercício de autoridade pública; (6) prossecução de interesses legítimos do responsável ou de terceiro a quem os dados sejam comunicados (desde que não devam prevalecer os interesses ou direitos do titular dos dados). Todavia, tratando-se de dados sensíveis, rege uma proibição geral de tratamento sujeita a algumas exceções, nomeadamente (a) consentimento do titular ou autorização legal específica, (b) a cláusula geral do artigo 7º/3, e (c) a situação específica do tratamento de dados de saúde.

cumprimento de um código de conduta ou outros fatores atenuantes ou agravantes incidentes sobre a infração.

Na LGPD as atividades de tratamento de dados parte do princípio da boa-fé, e conjugado a estes demais princípios[343]:

(i) finalidade[344]: 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[345]: 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.

Tanto quanto na GDPR[346], a norma brasileira impõe responsabilidade objetiva[347] ao sujeito da

[343] Art. 6º da LGPD.

[344] Na GDPR o princípio da finalidade traz a ressalva quanto ao tratamento posterior em conformidade com ao art. 89º, nº1.

[345] Equivalente ao Princípio da minimização dos dados constante na GDPR. Na norma brasileira o princípio da necessidade compõe a limitação do tratamento ao mínimo necessário para a realização da atividade de tratamento de dados, devendo abranger os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

[346] Art. 5º, nº 2 c/c art 24º da GDPR: O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo.

[347] Gonçalves, Carlos Roberto. Responsabilidade Civil. São Paulo: Editora Saraiva, 2009. (Gonçalves 22) Sobre a responsabilidade jurídica: "A lei impõe, entretanto, a certas pessoas, em determinadas situações, a reparação de um dano cometido sem culpa. Quando isto acontece, diz-se que a responsabilidade é legal ou "objetiva", porque prescinde de culpa e se satisfaz apenas com o dano e o nexo de causalidade. Esta teoria, dita objetiva, ou do risco, tem como

operação do tratamento de dados. Essa responsabilidade se reflete especialmente na obrigação de adotar medidas preventivas e reativas frente a incidentes de segurança. A Resolução CD/ANPD nº 15/2024[348] reforça esse dever ao estabelecer, de forma clara, os critérios que obrigam os agentes de tratamento a comunicar incidentes que envolvam dados pessoais. A norma determina que, sempre que houver risco ou dano relevante aos titulares, quando forem afetados 500 ou mais titulares, ou nos casos em que haja uso massivo de tecnologia no tratamento dos dados, deverá ser realizada comunicação à ANPD e aos titulares em até três dias úteis da ciência do fato. Essa comunicação deve conter informações detalhadas sobre a natureza do incidente, as categorias de dados afetados, os riscos envolvidos, as medidas de contenção e os canais de suporte aos titulares.

No setor da saúde, onde o tratamento de dados sensíveis é contínuo, volumoso e altamente vulnerável a ataques cibernéticos, torna-se indispensável a implementação de uma política robusta de resposta a incidentes, em conformidade com as exigências da Resolução. Tal política deve integrar o programa de governança em privacidade, prevendo fluxos de comunicação internos e externos, protocolos técnicos, definição de responsabilidades e planos de mitigação, como forma de assegurar o princípio da responsabilidade e prestação de contas previsto na LGPD. Dessa forma, promove-se a efetiva proteção dos dados de saúde e a integridade do sistema de saúde como um todo, além de se mitigar riscos de sanções administrativas e judiciais.

3 PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

3.1. Governança e Boas Práticas

Nota-se que a extensão dos diplomas que tratam a proteção de dados impõe aos responsáveis (controladores e operadores) pelo tratamento a necessidade, mesmo sendo facultativa, de implementar regulamentos que cuidem zelar pela segurança e prevenção como esforço a mitigar riscos aos indivíduos titulares de dados pessoais. Para além desta tarefa, tais regulamentos desempenham uma fundamental função de comprovar o cumprimento da lei e por consequência dos *códigos de conduta* e regulamentos instituídos pela ANPD que a lei atribuído esta competência regulatória.

A LGPD dedica o art. 50 as regras de *boas práticas* e a *governança* em matéria de tratamento de dados.

postulado que todo dano é indenizável, e deve ser reparado por quem a ele se liga por um nexo de causalidade, independentemente de culpa"

[348] Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024 Acesso em 06 abril 202

Por empréstimo à noção pela qual Jorge Manuel Coutinho de Abreu[349] leciona sobre governança (termo adotado no Brasil) *governação* ou *governo* das sociedades "*designa o complexo de regras (legais, estatutárias, jurisprudenciais, deontológicas), instrumentos e questões respeitantes à administração e ao controlo (ou fiscalização) das sociedades".* Podemos aplicar esta definição para entender que, nas atividades de tratamento de dados, a *governança* é um instrumento de fundamental importância para as unidades de saúde[350].

Assim a prática da *governança* tem presença certa para a segurança e prevenção no tratamento de dados pessoais. Exemplificando a necessidade de cuidados, como é no caso do acesso à informação genética, André Gonçalo Dias Pereira[351] traz reflexão sobre os riscos a que os indivíduos podem estar expostos, portanto, riscos equivalentes às atividades de tratamento de dados de saúde.

A *governança* como instrumento de responsabilidade ética e social, inclui-se na missão da proteção de dados. Tal qual no recorrente *Compliance*[352] (no dever de agir de acordo com as regras), a LGPD ao fomentar o engajamento de instrumento de *governança* e *boas práticas* por iniciativa dos controladores e operadores responsáveis pelo tratamento de dados pessoais.

A estrutura das regras de *boas práticas* e *governança* em tratamento de dados são compostas, nos termos da LGPD[353], das condições de organização, funcionamento, procedimentos (incluindo reclamações e petições de titulares de dados), normas de segurança, padrões técnicos, obrigações específicas (aos envolvidos no tratamento), ações educativas, mecanismos internos de supervisão e de avaliação e enfrentamento de riscos.

Na União Europeia o instrumento responsável equivalente às *boas práticas* e *governança* é tratado nos *códigos de conduta*. A elaboração deste instrumento é promovida no âmbito dos

[349] Abreu, Jorge Manuel Coutinho de. Governação das Sociedades Comerciais. Coimbra: Gráfica de Coimbra, 2010.(Abreu 7)

[350] São os estabelecimentos de **saúde** destinados a prestar serviços de assistência médica.

[351] Pereira, André Gonçalo Dias (A. G. Pereira, O MÉDICO-ROBÔ E OS DESAFIOS PARA O DIREITO DA SAÚDE: ENTRE O ALGORITMO E A EMPATIA): 1) **A discriminação injustificada** dos portadores de determinadas variações deve ser impedida, pois pode privar certas pessoas do acesso a direitos fundamentais, à educação, ao trabalho, à habitação, a constituir família, apenas por razões de probabilidades de vir a desenvolver doenças genéticas, privando assim a sociedade de beneficiar do contributo de muitos de nós e afastando da "comunidade" tantos de nós... 2) **A confidencialidade** assume ainda maior importância num tempo em que a informação clínica é entregue a sistemas informáticos expostos a grandes riscos de ataques por parte de empresas de big data, que usam a nossa informação como o petróleo do século XXI, donde o reforço das precauções e a proteção dos dados pessoais assume extrema relevância atualmente.

[352] CARVALHO, KARINE CITÓ CARNEIRO DE. ""Compliance" no Combate à Fraude Organizacional e à Corrupção." Coimbra: Dissertação de Mestrado na Área de Especialização em Ciências Jurídico-Empresariais/Menção em Direito Empresarial, apresentada à Faculdade de Direito da Universidade de Coimbra Orientador: Professor Doutor Alexandre Libório Dias Pereira, julho de 2018 (CARVALHO 16) Sobre *compliance* define a Autora: ..."tem-se no compliance a obediência a regras, sejam estas impostas por uma legislação ou não, podendo ser estipuladas cláusulas intrínsecas nos programas de compliance que visem a redução de riscos e que diminuam a possibilidade do cometimento de infrações às regras da concorrência, tornando mais confiáveis as relações no mercado empresarial.

[353] (EUR-LEX, União Europeia) Art. 40º

Estados-Membros pela autoridade de controle, Comitê e a Comissão de proteção de dados. Permite, ainda, que os responsáveis pelo tratamento utilizem os *códigos de conduta* com a função de comprovar o cumprimento do GDPR, e ainda, podem ser instituídas no âmbito nacional certificações (selos e marcas de proteção de dados), cujo procedimentos devem ser adotados pelos Estados-Membros para comprovação da conformidade das operações de tratamento de dados.

3.2. Programa de Governança em Privacidade e os Dados de Saúde

A ampla aplicação das regras de proteção no tratamento de dados em geral para os *dados de saúde* classificados segundo a LGPD como *dados sensíveis*, implica em precauções próprias diante da implementação do *programa de governança em privacidade*.

O adequado *programa de governança* envolta do tratamento de dados de saúde primordialmente tem como um de seus principais focos os deveres do responsável pelo tratamento de dados. Cabe aqui o alerta de Alexandre L. Dias Pereira[354], segundo o qual: "*O responsável pelo tratamento de dados tem, para começar, um dever especial de segurança e confidencialidade do tratamento*". E com razão.

Calha a boa prudência que os responsáveis pelo tratamento de dados em unidades de saúde, em razão do programa de governança em privacidade de dados, preocupem-se em implementar protocolos específicos em dados de saúde.

Os protocolos devem ser dotados de medidas técnicas e organizadas para salvaguardar os dados contra práticas contrárias a lei (tratamentos inadequados e ilícitos: destruição, perda, alteração, difusão, acesso não autorizado).

A Resolução CD/ANPD nº 19/2024 apresenta os elementos obrigatórios para que um programa de governança em privacidade seja considerado efetivo. Dentre eles, destacam-se:

- Comprometimento institucional com a privacidade;
- Políticas internas claras e revisadas periodicamente;
- Nomeação formal de encarregado pelo tratamento de dados (DPO);
- Capacitação dos colaboradores;
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- Prevenção de riscos e adoção de medidas técnicas e administrativas.

A resolução ainda exige que o programa seja proporcional à natureza das atividades e aos riscos envolvidos. Dessa forma, uma clínica odontológica

[354] Pereira, Alexandre L. Dias. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." *Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29* 2018: 51-70.

e um hospital de grande porte deverão ter programas distintos, mas ambos devem demonstrar efetividade e comprometimento com os princípios da LGPD.

Também podemos admitir adequado que estes protocolos contemplem medidas considerando níveis de segurança[355] (observando a transmissão de dados em rede), bem como apropriado controle desde a entrada de pacientes no ambiente hospitalar/ambulatorial, de coleta de dados, suportes de segurança da rede (inserção, utilização, acesso, transmissão, e cadeia de operadores autorizados com identificação/certificação digital inequívoca de acesso com assinatura digital).

Para os níveis de acesso dos operadores e encarregados do tratamento de dados equivalentes níveis de classificação de dados se mostram úteis. No Brasil, a Lei nº 12.527/2011 (Lei Geral de Acesso à Informação) disciplina no âmbito da administração pública a adoção de níveis de classificação de informações de saúde, por considera-las imprescindíveis à segurança da sociedade ou do Estado. Isto posto, admitir nos protocolos que integrem o programa de governança em privacidade níveis de acesso e classificação de dados alinha-se com a segurança e prevenção contra o tratamento inadequado ou ilícito de dados.

No que diz especialmente aos dados de saúde a Lei nº 13.787/2018 disciplinou a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente, atuando suplementarmente com a norma geral de proteção de dados LGPD. A regra em referência estabelece que o documento eletrônico deverá assegurar a integridade, a autenticidade e a confidencialidade do documento digital.

Considerando a expressa referência que a Lei nº 13.787/2018 remete à proteção de dados na LGPD é razoável que em nível de informações digitais a segurança e a prevenção sejam igualmente exigíveis e integrem o programa de governança em privacidade em unidades de saúde. Muito embora, no nível do profissional médico[356] se tenha há tempos o dever de sigilo, as unidades de saúde (hospitais, clínicas e consultórios) estão vulneráveis a acessos não autorizados à base de dados. Esta exposição os sujeita a responsabilização e sanções na LGPD, o que traz mais uma razão para a implementação de um cauteloso *programa de governança em privacidade* na unidade de saúde.

---

[355] Pereira, Alexandre L. Dias. 2018. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29, 51-70. (A. L. Pereira 61) Em alusão ao art. 4º, nº 1 da Lei nº 12/2005 de Portugal. "*É proibido o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, e são exigidos níveis de segurança que evitem nomeadamente a sua destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação".*

[356] Código de Ética Médica, art. 11.

Torna-se conveniente que no *programa de governança em privacidade*, especialmente em dados de saúde, a adoção de medidas técnicas que tornem os dados de saúde ininteligíveis para terceiros não autorizados a acessá-los, integrando esta prática nos protocolos de segurança e prevenção. Esta cautela mostra-se fundamental como medidas de segurança, técnicas e administrativas voltadas para proteger dados, refutando e evitando que sejam obtidos dados por acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A Resolução CD/ANPD nº 15/2024 detalha as hipóteses em que a comunicação de incidentes é obrigatória. O artigo 5º traz três critérios para essa obrigatoriedade:

I - risco ou dano relevante aos titulares;
II - número igual ou superior a 500 titulares afetados;
III - utilização massiva de tecnologia para tratamento.

Uma vez preenchido um desses critérios, a comunicação à ANPD e aos titulares deve ocorrer em até três dias úteis da ciência do incidente, conforme artigo 7º da mesma norma. Além disso, a comunicação deve conter informações detalhadas sobre o incidente, os riscos, as medidas de contenção e mitigação, bem como canais de atendimento aos titulares. No setor da saúde, onde incidentes de vazamento de dados podem gerar danos reputacionais e à segurança dos pacientes, é fundamental estruturar uma política de resposta a incidentes conforme o previsto na resolução.

Desta forma o programa de governança em privacidade que contemple protocolos com tais cautelas será considerado conforme a LGPD para fins de avaliação da gravidade do incidente de segurança, impactando na mensuração da sanção, dando meios, inclusive, no exercício do contraditório que sejam adequadamente considerados pela autoridade fiscalizadora.

Assim, conjugando o disposto nos §§ 2º e 3º do art. 48 da LGPD a autoridade nacional deverá tomar em conta as cautelas aplicadas comprovadas pelo responsável pelo tratamento de dados. Portanto, no programa de governança em privacidade, "*o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares*"[357].

Por fim, no que tange a transferencia internacional de dados de saúde**, a** Resolução CD/ANPD nº 18/2024 que regulamenta esta matéria, traz deveres que são especialmente relevante para hospitais e laboratórios que utilizam sistemas baseados em nuvem ou contratam fornecedores de tecnologia

[357] Art. 49 da LGPD

estrangeiros, para armanezamento de base de dados. O artigo 4º da resolução permite a utilização de Cláusulas-Padrão Contratuais (CPCs) aprovadas pela ANPD, admite instrumentos como regras corporativas globais (Binding Corporate Rules) e aditivos contratuais específicos. Bem como, é obrigatória a elaboração de Relatório de Transferência Internacional de Dados (RTID), demonstrando a segurança e a legitimidade da operação.

Entretanto, é vedada a transferência de dados sensíveis para países que não proporcionem grau de proteção adequado, salvo se houver consentimento específico e destacado do titular, ou se a transferência for essencial para proteção da vida e da saúde, conforme artigo 33 da LGPD.

Desta forma, necessáriose faz ter especialcuidado ao contratar o servidor de base de dados, para que seja atendido o requisite de governança exigido pela referida Resolução da ANPD.

A relevância preventiva da implementação de boas práticas e programa de governança voltado para a proteção de dados é reconhecida no inciso IX do §1º do art. 52 da LGPD, vez que as sanções decorrente do procedimento administrativo correlato, serão gradativas e considerarão de forma isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e segundo parâmetros e critérios[358], cuja forma de aplicar a dosimetria das sanções administrativas, está prevista na Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

CONCLUSÃO

Com base na máxima do direito fundamental da proteção de dados, na ampla definição de dados pessoais, na classificação destes dados em dados sensíveis, portanto na esfera dos dados de saúde, buscamos analisar as principais noções que conduzem à importância de implementar ferramenta que tenha dedicação nas *boas práticas* consolidadas em um *programa de governança em privacidade de dados em unidades de saúde*, tendo em vista o GDPR (EU), a LGPD e as Regulamentações da ANPD.

Cada vez mais a segurança das sociedades (*corporate governance*) exige medidas de governança e de *compliance* para o alcance de seus fins sociais. Não se dissociando da relevância a qual o *consentimento* é um dos elementos indispensáveis no ato de disposição de vontade em matéria de tratamento de dados e na proteção da intimidade privada as informações do indivíduo devem ser tratadas com extrema cautela.

Aspectos gerais nas normas pesquisadas demonstram que outros valores jurídicos com

[358] Art. 52 da LGPD: Parâmetros e critérios: "I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

status de princípios se interagem. A *dignidade*, a *integridade* e *autonomia*. As informações com tratamento de dados têm potencial para conduzir a uma nova identidade apta para apontar para um indivíduo ou para um grupo, surgindo disso inúmeros possíveis desdobramentos com potenciais impactos na sociedade da informação, e nas sociedades comerciais.

A noção expansionista de dados pessoais alarga as possíveis abordagens, de forma que demonstrou-se ser apta a justificar especial preocupação na adoção de uma ferramenta de *boas práticas* e *governança*. Assim, os responsáveis pelo tratamento de dados em unidades de saúde, devem ter uma visão atenta para a implementação e execução do *programa de governança em privacidade de dados*, sendo prudente a integração de *protocolos específicos em dados de saúde*.

Os protocolos seriam dotados de medidas técnicas e organizadas para salvaguardar os dados contra práticas contrárias a lei (tratamentos inadequados e ilícitos: destruição, perda, alteração, difusão, acesso não autorizado), concluindo que estes protocolos contemplem medidas considerando níveis de segurança (observando a transmissão de dados em rede), bem como apropriado controle desde a entrada de pacientes no ambiente hospitalar/ambulatorial, de coleta de dados, suportes de segurança da rede (inserção, utilização, acesso, transmissão, e cadeia de operadores autorizados com identificação/certificação digital inequívoca de acesso com assinatura digital).

Por fim, a relevância preventiva da implementação de *boas práticas* e *programa de governança* tem expresso reconhecimento na LGPD e deveres impostos pela ANPD por meio de diferentes Resoluções, o que se mostra em grande contexto de importância desta ferramenta. Adequada implementação como remédio preventivo para as unidades de saúde em geral independentemente de sua natureza jurídica (pública ou privada) se torna indiscutivelmente essencial para os fins da proteção de dados sensíveis, como os de saúde.

REFERÊNCIAS BIBLIOGRÁFICAS

Abreu, Jorge Manuel Coutinho de. *Governação das Sociedades Comerciais*. Coimbra: Gráfica de Coimbra, 2010.

Bezerra, Carlos. 20 de novembro de 2019. <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>.

Bioni, Bruno Ricardo. *Proteção de Dados Pessoais: A função e os limites do consentimento*. Rio de Janeiro: Editora Forense Ltda, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de fevereiro de 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/resolucao-15.pdf. Acesso em: 2 abr. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 18, de 20 de março de 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/resolucao-18.pdf. Acesso em: 2 abr. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 20 de março de 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-

publicacoes/resolucao-19.pdf. Acesso em: 2 abr. 2025.

Carvalho, Karine Citó Carneiro de. ""Compliance" no Combate à Fraude Organizacional e à Corrupção." Coimbra: Dissertação de Mestrado na Área de Especialização em Ciências Jurídico-Empresariais/Menção em Direito Empresarial, apresentada à Faculdade de Direito da Universidade de Coimbra Orientador: Professor Doutor Alexandre Libório Dias Pereira, julho de 2018.

EUR-LEX. *União Europeia*. 03 de dezembro de 2019. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14522>.
—. *União Europeia*. 03 de dezembro de 2019. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527>.

Gonçalves, Carlos Roberto. *Responsabilidade Civil*. São Paulo: Editora Saraiva, 2009.

Lorga, Carlos Alexandre. "SAÚDE E DESENVOLVIMENTO: A INFLUÊNCIA DA UNIVERSALIDADE E DA INTEGRALIDADE NO DESENVOLVIMENTO SUSTENTÁVEL." Saúde, CONASS - Conselho Nacional dos Secretários de Estado da. *Para entender a gestão do SUS*. Brasília: Conass, 2015. artigo nº 7.

Pereira, Alexandre L. Dias. "BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA» A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)." *Lex Medicinae - Revista Portuguesa de Direito da Saúde Nº 29* 2018: 51-70.

Pereira, André Gonçalo Dias. *Direitos dos Pacientes e Responsabilidade Médica*. Coimbra: Coimbra Editora, 2015.
Pereira, André Gonçalo Dias — "O MÉDICO-ROBÔ E OS DESAFIOS PARA O DIREITO DA SAÚDE: ENTRE O ALGORITMO E A EMPATIA." *GAZETA DE MATEMÁTICA* Novembro de 2019: 32-36.

Pinheiro, Alexandre Sousa. "Apresentação do regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral de Proteção de Dados (RGPD)." *Revista do Centro de Estudos Judiciários* 1º semestre de 2018: 303-327.

Tribunal de Justiça da União Europeia reconheceu o direito dos cidadãos a serem "esquecidos" na internet, e o de pedirem à Google e outros motores de busca que suprimam as ligações às suas informações pessoais. Nº Processo C-131/12. Tribunal de Justiça da União Europeia. 13 de maio de 2014.