FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

ROSIMERIE POLICIANO MENDES CONSTANTINO

A EMERGÊNCIA DA PROTEÇÃO DE DADOS SENSÍVEIS NO DIREITO À SAÚDE

VOLTA REDONDA
2023

FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

A EMERGÊNCIA DA PROTEÇÃO DE DADOS SENSÍVEIS NO DIREITO À SAÚDE

Monografia apresentada ao Curso de Direito do UniFOA como requisito à obtenção do título de bacharel em Direito.

Aluna:
Rosimerie Policiano Mendes Constantino

Professor Orientador:
Luiz Claudio Gonçalves Junior

VOLTA REDONDA
2023

Fundação Oswaldo Aranha

UniFOA Centro Universitário de Volta Redonda

FOLHA DE APROVAÇÃO

Trabalho de Conclusão de Curso intitulado:

A EMERGÊNCIA DA PROTEÇÃO DE DADOS SENSÍVEIS NO DIREITO À SAÚDE

Elaborado por Rosimerie Policiano Mendes Constantino, apresentado publicamente perante a Banca Avaliadora como parte dos requisitos para conclusão do Curso de Direito.

Aprovado em 22 de junho de 2023

Banca Avaliadora:

.....

Professor(a) Orientador(a) - Unifoa

.....

Professor(a) Avaliador(a) - Unifoa

.....

Professor(a) Avaliador(a) - Unifoa

À minha Família.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me proporcionar esse momento único e por permitir chegar até aqui.

À minha Família pelo apoio e por ter acreditado na minha capacidade.

Aos Professores desta conceituada Instituição, pelos ensinamentos e por me permitir apresentar um melhor desempenho dessa jornada.

Ao meu Orientador Professor Doutor Luiz Claudio Gonçalves Junior, por ter se prontificado a me ajudar e se dedicar tanto nesse trabalho.

RESUMO

A monografia tem por objetivo analisar a legislação, pertinente ao tema, e apresentar pontos relevantes sobre a proteção de dados pessoais no Brasil no contexto da LGPD na área da saúde. É feita uma breve síntese a despeito do desenvolvimento da proteção de dados pessoais a luz da Constituição Federal, o foco está principalmente no surgimento da LGPD em relação ao processamento de dados sensíveis na saúde. Várias facetas são abordadas, incluindo possíveis riscos relativos à conformidade, responsabilidade, práticas discriminatórias e aplicabilidade. Em última análise, conclui-se que ainda há um caminho significativo pela frente em termos de integração completa do sistema de saúde brasileiro com a LGPD. Para garantir o direito fundamental à confidencialidade de todos os cidadãos, os profissionais de saúde, clínicas e hospitais devem implementar medidas para cumprir os regulamentos. É direito do indivíduo ter seus dados pessoais protegidos, o que é assegurado pelo seu direito fundamental à privacidade.

Palavras-chave LGPD; direito à saúde; dados sensíveis; privacidade.

Sumário

1. INTRODUÇÃO

A tecnologia traz dinamismo e mudança aos dados pessoais na vida dos indivíduos, por isso com a criação e recriação de ferramentas utilizadas no mundo digital, surge o problema do limite imposto à proteção de dados em relação ao meio técnico e como tais ferramentas são usadas para acessar essas informações específicas.

Com o desenvolvimento da tecnologia, que proporcionou uma nova forma de organizar, transmitir, coletar, armazenar e processar informações na Internet, a informação foi cada vez mais utilizada para desenvolver necessidades econômicas e segurança do usuário. No entanto, a posição do proprietário da informação e do consumidor de bens foi duramente criticada e tornou-se mais vulnerável, pois a informação passou a circular entre os participantes da atividade econômica e a intimidade e as opções foram ultrapassadas pelos interesses de grandes empresas em detrimento da vontade individual.

Além disso, o indivíduo passa por um processo de despersonalização ao perder o direito exclusivo à sua personalidade. Justamente nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) é criada para mobilizar a sociedade e o mercado quanto à importância dos dados pessoais para avaliar qual limite de exposição é aplicável e quando é permitido. A LGPD controla a regulamentação do relacionamento entre as partes envolvidas e, além da fiscalização do caso, esclarece a rotulagem positiva, as regras e as penalidades cabíveis caso o uso adequado e sigiloso dos dados coletados para fins financeiros não seja seguido.

No contexto da saúde, a proteção dos dados é especialmente crucial, uma vez que informações sensíveis e privadas dos pacientes são frequentemente coletadas, armazenadas e compartilhadas por profissionais de saúde, hospitais, clínicas e seguradoras.

Com a implementação da LGPD, os profissionais de saúde e as instituições médicas devem adotar medidas adequadas para garantir a segurança e a privacidade dos dados dos pacientes. A aplicação adequada da LGPD nesse setor pode garantir que os pacientes tenham controle sobre suas informações pessoais e que esses dados sejam tratados com responsabilidade, evitando vazamentos, acesso não autorizado ou uso indevido.

O objetivo da lei é proteger os direitos básicos das pessoas físicas à liberdade, à privacidade, bem como, garantir que o processamento relacionado à coleta de dados pessoais seja realizado de forma responsável, de boa fé e de acordo com as melhores práticas de acordo com a legislação em vigor.

Sendo assim, faz-se necessário uma análise atual da conjuntura da privacidade bem como da legislação para que se possa assumir uma perspectiva coesa e coerente com o novo paradigma da intimidade e o mérito da lei ordinária citada.

O presente estudo, por meio de método cientifico e revisão bibliográfica como abordagens, busca destacar a importância e a urgência de adequar as práticas de tratamento de dados sensíveis na área da saúde, explorando as possíveis consequências da aplicação inadequada da LGPD no direito à saúde, como o comprometimento da confiança entre pacientes e prestadores de serviços de saúde, a exposição de informações sensíveis que podem levar a discriminação ou constrangimento, bem como as sanções e penalidades previstas na lei para aqueles que não cumprem suas disposições.

2. SINTESE HISTÓRICA DO DIREITO DE PRIVACIDADE NA ESTRUTURA CONSTITUCIONAL BRASILEIRA

O objetivo deste capítulo é fazer uma breve descrição a despeito do desenvolvimento da proteção de dados pessoais no Brasil, que possui como importante marco legal a Lei Geral de Proteção de Dados Pessoais (LGPD), conforme será demonstrado nas subseções a seguir.

2.1 A evolução da internet: breves apontamentos

O século XX foi uma época de enorme desenvolvimento tecnológico, de circulação de informações, de aperfeiçoamento da comunicação, como o computador, que iniciou sua trajetória em 1943, e de criações como a Internet, que começou a ser criada em 1969. Após a popularidade da Internet, ela gradualmente se desenvolveu significativamente e se tornou indispensável na vida humana, como um computador (DONEDA, 2011).

Quando o computador foi conectado à Internet, o desenvolvimento tecnológico atingiu uma velocidade sem precedentes e cruzou o horizonte, espalhando-se amplamente pelo mundo, diferenciando a vida social, seja em termos de métodos de comunicação, quanto mais fácil é reduzir atividades (DONEDA, 2011).

A chamada World Wide Web, também chamada de Internet, foi desenvolvida durante a Guerra Fria para fins militares, como o computador utilizado pelos militares dos Estados Unidos como meio alternativo de comunicação quando sob ataque de forças inimigas (CASTELLS, 2015).

Foi assim que surgiu a ARPANET (Advanced Research Projects Administration) como a primeira rede nacional de computadores, fundada em 1969 pelo Departamento de Defesa dos Estados Unidos e incumbida de conectar computadores em laboratórios de pesquisa, universidades e, principalmente, instituições militares. O governo dos EUA em 1972 possibilitou o compartilhamento de informações, pesquisas e estratégias militares. O objetivo também era levar a Internet às universidades americanas, conectando seus computadores a centros de pesquisa. Em 1980, foi lançado o protocolo aberto TCP IP (Transmission Control Protocol), que permitia a conectividade de sistemas heterogêneos (CASTELLS, 2015).

Assim, a rede poderia ser estendida a vários dispositivos como supercomputadores, microcomputadores, estações de trabalho e mainframes, mas foi em 1983 que a definição da Internet foi, na verdade, como ela foi separada da rede civil e ambiente militar (ADRIEN, 2014).

Em 1991, nasceu a rede mundial de computadores World Wide Web (WWW), que possibilitou a transmissão de vídeos, fotos e sons, pois, até aquele momento, o texto só podia ser transmitido pela rede, ou seja, a Internet mais populares entre os usuários e provedores de serviços foram inventados para permitir a navegação na web (ADRIEN, 2014).

Após seu mecanismo ter sido aprimorado e atualizado ao longo do tempo, a Internet se difundiu e ganhou dimensões globais, e no Brasil passou a ser utilizada na década de 90, segundo o Sindicato Brasileiro dos Provedores de Serviços de Comunicação em 1996, cerca de trezentos mil brasileiros ficaram online (BOFF; FORTES, 2014).

Segundo o Instituto Brasileiro de Geografia e Estatística, em 2014 mais da metade dos domicílios brasileiros tinha acesso à Internet (cerca de 36,8 milhões de domicílios), sendo este um dos principais motivos para o aumento do acesso, havia internet em celulares, tablets, televisões e outros aparelhos (BOFF; FORTES, 2014).

Os computadores, por muito tempo, foram os principais mecanismos de acesso à internet pelos usuários, sendo que com a evolução dos smartphones muitas pessoas passaram a acessá-la por meio destes aparelhos (BOFF; FORTES, 2014).

De acordo com a empresa de rastreamento de tráfego de Internet StatCounter, em 2016, o acesso à Internet via tablets e celulares foi pela primeira vez superior ao dos computadores tradicionais, ou seja, ambientes virtuais por meio de dispositivos móveis, embora o uso de computadores ainda seja significativo (CAVALCANTI; SANTOS, 2018).

Outro ponto que merece atenção diz respeito ao chamado ciberespaço, que segundo Lévy é um novo meio de comunicação que surge da interligação global de computadores. Essa terminologia abrange não apenas a infraestrutura física das comunicações digitais, mas também o vasto oceano de informações contido nele, bem como as pessoas que exploram e contribuem para esse universo. Por outro lado, o termo "cibercultura" define as tecnologias (tanto materiais quanto intelectuais), práticas, atitudes, formas de pensamento e valores que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 2000).

A era cibernético-tecnológica influenciou o cotidiano das pessoas de diversas formas, pois com sua criação foi introduzido um ambiente virtual, que possibilita amizades virtuais, comunidades, tornando a navegação nesses ambientes uma prioridade na vida das pessoas, como meio de comunicação social. Dadas as muitas interações e compartilhamento de informações, é importante saber a diferença entre informações pessoais e categorias especiais de informações, conforme discutido no próximo tópico.

2.2 Principais especificidades sobre dados pessoais e categoriais especiais de informação

A importância da proteção legal dos dados pessoais reside no fato de que tanto esses como outros dados deles obtidos quase representam uma pessoa perante a sociedade, o que representa uma parte real de sua personalidade. Portanto, embora nem sempre de uso prático óbvio, uma explicação da diferença entre os conceitos de dados pessoais e informações pessoais pode ser útil para uma discussão aprofundada sobre o assunto (BOFF; FORTES, 2014).

2.3 Dados pessoais X Informações pessoais

Quando se utilizam os termos dados pessoais e informações pessoais, é inegável que os dois se sobrepõem em diferentes circunstâncias e representam certos aspectos do fato, da realidade. Em termos de detalhes, dados podem ser vistos como um termo primitivo e fragmentado, que pode ser entendido como informação em estado potencial, que se torna informação somente quando é transmitida, recebida e compreendida (CAVALCANTI; SANTOS, 2018).

Segundo Souza esse conhecimento é anterior ao processo interpretativo e criativo. Assim, aparece como uma conjuntura de eventos, ações humanas que tendem a mudar as pessoas, conteúdos, entre outras coisas, segundo a personalidade, afetividade (SOUZA, 2018).

Normalmente, os objetos devem ser identificadas ou pelo menos identificáveis, mas nem sempre é esse o caso, por exemplo, nos casos em que a informação se refere a pessoa de natureza não especificada. Em tais situações, segundo Souza:

> As informações são mantidas anônimas e utilizadas para fins estatísticos e protegem as pessoas cujas informações foram previamente coletadas e armazenadas. Ressalta-se que, por serem esses dados anônimos e tratados de forma a impossibilitar a identificação, deixam de estar sujeitos à disciplina e proteção da proteção de dados pessoais, uma vez que não violam a natureza protetiva desse direito: a privacidade e personalidade humana (SOUZA, 2018, p.35).

Dados pessoais são algo que vão além de seu mero conteúdo e requerem um procedimento prévio para sua análise. Eles podem ser compartilhados de inúmeras formas, sejam fotos, vídeos, e diversas situações, inclusive coisas relacionadas a valores (CATALA, 2011).

Com base na Convenção de Strasbourg, uma boa forma de conceituar a terminologia seria a seguinte: "qualquer informação sobre uma pessoa natural identificada ou identificável" (SOUZA, 2018, p.41).

Desse modo as informações pessoais, diferem das demais por um viés mais objetivo entre o indivíduo e as informações relevantes, independentemente das questões que lhes dizem respeito. Segundo Doneda, essa conexão subjetiva seria “além de outras categorias de informações que, embora possam ter alguma relação com a pessoa, não seriam exatamente informações pessoais” (DONEDA, 2011, p.78).

Diante disso, é muito importante esclarecer que o objetivo da proteção de dados ou informações pessoais é proteger a pessoa e sua personalidade, e não o dano em si (CAVALCANTI; SANTOS, 2018).

Com isso em mente, o tópico a seguir discute categorias de dados específicas que representam uma categoria de dados que representa uma ameaça maior à personalidade do indivíduo.

2.4 Categorias especiais de informação: eventuais riscos de discriminação

A análise desta categoria de dados desenvolve-se a partir do conhecimento de que o tratamento de determinados dados pode constituir uma ameaça maior, e mais grave, à personalidade e à liberdade da pessoa do que outros, o que pode conduzir a uma nova questão de igualdade, que se fora infringida pode levar a ações potencialmente discriminatórias, por exemplo (BOFF; FORTES, 2014).

A questão é tratada de forma diferenciada nas normativas, além de costumar vir acompanhada de normativas gradativamente mais rígidas, visando a melhor proteção dos cidadãos e da sociedade (DONEDA, 2011).

É muito importante proteger todo tipo de informação, mesmo aquelas que não são consideradas tão importantes, pois mesmo que pareça algo insignificante, pode se tornar sensível ao longo do caminho (BOFF; FORTES, 2014).

Nesse sentido, Mendes acrescenta que: “É [...] com tratamento de dados sensíveis que é capaz de transformar dados inofensivos em dados potencialmente discriminatórios”. (MENDES, 2014, p.150).

O fato de que o tratamento de dados sensíveis, mesmo que inicialmente inofensivos, pode transformá-los em informações discriminatórias, o que pode trazer implicações éticas e legais significativas. O autor aponta que a crescente utilização de tecnologias de Big Data e análise de dados exige uma reflexão cuidadosa sobre como equilibrar a privacidade dos indivíduos e os interesses das empresas e governos que coletam e tratam esses dados.

Segundo Martins: “informações insignificantes podem adquirir um novo valor. Dessa forma, deixarão de ser gerados dados irrelevantes no tratamento eletrônico de dados” (MARTINS, 2014, p.02).

Certamente não deveria haver proibição absoluta de acesso e uso de dados pessoais, pois tal prática colocaria em risco a segurança necessária para a execução das ações judiciais e seria contrário à autonomia da negociação. Não só nestes casos, mas também quando a utilização é legal e necessária, por exemplo em atividades de investigação ou mesmo médicas, não cabe a recusa total no tratamento de dados pessoais (MARTINS, 2014).

Por último, importa referir que o artigo 6.º do RGPD (Regulamento Geral de Proteção de Dados), que regula a matéria na União Europeia, não impede a plena utilização desta informação, apenas em alguns casos (BOFF; FORTES, 2014).

As principais preocupações de proteção de dados pessoais referentes à saúde dizem respeito a não discriminação e à manutenção das oportunidades sociais. Em atenção a esse imperativo, a LGPD confere grau de proteção especial, ao tratar as informações relativas à saúde como dados pessoais de natureza sensível, submetidos a regime limitado de tratamento, especialmente em relação ao consentimento ou não do titular dos dados. Ou seja, o regime adotado para a saúde pela LGPD depreende que os dados sejam utilizados para a consecução de sua finalidade, exigindo coerência entre a natureza do dado e o respectivo emprego, de forma que não sujeite o seu titular a práticas discriminatórias.

O direito fundamental de proteção à saúde e ao bem-estar dos cidadãos é um bem coletivo, com status normativo e fundamentação no ordenamento jurídico brasileiro. A Constituição Federal de 1988 contém diversas disposições relacionadas a esse direito, incluindo o objetivo fundamental da República de promover o bem-estar de todos, sem discriminação, e o direito social à saúde, além de outras garantias, como o acesso universal e igualitário às ações e serviços de saúde.

> Art. 3º, IV: estabelece como objetivo fundamental da República Federativa do Brasil "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação".
> Art. 6º, caput: garante o direito social à saúde, bem como a educação, o trabalho, a moradia, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, e a assistência aos desamparados.
> Art. 196: define a saúde como direito de todos e dever do Estado, que deve garantir políticas sociais e econômicas que visem à redução do risco de doenças e de outros agravos, além do acesso universal e igualitário às ações e serviços para a sua promoção, proteção e recuperação.
> Art. 225: estabelece o direito ao meio ambiente ecologicamente equilibrado como um direito fundamental, cuja defesa cabe ao poder público e à coletividade, incluindo a proteção à saúde como uma de suas dimensões (BRASIL, 1988).

A LGPD estabelece penalidades administrativas que somente a ANPD (Autoridade Nacional de Proteção de Dados) pode aplicar em caso de violação do direito fundamental à saúde. A Lei confere ainda prioridade à ANPD na salvaguarda dos dados pessoais, sobrepondo-se a qualquer outra entidade ou órgão da administração pública.

A importância dos direitos e liberdades fundamentais justifica um tratamento especial para os dados pessoais que são inerentemente sensíveis. O processamento de tais dados pode representar graves riscos para os direitos e liberdades acima mencionados. Além disso, os dados pessoais que divulgam detalhes de origem racial ou étnica, sexualidade e direito à saúde também devem ser tratados com muito cuidado. O Capítulo 4 deste estudo fornece mais informações sobre esses pontos.

2.5 Evolução da proteção de dados no Brasil

A respeito do contexto da proteção à privacidade no Brasil, Salete Oro Boff e Vinicius Borges Fortes, em texto “A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco

regulatório para o Brasil” explicam em suma a evolução da tecnologia principalmente na questão da comunicação e informação, também analisam sob a realidade brasileira, as legislações, marcos pontos de princípio de proteção ,como instrumentos normativos e controle da distribuição das informações pessoais, visando o asseguramento de proteção de forma jurídica aos direitos a privacidade e inviolabilidade dos dados (BOFF; FORTES, 2014, p.245).

Os autores com a proposta de pesquisa no Brasil, país que deu, tardiamente, a devida relevância sociocultural, jurídica para esse tema de privacidade em contemporaneidade com o advento de novas tecnologias e de que forma deve ser feita a proteção jurídica do direito à privacidade e proteção dos dados, as principais propostas e instrumentos, contextualização e delimitar as dimensões das violações desses direitos para o estudo (BOFF; FORTES, 2014).

Com o conceito de ciberespaço, para noções de base do estudo, sociedade da informação, demonstra o histórico do surgimento da internet, com base em estudos e pesquisas de novas formas de comunicação e informação, a criação dos primeiros softwares para navegação nas World Wide Web, por conta da Guerra Fria, onde não há um confronto direto, mas de guerra de informações, narrativas ideológicas. Com o tempo, finda a guerra fria, ocorreu uma democratização da informação, o acesso a população e processos de inclusão digital para a população e citam, por reflexos pela chegada das novas tecnologias a época (BOFF; FORTES, 2014).

A partir de então, surgem problemas jurídicos decorrente da popularização do uso das redes, promovendo questões referentes ao direito à privacidade e proteção dos dados pessoais, com isso surgem diretrizes e marcos regulatórios em escala global, com os objetivos de criar normas para o uso da rede e regulação das redes sociais. E mencionado, estudos de Keen, onde há cada vez mais a indução, sedução incentivo aos usuários da rede, ao exibicionismo, para o fornecimento de dados pessoais, conteúdo da internet, o da neutralidade da rede, por conta do filtro e privilegio de trafego de acordo com os fins sócio-políticos ou econômicos, além desse o da padronização e interoperabilidade com o fechamento de padrões e participação da operação da internet, afetando a privacidade dos usuários (BOFF; FORTES, 2014).

O direito à privacidade é reconhecido constitucionalmente pelo Brasil. Abrange a preservação da intimidade, vida privada, inviolabilidade e assegura o direito a indenização pelo dano material ou moral, decorrente dessas violações. Anteriormente, havia uma lacuna na legislação e no sistema jurídico brasileiro em

relação às violações de garantias e direitos fundamentais na rede, bem como à proteção de dados e à infraestrutura tecnológica para garantir o acesso à internet a toda a população, entendido como um direito essencial para o exercício da cidadania. Isso inclui o sigilo das comunicações, a não suspensão da conexão e a inviolabilidade. No entanto, essa falta de regulamentação foi suprida com a aprovação do Marco Civil da Internet, que estabelece princípios para o uso e controle da internet. Esses princípios incluem a neutralidade da rede, a liberdade de expressão e a privacidade (BRASIL, 2014).

No Brasil se há o entendimento da privacidade como direito fundamental e prevê a possibilidade de indenização pelo dano causado. Contudo, só houve uma regulamentação da matéria, propriamente dita, a partir de meados de 2000, antes eram usadas legislações de formas subsidiarias para os determinados casos concretos (BOFF; FORTES, 2014).

Um dos exemplos do uso de forma subsidiaria para a proteção de privacidade dos dados é com o Código de Defesa do Consumidor o qual prevê artigos como o art.43 (Lei nº 8.078/90), que dispõe em suma sobre a possibilidade de acesso pelo consumidor a qualquer espécie de dados cadastrados no banco de dados da empresa, também há a lei de habeas data que permite o conhecimento ou retificação de informações em bancos de dados de entidades governamentais ou de caráter público.

Por outro lado, parece haver uma proteção ampla por parte do legislativo, mas recentemente contraditoriamente foi aprovada a Lei do Cadastro Positivo (Lei nº 12.414/11), o qual permite a troca de dados entre instituições financeiras sobre informações de adimplemento ou não dos débitos, para então haver a formação criação de histórico de credito, então por seguinte criar uma linha de credito diferenciado, com juros diversos aos que estejam adimplentes em dia (bom pagador) .Há a Lei de acesso à informação (Lei nº 12.527/11), respaldada no inc. XXXIII do Art. 5 da CF:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (BRASIL, 1988).

Vale mencionar a Lei Carolina Dieckmann, Lei número 12.737/2012, que surgiu em um momento de ocorrência de diversos crimes cibernéticos, de informática,

como invasões bancarias, divulgação sem autorização de fotos pessoais, hackeamentos e então com a necessidade de tutelar bens jurídicos como privacidade e sigilo da informação e responsabilizar as infrações do mundo virtual.

Referido diploma legal, trouxe para o ordenamento jurídico brasileiro a criminalização da conduta de invasão de dispositivo informático, inserindo ao Código Penal brasileiro o artigo 154-A, que atualmente detém a seguinte disposição:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal" (BRASIL, 2012).

Outra lei importante para o ordenamento jurídico brasileiro, no que diz respeito a proteção de dados pessoais, foi o Marco civil da internet, sancionado em 2014, lei (número 12.965/14) ,tem a sua importância como a principal que regulamenta a utilização da internet, sob o prisma de 3 princípios ,são eles: Princípio da neutralidade da rede (trata-se da obrigação dos provedores de internet de tratar todos os dados que trafegam na rede de forma isonômica, sem distinção de conteúdo, origem, destino ou serviço); Privacidade (Esse princípio assegura a inviolabilidade e o sigilo da troca de informações entre os usuários e o da liberdade de expressão, prevendo a devida responsabilização e a quebra do sigilo de dados, sob intimação judicial, para os casos em que os dados coletados possam contribuir para descoberta de ilícitos) e princípio

da colaboração (estabelece que a governança da internet deve ser feita de forma colaborativa, envolvendo diversos setores da sociedade, como governo, empresas, sociedade civil e academia).

Portanto, como se pode observar, ante a evolução dos mecanismos tecnológicos, tem sido uma tendência a evolução das leis, de maneira que o ordenamento jurídico acompanhe tal evolução, sendo que o Marco Civil da Internet foi um importante ponto de partida para a evolução da legislação brasileira nesse sentido. Diante disso, a seguir, será feita uma breve contextualização a despeito da relevância desta lei para a temática ora abordada.

2.6 O marco civil da internet

Desde o ano de 1999, por meio da apresentação, no Senado Federal, do Projeto Lei 84/99, a qual ficou conhecida como Lei Azeredo, que buscava uma ampla punição penal para crimes cometidos virtualmente, observa-se a preocupação em se regular, juridicamente, as ações no mundo virtual. Diversas foram as reações a tal projeto, que a época fora motivo de críticas, tendo em vista seu potencial de "vigilantismo"[1], o qual levaria aos usuários da rede a expor e punir os criminosos virtuais (LEMOS, 2014).

Entretanto, muitas foram as reações favoráveis ao projeto, as quais viam a importância de se criar uma lei civil, para dispor sobre o assunto.

Conforme aduz Lemos, o Marco Civil da Internet foi criado como uma opção à chamada "Lei Azeredo", um projeto de lei que buscava implementar uma ampla legislação criminal para a internet e que recebeu esse nome em referência ao seu principal defensor e relator, o deputado Eduardo Azevedo (PSDB-MG). Muitos segmentos da sociedade brasileira acreditam que a aprovação da Lei Azeredo resultaria em um significativo retrocesso no cenário regulatório da internet no país (LEMOS, 2014).

[1] O Vigilantismo digital, cibervigilantismo ou Digilantes é conhecido pela prática de internautas que se utilizam dos recursos da internet e outras tecnologias digitais para combater alguma prática criminosa ou socialmente recriminada. O vigilantismo pode englobar os mais diversos temas, de golpes na rede à exploração sexual de crianças, passando por questões de proteção ambiental, direitos sexuais e corrupção. Nem sempre é claro o limite do vigilantismo como prática de combate aos crimes, pois há casos de justiceiros que cometem crimes para combater outros crimes, o que pode gerar problemas na justiça (LEMOS, 2014).

Diante desse contexto, o Marco Civil da Internet foi amplamente debatido e elaborado com a participação de diversos membros da sociedade civil, especialmente os usuários das redes sociais, com o objetivo de tornar o tráfego na internet mais justo e democrático, evidenciando que a internet não é mais “terra sem lei”. Como resultado, o Marco Civil da Internet é considerado um marco no ordenamento jurídico brasileiro.

Em 2010, quando o Marco Civil da Internet ainda estava em discussão, a Desembargadora Letícia Sardas utilizou os fundamentos presentes neste diploma legal para embasar a sua decisão em um Agravo de Instrumento. Ela destacou a importância do Marco Civil da Internet no Brasil, que estabelece os direitos dos cidadãos brasileiros na internet, em especial a regulação dos direitos e deveres relativos aos dados gerados pelos usuários durante a navegação. A desembargadora também observou que os registros relativos à conexão, como data, hora, duração e endereço IP, devem ser armazenados pelo provedor de acesso à internet, enquanto o registro de acesso aos serviços de internet, como e-mails e perfis em redes sociais, não é uma obrigação do provedor. No entanto, se o provedor decidir armazenar esses dados, ele deve informar o usuário e estabelecer o tempo de armazenamento. A desembargadora ressaltou que a alegação de impossibilidade técnica de cumprimento da decisão judicial não tem o poder de afastar a determinação concedida na Medida Cautelar e que a medida não traria prejuízo ao agravante. Além disso, ela aplicou a Súmula 372 do STJ, que estabelece as regras para a ação de exibição de documentos.[2]

O Marco Civil da internet, lei 12.965/2014, fora aprovado na Câmara dos Deputados no dia 25 de março de 2014, sendo sancionado um mês depois, pela então presidente Dilma Rousseff, na Conferência NET Mundial, em São Paulo (ABDET, 2015).

Desse modo, conforme já aduzido, anteriormente, tal lei fora o primeiro diploma legal elaborado, colaborativamente, entre a sociedade e o Poder Executivo, sendo que a própria internet fora o instrumento utilizado para debate.

A partir de sua promulgação, as relações virtuais passaram a ser, especificamente, reguladas, tendo em vista que, o Código Civil, lei utilizada anteriormente para tratar sobre o tema, dispunha de diversas lacunas.

---

[2] BRASIL. Tribunal de Justiça do Rio de Janeiro. Agravo de Instrumento número 0013822-08.2010.8.19.0000. Relatora Leticia Sardas. Data de Julgamento: 30/06/2010.

O Marco Civil da Internet é considerado uma referência internacional no estabelecimento de direitos e deveres no contexto da Internet. Ele busca equilibrar a proteção dos direitos individuais e a promoção da inovação e do desenvolvimento tecnológico. Sua implementação tem impacto significativo na forma como a Internet é regulada e utilizada no Brasil.

Por fim, o Marco Civil da Internet trata de diversos direitos, deveres, dos usuários e prestadores de serviço, sendo um diploma normativo, ao mesmo tempo, criticado e amado pela sociedade.

2.7 Do direito à privacidade e a proteção de dados pessoais

No final do século XIX, houve um aumento significativo na disseminação de novas tecnologias e métodos que levou ao surgimento de um debate sobre o direito à privacidade. Os pioneiros na área, segundo Doneda, foi Warren e Brandeis ao escrever um artigo em 1890 intitulado "O direito à privacidade", publicado na Harvard Law Review, onde criticaram a invasão de privacidade por jornais, fotografia e outras tecnologias emergentes na época, argumentando que as pessoas têm o direito de proteger sua privacidade e intimidade contra a invasão da imprensa sensacionalista e da exposição pública não autorizada de suas vidas privadas. Desde então, o direito à privacidade tornou-se um tema central no debate sobre as implicações sociais das tecnologias de informação e comunicação em constante evolução (DONEDA, 2016).

No século XX, a evolução do papel do Estado e a revolução tecnológica em curso contribuíram para alterar o significado e o escopo da proteção da privacidade. (DONEDA, 2016).

A proteção dos dados pessoais, embora fundamentada no direito à privacidade, extrapola seu escopo e pode ser compreendida como um fenômeno coletivo em razão dos danos causados pelo uso indevido dessas informações. De fato, esses dados são, em sua essência, fragmentados e demandam uma proteção jurídica coletiva específica.

Como acrescenta Doneda, pode ser difícil resolver todos os problemas decorrentes do processamento de dados pessoais em relação à proteção da privacidade. Isso ocorre porque o conceito não abrange os problemas individuais e coletivos decorrentes dos sistemas atuais de classificação e risco, como o uso de

informações genéticas de pacientes de planos de saúde ou a discriminação em supermercados com base no CEP (DONEDA, 2016).

Com o avanço das novas tecnologias, o armazenamento e processamento eficiente de dados pessoais possibilita a proteção da privacidade, bem como a combinação dessas informações. A mudança não se restringe apenas ao conteúdo dos direitos da personalidade, mas também aos conceitos presentes em sua própria nomenclatura, tais como a confidencialidade da informação, a proteção de dados pessoais e o direito à autodeterminação da informação, entre outros. Além disso, a proteção da propriedade, prevista na Constituição, ultrapassa os limites da privacidade, pois atualmente esses dados são considerados reflexos da própria personalidade do indivíduo. (MENDES, 2008).

A doutrina brasileira faz uso de uma profusão de termos distintos para se referir à privacidade: vida privada, intimidade, segredo, sigilo, recato, reserva, entre outros. Isso ocorre porque, tanto o constituinte quanto o legislador ordinário, ao elaborarem a Constituição de 1988 e o Código Civil de 2002, escolheram não fazer menção expressa ao termo “privacidade”, mas das expressões “vida privada” e “intimidade”, contudo não se encarregaram de diferenciá-las, papel que foi atribuído à doutrina.

O direito à vida privada e à intimidade são considerados ramificações do direito à privacidade, portanto, a diferenciação entre vida privada e intimidade não possui muita utilidade, vez que são atributos da personalidade que podem assumir o mesmo significado ou alcance jurídico em razão da subjetividade que carregam. Em razão disso, a jurisprudência tem utilizado a expressão privacidade para se referir, sem distinção, à proteção da intimidade e da vida privada. (SCHREIBER, 2013)

A Constituição de 1988 não menciona explicitamente o termo "privacidade", mas utiliza as expressões "vida privada" e "intimidade". A falta de uma definição clara desses conceitos na legislação permitiu que a doutrina jurídica elaborasse diferentes interpretações e distinções entre eles.

Assim, na doutrina brasileira, é comum encontrar uma variedade de termos e definições para se referir à privacidade, como vida privada, intimidade, segredo, sigilo, recato, reserva, entre outros. Cada termo pode ser usado em contextos específicos para abordar nuances e aspectos particulares relacionados à proteção da privacidade.

Independentemente da forma como é designada, a privacidade é consagrada como um direito fundamental e faz parte do conjunto de direitos que integra a

personalidade. A proteção à privacidade encontra-se tanto na legislação infraconstitucional, art. 21 do Código Civil, quanto na Constituição, no qual o constituinte alude expressamente à inviolabilidade da “intimidade” e da “vida privada”, assegurando no art. 5º, inciso X: “o direito a indenização pelo dano material ou moral decorrente de sua violação.”

A Constituição, Art. 5º, inciso XII e XI, faz menção ao termo “sigilo” ao garantir a inviolabilidade do sigilo das comunicações, das correspondências, das comunicações telegráficas, de dados e telefônicas e expande o âmbito da privacidade individual ao garantir a inviolabilidade da casa do indivíduo.

O legislador ordinário limitou-se a repetir o conteúdo do art. 5º, inciso X, da Constituição e, desta forma, falhou em desenvolver o comando constitucional para regular as hipóteses de violação à privacidade e oferecer mecanismos para prevenção e solução de conflitos.

No que tange aos remédios constitucionais, o habeas data (art. 5º, inciso LXXII) é considerado instrumento útil para coibir e corrigir violações à privacidade, sendo assim, uma base constitucional para o direito ao controle de dados pessoais. Portanto, o direito à privacidade, deve ser reconhecido em sentido genérico e amplo, “de modo a abarcar todas as manifestações da esfera íntima, privada e da personalidade, que o texto constitucional consagrou” (SILVA, 2013).

Ademais, a tutela da privacidade, em todas as suas perspectivas, deve garantir, antes de tudo, a liberdade da pessoa para a construção e desenvolvimento de sua identidade e esfera íntima. Nesse sentido, importante se faz abordar a despeito da Lei Geral de Proteção de Dados Pessoais (LGPD), que é um importante marco no ordenamento jurídico brasileiro para o tema em questão, conforme será demonstrado a seguir.

3. A LGPD: PRINCIPAIS ASPECTOS

A Lei Geral de Proteção de Dados (Lei nº 13.709/18 - LGPD) é um marco legal que entrou em vigor no Brasil em setembro de 2020 e tem por objetivo regulamentar a proteção de dados pessoais, estabelecendo regras claras para a entidades que coletam e tratam esses dados sendo uma importante ferramenta para proteger a privacidade dos cidadãos e regulamentar o tratamento de dados pessoais no Brasil, promovendo maior transparência e segurança. De acordo com a referida lei, é necessário obter o consentimento do titular dos dados para seu tratamento, além de garantir a segurança das informações e permitir seu acesso, sua correção e sua exclusão, quando solicitado.

3.1 Principais fundamentos da LGPD

A LGPD fornece uma estrutura com princípios e regras que regem todo o ordenamento jurídico. É uma lei relativamente pequena, dividida em dez capítulos e seções. Os regulamentos preliminares declaram os limites legais de aplicação, local de atuação, conceitos e princípios.

O artigo 1.º prevê o tratamento de dados pessoais, incluindo recursos digitais, por qualquer pessoa singular ou coletiva (pública ou privada) com vista à proteção dos direitos fundamentais, com destaque para a privacidade. O artigo 2.º, título I, descreve os fundamentos disciplinares para obter a proteção de dados de forma a respeitar a privacidade. Esse fundamento corrobora o que se encontra na Carta Magna, no art. 5, inciso X (MALDONADO, 2019).

O próximo fundamento é a autonomia informacional, que é bastante consistente porque é um alerta de que representa a capacidade de todos controlarem suas informações pessoais de alguma forma. Isso garante que uma pessoa possa decidir em determinadas circunstâncias se os dados podem ser processados (recolhidos, usados, transferidos) por terceiros, acessar bancos de dados para solicitar correção ou cancelamento de dados, porque todos os dados estão relacionados à vida de uma pessoa. Portanto, seu proprietário deve revisá-lo para decidir se deve ou não permitir o acesso e a quem conceder acesso (SÁ JUNIOR, 2019).

Posteriormente, a Seção III afirma a liberdade de expressão, informação, comunicação e opinião porque reconhece que o abuso da informação do titular também pode levar à violação daqueles direitos que são justificados por direitos e garantias constitucionais. Sabe-se que os primeiros fundamentos mostram uma preocupação com a proteção do indivíduo, e os demais incisos (V, VI e VII) indicam a preocupação do legislador com a livre iniciativa e o desenvolvimento econômico do país (SÁ JUNIOR, 2019).

Embora a proteção de dados pessoais seja discutida, é útil reconhecer a mudança de paradigma no desenvolvimento da tecnologia e da livre iniciativa do ponto de vista do desenvolvimento das pessoas e da sociedade. As normas de proteção à privacidade não podem, portanto, impedir o desenvolvimento econômico, tecnológico e inovador, pois se relacionam com os princípios da ordem econômica do art. 170 e seguintes da Constituição Federal, pois o objetivo da LGPD é proteger contra possíveis abusos do Estado ou de outros cidadãos em relação ao direito ao trabalho e ao engajamento (MALDONADO, 2019).

Além disso, o dispositivo da mesma constituição prevê indenização por danos causados pela violação da privacidade, amparo legal também se encontra no art. 21 do Código Civil/2002, que dá às vítimas de violações de privacidade a oportunidade de recorrer ao tribunal para garantir seu direito constitucional à privacidade (MALDONADO, 2019).

A partir disso, pode-se observar que a LGPD detém relevantes fundamentos no que diz respeito a proteção de dados pessoais. Nesse sentido, relevante se faz conhecer alguns dos principais princípios, contido nessa norma, de maneira a compreender como esta buscou resguardar o direito à privacidade nos meios digitais, o que será feito a seguir.

3.2 Princípios contidos na LGPD

Os princípios são o fundamento necessário do sistema jurídico. Nada pode ser determinado até que se verifique que corresponde a esta raiz fundamental, pois são parte necessária da interpretação dos textos legais. No entanto, a interpretação especial da norma LGPD leva em consideração apenas seu significado e aplicação específica (TEFFÉ, 2019).

Robert Alexy ajuda a distinguir as regras dos princípios:

> Crucial para a diferença entre regras e princípios é que os primeiros são padrões que exigem que algo seja aplicado o mais amplamente possível, dentro das possibilidades legais e factuais disponíveis. Os princípios são, portanto, comandos de otimização caracterizados pelo fato de que podem ser cumpridos de diferentes maneiras e a medida exata de sua satisfação depende não apenas de possibilidades fáticas, mas também jurídicas. O escopo das opções legais é determinado por princípios e regras conflitantes. (ALEXY, 2006, p.90).

Assim, os princípios são sempre aplicados, mais ou menos, ao contrário das regras que se aplicam ou não a um caso particular. Por isso, Robert Alexy segue definindo melhor as regras para dirimir dúvidas:

> [...] padrões que são sempre atendidos ou rejeitados. Se a regra se aplicar, faça exatamente o que ela diz; nem mais nem menos. Portanto, as regras envolvem determinar o que é factual e juridicamente possível. Isso significa que a diferença entre regras e princípios é uma diferença qualitativa, não uma diferença de grau. Toda norma é uma regra ou um princípio. (ALEXY, 2006, p.91).

O princípio da finalidade atribui ao órgão administrativo o dever de praticar o ato administrativo de acordo com a concretude da finalidade almejada pela lei. Enfatizando a LGPD, pretende dar ao titular dos dados o direito de analisar se há um motivo e uma necessidade para os dados coletados. Considerando que os dados só podem ser tratados com autorização do titular, sendo ainda necessário assegurar que não haja desvio da finalidade de recolha e tratamento acordada na legislação (SÁ JUNIOR, 2019).

A concretude da boa-fé evita que as sentenças sejam vagas ou criem dúvidas quando se referem a um princípio, pois considerando que o titular deve avaliá-las para aprovar a medida, deixa claro que ele pode não concordar para a proteção dos dados que você usa divulgados a terceiros. Assim, o dado deve estar completamente convencido do que ele transmite, confirmando (SÁ JÚNIOR, 2019).

O princípio da adequação está diretamente relacionado ao princípio da finalidade, pois segundo ele a finalidade deve ser seguida no tratamento de dados pessoais para evitar o uso indevido. É claro que informa o titular de outra garantia e dúvida se é garantido que os dados serão utilizados mais ou menos do que o acordado na legislação (TEFFÉ, 2019).

O princípio da necessidade também está relacionado ao princípio da finalidade, pois define os dados a serem coletados e tratados, ou seja, a menor quantidade possível de dados que seja suficiente para um determinado propósito (MALDONATO, 2019).

Esse princípio permite que os dados sejam transparentes para seu titular sendo chamado de acesso aberto. Seria inconsistente se o titular dos dados não tivesse livre acesso às informações relacionadas aos seus dados. Este princípio cria uma obrigação que é sólida porque um terceiro é responsável por abrir o arquivo para que o proprietário possa avaliar se foi feito corretamente. A integridade inclui a integridade dos dados vinculados, o que significa que o controlador não pode processá-los ou excluí-los arbitrariamente (HAGE, 2019).

Conforme Hage, o princípio da transparência é um meio para que a sociedade possa fiscalizar e controlar as atividades do setor público. Ele permite que informações sejam acessíveis e compreensíveis para todos, garantindo assim a responsabilização dos agentes públicos. Além disso, a transparência também é importante no contexto do tratamento de dados pessoais, permitindo que os titulares dos dados tenham acesso às informações sobre como seus dados estão sendo coletados, usados e compartilhados (HAGE, 2019).

O princípio do consentimento para Maldonado, implica que a eficácia de uma disposição legal depende da observância desse princípio, que deve ser seguido com especial atenção antes da obtenção do consentimento do titular dos dados. Isso está diretamente relacionado ao fato de que o titular deve estar plenamente ciente das condições de coleta, finalidade, tratamento, armazenamento, processamento e exclusão dos dados, com exceção dos segredos industriais e comerciais (MALDONADO, 2019).

A proteção de dados é fundamental para garantir a segurança e privacidade das informações pessoais dos titulares. O princípio da segurança é um dos pilares da LGPD e exige que os controladores e operadores de dados adotem medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Caso ocorra algum incidente de segurança, é importante que os responsáveis investiguem e adotem as medidas necessárias para minimizar os impactos e evitar que novas violações ocorram. Em alguns casos, é possível que sejam aplicadas sanções e responsabilidades civis e penais. (TEFFÉ, 2019).

Assim como a segurança define o padrão para a concepção do projeto, a prevenção é um elemento crucial na proteção de dados e segurança da informação. A adoção de medidas preventivas, como a criptografia, o controle de acesso, a monitorização constante e a realização de testes de segurança, podem evitar ou minimizar os efeitos de possíveis falhas de segurança. Além disso, a prevenção pode reduzir o risco de violações de dados e outras consequências negativas, como danos à reputação da organização e sanções legais. É importante lembrar que a segurança da informação é um processo contínuo e que as medidas de prevenção devem ser atualizadas e adaptadas constantemente para acompanhar as mudanças tecnológicas e as ameaças emergentes. (SÁ JUNIOR, 2019).

De acordo com o princípio da responsabilização e prestação de contas, o controlador ou operador deve demonstrar todas as medidas eficazes que podem ser utilizadas para demonstrar o cumprimento da LGPD, bem como a eficácia das medidas implementadas. Refere-se às consequências de infringir a lei. Ou seja, o tratamento dos dados é lícito e de acordo com as normas, se cumprir os regulamentos exigidos por lei, a negligência e os danos causados ao titular acarretarão responsabilidade (MALDONATO, 2019).

Pelo que foi exposto, é perceptível que os operadores e processadores de dados devem estar cientes pela lei de que são responsáveis pelo cumprimento de todas as disposições dela decorrentes, como os princípios, bases e objetivos básicos delineados. Esses agentes podem até responder civilmente se descumprirem as regras, o que será analisado na próxima seção.

3.3 Responsabilidade civil na LGPD

Do ponto de vista da responsabilidade dos operadores, a proteção de dados é de extrema importância. Com o desenvolvimento da tecnologia, o mercado da informação faz parte do cotidiano, e por isso o prejuízo causado ao titular dos dados é consequência direta e relativa do tamanho da importância econômica e abrangência (MALDONATO, 2019).

A LGPD inova ao estabelecer um conjunto de condições de tratamento de forma consistente, uniforme e legal. No entanto, esta é uma atividade que envolve riscos e pode causar danos (patrimonial ou moral) ao proprietário.

Nos casos em que o dano tenha sido causado pelo tratamento de dados, há, portanto, regras estabelecidas em lei sobre como a compensação deve ocorrer.

Com relação à responsabilidade civil prevista na LGPD, há clara distinção entre relações civis e relações de consumo. Nas relações civis, o âmbito é o aspecto contratual e aplica-se a regra geral do direito civil – a responsabilidade. Isso deve levar em conta a negligência do agente e, se houver responsabilidade objetiva, deve ser explicitamente apontado. No que diz respeito às relações de consumo, a reparação pode ser realizada em relação a uma determinada pessoa ou comunidade, dependendo da natureza da atividade de processamento de dados. Isso se torna mais preciso e informativo à medida que as medições aumentam (TEFFÉ, 2019).

Outro ponto importante que deve ser abordado na LGPD é que a solidariedade entre controladores e operadoras em sua responsabilidade por danos nos termos inciso I, §1º, do art. 42, pois é relevante para todos os agentes de processamento o cumprimento das leis e segurança operacional, independentemente, de um seguir as ordens do outro. Isso significa que uma ou ambas as partes podem ser responsabilizadas por danos (TEFFÉ, 2019).

A responsabilidade civil objetiva aplica-se por previsão legal quando o legislador constatar fragilidade estrutural de uma das partes. No caso da LGPD, isso está previsto em duas situações: tratamento de dados no âmbito das relações de consumo de acordo com o artigo 45 da lei, e tratamento de dados pelo poder público, conforme art. 37, §6º da Constituição (SÁ JUNIOR, 2019).

Segundo o Supremo Tribunal Federal, não há responsabilidade objetiva, especialmente por atos comissivos. Esse é um entendimento que ainda não abordou as idiossincrasias do processamento de dados e deve ser observado em estudos futuros (MALDONADO; BLUM, 2019).

O entendimento mencionado se refere à responsabilidade civil objetiva, que é aquela em que o agente causador do dano é responsável independentemente de ter agido com culpa ou dolo. No Brasil, a regra geral é a da responsabilidade subjetiva, em que é necessário comprovar que o agente agiu com culpa ou dolo para que seja responsabilizado pelo dano causado.

No contexto do processamento de dados, as idiossincrasias envolvem questões como a complexidade dos sistemas de tecnologia da informação e a dificuldade de atribuição de responsabilidades em casos de vazamento ou violação de dados pessoais. Nesse sentido, é importante que sejam realizados estudos

específicos para avaliar a possibilidade de se aplicar a responsabilidade civil objetiva em situações relacionadas ao processamento de dados.

No entanto, é importante destacar que, mesmo que a responsabilidade objetiva não seja aplicável, os responsáveis pelo processamento de dados ainda podem ser responsabilizados caso tenham agido com culpa ou dolo na proteção dos dados pessoais. Além disso, o Marco Civil da Internet e a Lei Geral de Proteção de Dados estabelecem regras claras sobre a responsabilidade dos controladores e operadores de dados pessoais, incluindo a necessidade de adoção de medidas de segurança adequadas para proteger esses dados.

Portanto, já se sabe que a LGPD traz um novo paradigma para a gestão de dados pessoais, garantindo a liberdade e a privacidade dos titulares dos dados pessoais. E para atingir seu objetivo principal, esta norma impõe restrições, obrigações a todas as pessoas, sejam elas pessoas físicas ou jurídicas, sejam elas pessoas físicas ou jurídicas, que tratem dados pessoais digitalmente ou de outra forma, e imponha penalidades.

Na prática, porém, as obrigações e a responsabilidade pelos danos causados ao titular dos dados cabem aos processadores, ou seja, o processador responsável e o mantenedor. A fim de cumprir efetivamente as diretrizes da LGPD e minimizar o risco de um evento gerar passivos, os processadores de dados responsáveis devem zelar para que seja assegurada a segurança dos dados sob controle de terceiros (MALDONADO; BLUM, 2019).

Embora essas medidas temporárias não protejam os processadores de todos os problemas futuros, elas garantem que o processamento de dados seja mais compatível com as disposições da LGPD, o que garante que os riscos aos dados que possam prejudicar o titular sejam minimizados.

Por conseguinte, pelo exposto, infere-se a relevância do instituto da responsabilidade civil no ordenamento jurídico brasileiro, especialmente no que diz respeito à proteção da vida humana, da honra e da reputação e do direito à privacidade na internet.

A questão da proteção de dados pessoais mostra-se tão atual e de suma importância, que o próprio legislador, por meio da Emenda Constitucional 115/2022, deu a este direito status de direito e garantia fundamental, conforme será analisado no tópico que segue.

3.4 A Emenda Constitucional 115/2022 e a privacidade

A Emenda Constitucional nº 115 (EC 115/22), promulgada em 11 de fevereiro de 2022 tornou a proteção de dados pessoais um direito fundamental. Assim, torna-se ainda mais contundente e necessária a defesa da privacidade e, como resultado desta, a salvaguarda da dignidade humana consubstanciada no livre desenvolvimento da personalidade da pessoa natural.

Em decorrência disso o artigo 5º, da Constituição da República Federativa do Brasil (CRFB/1988) que previa a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, agora, também passou a conter, no seu inciso LXXXIX, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Assim, uma significativa mudança parece advir dessa nova configuração sistêmica de proteção do instituto da privacidade, pela proteção dos dados pessoais que, agora, possui expresso agasalho constitucional, hierarquicamente posicionado no rol dos direitos fundamentais.

Os dados pessoais são elementos do direito à privacidade que não recebeu proteção institucional recente, mas ainda em 1948, quando fora previsto no art. 12 da Declaração Universal dos Direitos do Homem:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e propriedade. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei (ONU, 1948).

Uma grande influência no campo da proteção de dados, advém do fator econômico, porque diante das inúmeras notícias de vazamentos e exposições de dados pessoais, passou-se a exigir maior comprometimento das empresas para a proteção dos dados que coletavam ou compartilhavam. A boa imagem da empresa passou a ser associada ao grau de comprometimento com a guarda dos dados elevando a confiança do público, gerando perdas ou ganhos econômicos, conforme os meios que adota para garantir a proteção.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, em 24 de outubro de 1995, consagrou-se como um instrumento relevante para exigir de governos e

demais instituições, sistemas mais robustos de proteção da privacidade no âmbito europeu.

Em seguida, o General Data Protection Regulation 2016/67940 (GDPR) importante norma da União Europeia (UE) que sucedeu a Diretiva 95, intensificou a obrigatoriedade de uma nova governança, mais adequada à proteção e à segurança da privacidade. O GDPR reverberou para todos os países que mantinham contratos com a UE impondo condições e exigências de compliance para realização de contratos. Tanto a Diretiva 95 quanto o GDPR influenciaram sobremaneira os países com os quais possuem relações comerciais, entre eles o Brasil[3].

Portanto, a Emenda 115/2022, ao tornar o direito à proteção de dados pessoais um direito fundamental, inscrito hierarquicamente, no ápice da pirâmide constitucional visou consagrar a proteção integral do indivíduo, principalmente, no que diz respeito a honra e imagem da pessoa, sob os aspectos digitais.

De acordo com Tibúrcio “o fato de a Proteção de Dados ser agora uma cláusula pétrea impede que se tramite no Legislativo proposta de emenda tendente a suprimir ou reduzir a proteção constitucional conferida a esse direito” (TIBÚRCIO, 2022).

Para melhor compreender essa nova configuração exige-se, necessariamente, um novo olhar que vislumbre a nova configuração dimensão do livre desenvolvimento da personalidade da pessoa natural, que existe no direito à privacidade daqueles que atuam no setor público, em especial no que diz respeito aos componentes das Forças Armadas.

O livre exercício dos direitos da personalidade e seu desenvolvimento implicam em tornar compatível a proteção de dados pessoais às novas exigências da sociedade digital. Para que isto ocorra devemos realizar um exercício constante de girar a situação fática para transparecer suas formas e, assim, encontrar os meios adequados à proteção integral da dignidade humana.

De acordo com Bioni BR, é crucial que o direito à proteção dos dados pessoais seja reconhecido como uma nova categoria de direitos da personalidade, a fim de ampliar a cláusula geral de proteção à pessoa humana. Caso contrário, corre-se o risco de limitar seu significado aos conceitos e à dinâmica do direito à privacidade, o

[3] Regulamento Geral de Proteção de Dados Pessoais (GDPR) da União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 27/032023.

que tornaria impossível uma regulamentação adequada do fluxo de informações como uma ferramenta promocional para a pessoa humana (BIONIBR, 2019).

Assim sendo, a regulamentação da proteção de dados pessoais como um direito fundamental do indivíduo pela EC 115/22 proporciona mais um meio de proteção ao direito da personalidade.

Dessa forma, é evidente que as alterações na legislação relativa à proteção de dados geraram grandes consequências na sociedade, em especial para as empresas que lidam diretamente com o tratamento de informações pessoais. O próximo capítulo deste trabalho discutirá os principais impactos para essas empresas e os desafios que se apresentam para a efetiva implementação da LGPD no Brasil.

4. DIREITO FUNDAMENTAL A SAÚDE E A APLICABILIDADE DA LGPD

O presente capítulo tem por finalidade analisar os principais aspectos do Direito à Saúde sob o contexto da Lei Geral de Proteção de dados, em especial, no que diz respeito a proteção de dados sensíveis, os quais necessitam de consentimento especial para seu tratamento, conforme será abordado ao longo deste tópico.

4.1 Do direito à saúde

Sabe-se que a promulgação da Constituição Federal de 1988, em 5 de outubro, foi um grande marco, principalmente, por ter sido promulgada após o fim de um longo período ditatorial em que o Brasil se encontrava, o qual ficou evidenciado pela grande repressão e retirada de direitos dos cidadãos. Sua formulação iniciou-se em 1987, momento em que o país passava por um processo de redemocratização. Deste modo, a Constituição surgiu como o marco de devolução e consagração dos direitos sociais, econômicos, políticos e culturais.

Com a promulgação da Constituição de 1988, uma nova ordem constitucional foi estabelecida no Brasil, fundamentada no Estado Democrático de Direito. Esse princípio foi consagrado no artigo primeiro da Carta Magna, que trata dos princípios fundamentais, incluindo a soberania, a cidadania e a dignidade da pessoa humana. Dessa forma, o princípio democrático foi firmado na ordem jurídica brasileira, estabelecendo que “todo poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição” (FIGUEIREDO, 2017, p.150)

A Constituição de 1988 foi apelidada de Constituição Cidadã por ter sido elaborada com a participação ativa da sociedade civil e por trazer importantes avanços na proteção dos direitos fundamentais e sociais. Além de restabelecer a democracia no país, a Constituição garantiu direitos que haviam sido suprimidos durante a ditadura militar, como a liberdade de expressão, de associação e de manifestação.

Um dos grandes avanços da Constituição de 1988 foi a consagração do direito à saúde como um direito social, garantindo a todos o acesso aos serviços públicos de saúde de forma gratuita e universal. Isso significa que é dever do Estado garanti-lo a

todos, pois, este é tão importante quanto o direito à vida, e medidas devem ser recepcionadas para que se consigam concretizar tal direito.

Com o transcorrer dos anos, as alterações na definição do que seria saúde ajudaram ainda mais na efetivação deste direito, segundo Figueiredo, mencionada evolução permitiu um entendimento mais abrangente do que realmente seria essa garantia hodiernamente. Constituindo-se com um direito humano e fundamental, o Direito a Saúde é fruto de uma longa e expressiva jornada na formulação não somente de um direito, porém também de uma ideia mais própria do que seria a saúde (FIGUEIREDO, 2017).

Conforme destacado por Pilau Sobrinho, a garantia do direito à saúde pode ser interpretada de diversas maneiras, a depender da titularidade e da divisibilidade do bem tutelado. Embora haja um direito individual à saúde, enquanto um direito restrito à incolumidade ou segurança pessoal, a tendência contemporânea deve ser centrada na dimensão de proteção dos direitos metaindividuais da sociedade (SOBRINHO, 2016).

Tendo em vista a importância global deste direito, fora firmada pela Declaração Universal dos Direitos Humanos em 1948, onde, reconheceu a saúde como um direito humano fundamental, estabelecendo a obrigação dos Estados de garantir um padrão de vida capaz de assegurar a saúde e o bem-estar.

Apenas, como já mencionado, com a Constituição Federal de 1988, que fora efetivado o direito a saúde no Brasil, garantindo-o, em seu artigo 6º, como um direito social e no artigo 196, um direito de todos. O Estado tem a responsabilidade de assegurar o acesso universal e igualitário aos serviços de saúde e promover medidas de prevenção e tratamento de doenças para proteger a saúde individual e coletiva da população.

De acordo com Sarlet, a Carta da República de 1988 elevou o direito a saúde a um patamar irrevogável, agasalhando-o não apenas como um bem jurídico digno de tutela, porém indo mais além, dando a este um status de direito fundamental, reconhecendo-lhe maior proteção jurídica (SARLET, 2012).

O direito fundamental à saúde é reconhecido como direito humano universal e previsto na Constituição Federal brasileira. A garantia deste direito implica na necessidade de proteção dos dados pessoais dos indivíduos, especialmente no contexto da saúde, e é neste sentido que a Lei Geral de Proteção de Dados (LGPD) traz importantes disposições.

4.2 Dados sensíveis e a LGPD

Os dados pessoais sensíveis são definidos como aqueles que estão diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo. Dessa forma, são considerados dados pessoais sensíveis informações que dizem respeito à origem racial ou étnica, crença religiosa, opinião política, filiação a sindicato ou a organizações religiosas, filosóficas ou políticas, dados relativos à saúde ou à vida sexual, dados genéticos ou biométricos quando vinculados a um indivíduo.

O conceito de dados sensíveis é abordado no artigo 5º, II, da Lei Geral de Proteção de Dados, que inclui informações relacionadas à saúde. Esses dados são considerados extensões da personalidade do indivíduo e são relevantes para sua privacidade e identidade, merecendo, portanto, uma proteção jurídica mais robusta. De acordo com Dallari e Monaco, levando em conta o artigo 35 do Regulamento Geral de Proteção de Dados (RGPD), informações pertinentes à saúde incluem aquelas que dizem respeito ao estado de saúde do titular de dados e que revelem informações sobre sua saúde física ou mental no passado, presente ou futuro (DALLARI; MONACO, 2021).

Assuntos relacionados à saúde são de grande relevância, uma vez que afetam diretamente a privacidade e a intimidade do indivíduo, tornando-se, assim, dados sensíveis. Consequentemente, é necessário que haja mecanismos mais rigorosos que garantam a proteção desses dados.

Segundo Tinto, os dados médicos e genéticos são considerados excepcionalmente sensíveis pelas leis de proteção de dados atuais, e possuem um status especial que requer medidas adicionais de proteção, segurança e confidencialidade (TINTO, 2018).

Outra questão importante de ser frisada seria o fato de que a divulgação destes dados poderia vir a causar uma possível discriminação a um indivíduo, justificando assim a relevância de sua maior proteção, visto que detém um grande potencial de atingir os direitos humanos. Desse modo, o compartilhamento não autorizado destas informações pode vir a causar discriminação e estigmatização social aos seus titulares (VIEIRA; COSTA, 2021).

O setor médico, coleta e processa grandes quantidades de dados pessoais com base nos serviços prestados aos pacientes e tem grande responsabilidade pela proteção desses dados.

No entanto, Tinto defende que o problema das violações de dados sensíveis em hospitais é agravado quando são considerados “devassáveis”. Diante disso, as organizações de saúde precisam proteger melhor a confidencialidade dos dados do paciente por meio de fortes políticas de privacidade que possam garantir transparência, simplicidade e acessibilidade do paciente. Entende-se, portanto, que as instituições médicas devem zelar pela validade dos direitos de confidencialidade do paciente e entender que são meras guardiãs das informações pertencentes aos pacientes. Os pacientes são, portanto, muito importantes porque são proprietários dos dados e devem ser informados sobre como eles são usados (TINTO, 2018).

Consequentemente, a LGPD define em seu artigo 5º, inciso V, o titular como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. É importante ressaltar que os direitos do titular dos dados, independentemente de serem sensíveis ou não, estão previstos no artigo 18 da LGPD, garantindo a toda pessoa física a titularidade plena dos dados que se referem a ela. Além do direito de propriedade, são concedidos os seguintes direitos: confirmação da existência do tratamento; acesso aos dados; informações sobre o compartilhamento; correção de dados; eliminação de dados; portabilidade de dados; possibilidade de não consentimento; e retirada do consentimento (BRASIL, 2018).

Os titulares dos dados estão no centro dos debates sobre proteção de dados, pois, as disposições normativas tratam especialmente de garantir seus direitos, visto que são os verdadeiros detentores dos dados. Assim, a LGPD conferiu a estes um protagonismo, um conjunto de direitos que devem ser respeitados durante o processo de tratamento de dados, como o direito de solicitar a anonimização e a exclusão de dados desnecessários ou tratados com base no consentimento (DALLARI; MONACO, 2021).

Segundo Aragão e Schiocchet, a LGPD tem como princípio fundamental que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações pessoais, especialmente aquelas que as identificam, permitindo que possam limitar esse processo. Para que haja uma evolução no tratamento desses dados, é essencial que haja uma finalidade determinada, com medidas adequadas para prevenir danos e proteger as informações, mantendo-as apenas quando necessário e com o consentimento do titular durante todo o processo. Além disso, o titular tem o direito de acessar seus dados e solicitar sua exclusão. (GREGORI, 2020).

Uma relevante questão, trata do consentimento, visto que o artigo 7º, I, da LGPD afirma que o tratamento de dados pessoais apenas pode ocorrer com o consentimento de seu titular. Desse modo, o ordenamento normativo dá maior privilégio a participação ativa de seu titular, mediante a prioridade de seu consentimento (BRASIL, 2018).

A autorização do titular deve ser concedida de maneira voluntária, informada e inequívoca, indicando que seus dados pessoais serão processados para um propósito específico, conforme descrito no Artigo 5º, XII da LGPD.

Conforme Aragão e Schiocchet, o termo "livre" refere-se à ação do proprietário sem qualquer tipo de coação física, moral, mental ou artificial. Para obter informações, o titular deve ser informado de maneira clara e compreensível sobre o uso e o compartilhamento de suas informações. No entanto, uma finalidade específica requer a indicação clara e precisa dos objetivos do processamento de dados, proibindo licenças e usos gerais que se afastem do contexto final (GREGORI, 2020).

Para Albuquerque, o consentimento informado é uma escolha voluntária e informada que visa promover a autonomia, a autodeterminação, a integridade física do paciente. Entende-se que os pacientes têm direito a: participar nas decisões sobre os seus cuidados de saúde; de participar ativamente no aconselhamento sobre seus cuidados; de retirar o consentimento sem retaliação e ao consentimento informado sem coerção ou influência indevida. A partir disso, o autor obtém o direito de respeitar sua vida privada:

> Tem uma ampla gama de aplicações no atendimento ao paciente, incluindo o direito de recusar qualquer tipo de tratamento, o direito de fazer escolhas quanto a visitas e exames físicos por profissionais médicos e o direito à confidencialidade das informações de saúde que eles respeitam. Direito de consentir em qualquer tipo de procedimento (ALBUQUERQUE, 2016).

Portanto, no âmbito da LGPD, os titulares devem ser notificados sobre o uso e a divulgação de seus dados de forma clara e compreensível. A finalidade declarada para o uso e processamento da informação deve ser clara e específica, sendo proibida a permissão geral e o uso fora do contexto.

Segundo Dove e Taylor, a divulgação de dados pessoais sempre acarreta riscos, os dados pessoais de saúde podem ser considerados mais arriscados do que outros, pois, há uma suposição de os dados pessoais não podem ser usados para colocar o paciente em risco, o que os autores discordam. O consentimento, portanto,

respeita os indivíduos como atores e tem uma função protetora, pois, os indivíduos têm o direito de assumir, voluntariamente, os riscos de divulgação e uso de seus dados com base nessas características. Dessa forma, o consentimento funciona como uma proteção, pois evita erros que constituem um processo contínuo no qual uma pessoa pode mudar de ideia (DOVE; TAYLOR, 2021)

Neste contexto, enfatiza-se que os pacientes são os verdadeiros proprietários de suas informações e, portanto, devem desempenhar um papel na proteção de seus dados. Portanto, fica claro que ter processos e ferramentas para proteger esses dados é essencial para garantir a confidencialidade dos dados do paciente. Porque sem proteção de dados, não se pode falar sobre a confidencialidade dos dados do paciente.

4.3 Tratamento dos dados de saúde

No tocante à guarda dos prontuários, os profissionais ou a instituição que assistem o paciente são responsáveis por armazená-los de modo seguro (Art. 87 §2º, da Resolução CFM 2.227/2018), seja em meio físico ou digital, de modo a preservar-lhes o conteúdo e, consequentemente, o segredo e a não violação à esfera de privacidade e intimidade do assistido. Na área da saúde, portanto, a noção de que os dados de saúde são espécies de dados sensíveis encontra respaldo na regulamentação ética e administrativa. O profissional da saúde, para atuar conforme a ética, deve partir da premissa de que o histórico médico de um paciente contém informações sensíveis cujo vazamento acidental ou voluntário pode ser catastrófico para a vida dele e de seus familiares e com efeitos irreversíveis (LUCIANO; BRAGANÇA; TESTA, 2011).

Dados os riscos envolvidos no tratamento de dados de saúde, tem se formado uma legislação setorial robusta para impor obrigações e padrões mínimos de segurança no dever de guarda e manuseio dos registros dos pacientes. Processo este que vem se intensificando com o surgimento de tecnologias da informação e comunicação para mediar a atenção à saúde, as denominadas “e-Saúde”, que englobam serviços como tele consultorias, telediagnóstico, segunda opinião formativa, tele cirurgia, tele monitoramento, teleducação e prontuário eletrônico (KAMEDA; PAZELLO, 2015).

Com relação às tecnologias de e-Saúde, como o prontuário eletrônico e a telemedicina, também existem normas específicas que regulamentam o uso dessas tecnologias, tais como a Resolução nº 1.821/2007 do Conselho Federal de Medicina, que trata da telemedicina, e a Resolução nº 2.232/2019, que dispõe sobre o uso de sistemas eletrônicos para a guarda e manuseio de prontuários médicos.

Dessa forma, é fundamental que os profissionais de saúde e as instituições de saúde sejam diligentes na adoção de medidas de segurança e privacidade de dados, a fim de proteger a saúde e a privacidade dos pacientes, além de estarem em conformidade com as normas e leis em vigor.

Segundo Maldonado, o prontuário médico, trata-se de documento único que reúne todos os dados da assistência prestada ao paciente, a permitir uma prestação continuada. A Resolução CFM nº 1.638/2002, além de trazer o conceito de prontuário médico, traz informações sobre seu conteúdo essencial e as atribuições de responsabilidade sobre preenchimento, guarda e manuseio, bem como torna obrigatória a criação de Comissão de Revisão de Prontuários, a quem compete observar a qualidade dos dados inseridos no prontuário e verificar a presença dos seguintes requisitos mínimos necessários para sua efetivação. Esses requisitos incluem a identificação completa do paciente, registro da anamnese, exame físico, exames complementares solicitados e seus resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento realizado, evolução diária do paciente, descrição de todos os procedimentos realizados e identificação dos profissionais responsáveis, com assinatura eletrônica quando armazenado em meio eletrônico, e, nos casos de prontuários em papel, a legibilidade da letra do profissional, identificação clara dos profissionais envolvidos, incluindo assinatura e número do CRM. (MALDONADO, 2015).

É crucial que o prontuário médico contenha todas essas informações para assegurar a qualidade do atendimento ao paciente e a continuidade dos cuidados prestados. Além disso, o prontuário médico é considerado um documento legal e pode ser utilizado como prova em processos judiciais. Assim, é de extrema importância que seja preenchido de forma clara, completa e objetiva.

Por sua vez, a Resolução CFM nº 1.821/2007, que revogou a Resolução CFM nº 1.639/2002, trouxe respaldo legal ao uso cada vez mais frequente de sistemas informatizados de guarda e manuseio dos prontuários, o chamado prontuário eletrônico do paciente (PEP) ou ainda prontuário médico eletrônico (PME). A

legislação veio a tornar possível a eliminação total de prontuários em suporte de papel, desde que garantidos padrões mínimos de segurança aos sistemas informatizados aptos a garantir a preservação integral dos dados, o que compreende o uso de certificação digital e método de indexação que permita criar arquivo organizado, possibilitando a pesquisa de maneira simples e eficiente (KAMEDA; PAZELLO, 2015).

Cientes da complexidade de aprofundamento dos aspectos técnicos sobre o tema, o Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) firmaram um convênio de cooperação técnica científica para a elaboração de requisitos e avaliação da conformidade de sistemas de informação, mediante a edição contínua de manuais de certificação e expedição de selos de qualidade. O SBISCFM mantém em seu site cartilhas explicativas sobre a utilização de PEPs, bem como lista atualizada dos sistemas ativos certificados e auditados pelo convênio, com informações detalhas sobre o grau de segurança e as funcionalidades de cada sistema, o que denota a preocupação do setor em garantir o tráfego seguro de informações sensíveis de pacientes (LUCIANO; BRAGANÇA; TESTA, 2011).

No que tange aos prontuários, a migração para sistemas de informação eletrônicos apresenta inúmeras vantagens que contribuem para a eficiência na prestação dos serviços de saúde e qualidade dos dados: maior legibilidade, acurácia, compartilhamento remoto, capacidade de processar grande volume de dados, entre outros. Porém, apesar do ganho de eficiência da redução de custos no longo prazo, a migração demanda um complexo e custoso processo de implementação, já que os dados sensíveis não podem estar sujeitos ao armazenamento em bases de dados vulneráveis.

Pesquisas indicam que a migração para prontuários eletrônicos ainda enfrenta uma série de desafios, os quais são descritos por Serpa Neto como: a falta de interoperabilidade entre os PME e outros sistemas de informação, não apenas entre diferentes sistemas, mas até dentro de um mesmo hospital ou clínica; o alto custo de sua implementação e de sua manutenção; e o impacto negativo real e/ou observado no fluxo de trabalho dos profissionais (SERPA NETO, 2017).

Apesar das barreiras técnicas e financeiras à plena migração dos estabelecimentos para sistemas eletrônicos, entende-se que a utilização das Tecnologias da Informação e Comunicação permitirão significativo salto qualitativo na prestação da saúde, de modo que há um esforço legislativo contínuo no sentido da implantação de padrões de informação e interoperabilidade entre sistemas, a permitir

a melhoria e modernização dos atendimentos em saúde, bem como uma maior segurança no tratamento de dados de saúde.

O início foi dado pelo Ministério da Saúde, por meio da Portaria 2.073/2011, que definiu parâmetros de estruturação dos dados de saúde para a implementação de um Registro Eletrônico de Saúde (RES) e a interoperabilidade entre sistemas de informação do Sistema Único de Saúde (SUS) operantes em municípios, estados e União, e de saúde suplementar, com vistas ao compartilhamento de dados "em meio seguro e com respeito ao direito de privacidade" (art. 2º, II).[4]

Do ponto de vista da privacidade no uso dos RES, enquanto a Portaria 2.073/2011 promove a utilização de uma arquitetura de dados e tem como escopo principal a promoção da segurança no compartilhamento de informações, a Portaria nº 940/2011, que regulamenta a criação do Sistema Cartão no âmbito do SUS, traz medidas expressas sobre garantia de sigilo no tratamento de dados. Além de abordar expressamente a privacidade ao colocar como um dos objetivos do cartão SUS: “Art. 4º, III segurança tecnológica da base de dados, respeitando-- garantir a se o direito constitucional à intimidade, à vida privada, à integralidade das informações e à confidencialidade”.[5]

Em conformidade com a Portaria 2.073/2011 mencionada anteriormente, a Agência Nacional de Saúde Suplementar (ANS), por meio das Resoluções Normativas nº 305 e 341/2012[6], instituiu o padrão TISS (Troca de Informação de Saúde Suplementar) como obrigatório para a troca de informações dos beneficiários de planos privados de assistência à saúde no âmbito da saúde suplementar, com o objetivo de possibilitar a interoperabilidade entre os sistemas de informação das operadoras de saúde e a adoção de "normas nacionais de informação, terminologia única e identificadores exclusivos".

Em relação ao tratamento de dados e requisitos de segurança para equipamentos médicos, a Agência Nacional de Vigilância Sanitária (ANVISA) editou

---

[4] Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Dispõe sobre a criação do Prontuário Eletrônico do Paciente no âmbito do Sistema Único de Saúde - SUS. Diário Oficial da União, Brasília, DF, 1 set. 2011. Seção 1, p. 48

[5] Ministério da Saúde. (2011). Portaria nº 940, de 28 de abril de 2011. Institui o Cartão Nacional de Saúde e estabelece diretrizes para sua utilização. Recuperado de http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html

[6] ANS. Resolução Normativa nº 305, de 9 de outubro de 2012. Diário Oficial da União, Brasília, DF, 11 out. 2012. Seção 1, p. 93-98;
ANS. Resolução Normativa nº 341, de 28 de dezembro de 2013. Diário Oficial da União, Brasília, DF, 30 dez. 2013. Seção 1, p. 104-109.

medidas regulatórias exigindo certificação compulsória de equipamentos que visam garantir a presença de mecanismos de segurança da informação, tendo em vista a importância dos dados sensíveis que trafegam em softwares médicos, bem como a interoperabilidade entre sistemas (RDC nº 40/2015)[7].

O fato é que o debate acerca da proteção de dados de saúde tem se intensificado com o surgimento de redes de telessaúde e desenvolvimento da telemedicina, que surgem como ferramentas importantes para o enfrentamento dos desafios contemporâneos dos sistemas de saúde universais. Por isso, é fundamental que sejam estabelecidos padrões de segurança e privacidade para o uso dessas tecnologias, a fim de garantir que os dados dos pacientes sejam protegidos e que seu uso ocorra de forma segura e adequada.

No tocante à proteção dos dados produzidos em atividades de telessaúde no SUS, compete à Coordenação Nacional de Telessaúde Brasil Redes garantir a interoperabilidade e segurança das informações:

> Art. 7º Compete à Coordenação Nacional do Telessaúde Brasil Redes: [...] V definir os padrões tecnológicos de interoperabilidade, conteúdo e segurança que permitirão a troca de informações entre os sistemas que viabilizam a operação do Telessaúde Brasil Redes e os diferentes sistemas de informação do SUS, incluídos o Cartão N acional de Saúde e o Sistema de Cadastro Nacional de Estabelecimentos de Saúde (SCNES); VI definir o conjunto de dados que fará parte do Registro Eletrônico de Saúde (RES) a partir das Teleconsultorias realizadas, visando à implementação de um registro nacional e longitudinal, conforme Portaria nº 2.073/GM MS, 2073/GM/MS de 31 de agosto de 2011; e (Retificado no DOU nº 209 de 31.10.2011, Seção 1, página 74)(BRASIL. Ministério da Saúde. Portaria nº 2.546, de 27 de outubro de 2011. Diário Oficial da União, Brasília, DF, 2011. Seção 1, p.48)

Para além das inovações na comunicação entre profissionais da saúde, as tecnologias da informação e comunicação trouxeram possibilidades inovadoras para uso da telemedicina diretamente na relação profissional e paciente, tais como a teletriagem médica, a teleconsulta, telediagnóstico, telecirurgia, teleconferência de ato cirúrgico.

A atividade, que está em pleno desenvolvimento na prática, chegou a ser regulamentada pelo CFM na Resolução CFM nº 2.227, no dia 13 de dezembro 2018, cujo objetivo era permitir e regulamentar a prática da modalidade no país, entretanto,

---

[7] ANVISA. Resolução da Diretoria Colegiada - RDC nº 40, de 26 de maio de 2015. Dispõe sobre requisitos de segurança para o funcionamento de equipamentos médicos. Disponível em: http://portal.anvisa.gov.br/documents/10181/1232766/RDC_40_2015_.pdf/b3ea963c-8aa8-41c1-b617-48c2e1bcbffe. Acesso em: 25 abr. 2023.

devido a um elevado número de críticas e propostas de alteração por diversas entidades médicas, além do impacto social envolvido na medida, o órgão voltou atrás e revogou seu próprio ato, a fim de amadurecer a discussão e chegar a um novo texto, que segue em debate.

5. REFLEXÕES JURISPRUDENCIAIS SOBRE A LGPD NA SAÚDE

Ao examinar a interpretação jurídica de diversos tribunais, que vão do Supremo Tribunal Federal aos Tribunais Estaduais, fica evidente que há um consenso de que o direito à saúde não é apenas um Direito Fundamental que atende a todos os indivíduos, mas também é um derivado constitucional que não pode ser separado do direito à vida.

5.1 Jurisprudências relacionadas à saúde

Em recente decisão recursal, o desembargador Nelson Schaefer Martins, do TJ-SC, enfatizou que é direito de todo cidadão receber assistência médica adequada, cabendo ao governo fornecê-la. De acordo com a Lex Fundamentalis, o tratamento de saúde deve incluir o fornecimento de medicamentos sem nenhum custo. Isso é essencial para garantir que aqueles que não podem pagar também possam manter uma boa saúde.

Entre várias decisões judiciais que cercam o tema, uma delas foi proferida pelo Ministro Celso de Mello em um caso envolvendo um paciente soropositivo que fazia uso de medicamentos do Sistema Único de Saúde. O ministro reconheceu que esse direito carrega uma obrigação constitucional, que não pode ser dissociada do direito do indivíduo à vida.[8]

A Suprema Corte possui inúmeros julgados sobre o assunto, em um destes, o Ministro Celso de Mello, julgando um caso de um paciente com HIV, dependente de medicamentos do Sistema Único de Saúde, garantiu que tal direito representa ônus constitucional, indissociável do direito à vida.[9]

Ao julgar a ação cautelar 2.836, o ministro Ayres Britto, do Supremo Tribunal Federal, afirmou que "a saúde é qualificada constitucionalmente como um direito fundamental de dupla dimensão (direito social e individual indisponível)".[10]

---

[8] BRASIL. Tribunal de Justiça de Santa Catarina. Apelação Cível n. 2012.089245-5, da capital, Rel. Des. Nelson Schaefer Martins, SC, 29 de janeiro de 2013.
[9] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 271286. RS, Relator: Celso de Mello. Data de Julgamento: 11/09/2000, Segunda Turma.
[10] BRASIL. Supremo Tribunal Federal. Ação cautelar 2.836. SP, Relator: Ayres Britto. Data de Julgamento: 27/03/2012, Segunda Turma.

Em sua decisão sobre um Recurso Extraordinário, o Ministro Lewandowski afirmou que, quando confrontado entre proteger o direito à vida e à saúde ou priorizar um interesse financeiro secundário do Estado, o julgador deve fazer apenas uma escolha possível e ético-jurídica: aquela que favorece o respeito absoluto à vida e à saúde humana.[11]

Além disso, a ministra Carmen Lúcia considerou a distribuição de fraldas descartáveis a uma criança doente, um real fim terapêutico, não se configurando mera comodidade, afirmando ainda:

> o direito à saúde de crianças e adolescentes detêm absoluta prioridade com respaldo nos artigos. 196 e 198 da CRFB/88 e no artigo 11, § 2º do ECA que atribui ao Poder Público o dever de fornecer gratuitamente àqueles que necessitem os medicamentos, próteses e outros recursos relativos a tratamento, habilitação ou reabilitação. (BRASIL. Supremo Tribunal Federal. Recurso Extraordinário com Agravo 741583. RS, Relator(a): Cármen Lúcia. Data de Julgamento: 17/05/2013)

Ante ao exposto, fica claro que é obrigação do Poder Público cumprir e avocar o direito que positivou, independentemente da forma utilizada para que tal direito seja concretizado, pois, de acordo com o artigo 23, inciso II, da Constituição Federal, cuidar da saúde é competência de todos os entes federados.

Conforme Schwartz, embora o direito à saúde dependa dos recursos materiais necessários para sua realização, é responsabilidade do Poder Público atuar na área da saúde e nenhum dos entes federativos que compõem a República Brasileira pode se eximir dessa obrigação. Além disso, os tribunais têm seguido essa mesma compreensão (SCHWARTZ, 2016).

A responsabilidade pelo fornecimento de atendimento médico é solidária entre a União, os Estados e os Municípios e, em caso de decisão sobre como dividir essa responsabilidade, cabe exclusivamente aos entes federativos fazê-lo em um momento adequado. Nenhum indivíduo pode ter seu direito constitucional à saúde limitado por ação da Administração Pública.[12]

Portanto, resguardar o direito a saúde é o mínimo que o Poder Público deve fazer ao cidadão, aja vista, que este é próprio do ser humano, sendo intrínseco ao

---

[11] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 706931. RN, Relator: Ricardo Lewandowski. Data de Julgamento: 15/05/2013.

[12] BRASIL. Tribunal de Justiça do Rio Grande do Sul. Agravo de Instrumento n. 70051324309, de Sapucaia do Sul, Rel. Ricardo Moreira Lins Pastl, SC. Julgamento em 02/10/2012

mínimo existencial e se o Governo não garante de maneira administrativa, cabe ao judiciário o fazer, por meio da tutela jurisdicional.

A partir disso, uma das formas de proteger tal direito seria por meio da proteção de dados referentes a saúde, que ganhou especial contorno após a promulgação da LGPD, visto que além de exporem o paciente, muitas vezes, sem consentimento, tratam-se de dados sensíveis, os quais necessitam de consentimento especial para seu tratamento, conforme será abordado no tópico que segue.

5.2 Jurisprudências relacionadas à LGPD

A Lei Geral de Proteção de Dados entrou em vigor no Brasil em setembro de 2020, e desde então, já existem algumas decisões judiciais importantes relacionadas a ela como por exemplo na Liminar para exclusão de dados, onde, em decisão de novembro de 2020, o Tribunal de Justiça do Distrito Federal e dos Territórios concedeu uma liminar determinando a exclusão de dados pessoais de uma pessoa de uma plataforma de vendas online. A pessoa alegou que seus dados foram coletados sem seu consentimento e que a empresa não adotou medidas adequadas para proteger seus dados pessoais.

Na sua decisão, o desembargador Cesar Laboissiere Loyola afirmou que a atividade realizada pela ré configura o tratamento de dados pessoais, o que a torna sujeita à regulamentação pela norma legal mencionada. Embora a norma permita o tratamento de dados para atender aos interesses legítimos do controlador ou de terceiros, ela também enfatiza a importância da proteção dos direitos e liberdades fundamentais do titular dos dados. Nesse sentido, mesmo que as informações em questão sejam normalmente fornecidas pelos indivíduos em suas relações comerciais e empresariais, como afirmado pelo juiz que proferiu a decisão inicial, a lei exige uma autorização específica para o compartilhamento desses dados.

Conforme alegado pelo Ministério Público, a prática em questão viola a Lei Geral de Proteção de Dados (LGPD), a qual atribui a responsabilidade pelo fluxo de dados pessoais na internet apenas ao proprietário dessas informações. Ademais, a conduta da empresa Serasa poderia infringir o direito à privacidade, à intimidade e à imagem dos indivíduos afetados, contrariando não apenas a LGPD, mas também

disposições previstas na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet, de acordo com o MPDFT.[13]

Recentemente, o juiz Douglas de Melo Martins, da Vara de Interesses Difusos e Coletivos do TJ-MA, decidiu condenar o Facebook ao pagamento de indenizações por danos morais a cada usuário que foi diretamente afetado pelo vazamento de dados pessoais ocorrido em 2021. Essa decisão foi tomada no Maranhão, e no Brasil, um total de 8.064 milhões de pessoas tiveram suas informações sensíveis expostas pela empresa.

> "INSTITUTO BRASILEIRO DE ESTUDO E DEFESA DAS RELAÇÕES DECONSUMO - IBEDEC - FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. –VAZAMENTO DE DADOS – FALHA DE SEGURANÇA – FALHA NAPRESTAÇÃO DE SERVIÇOS, COM FULCRO NA LEI GERAL DE PROTEÇÃODE DADOS – RESPONSABILIDADE DE REPARAR - DANO MORAL IN REIPSA - DANO MORAL COLETIVO" (BRASIL. Tribunal de Justiça do Estado do Maranhão. Ação Civil Coletiva n. 0812915-60.2021.8.10.0001, de São Luís/MA, Relator Douglas de Melo Martins. Data de Julgamento: 23/03/2023).

O Ministério Público Estadual se pronunciou em relação a uma ação judicial e afirmou que os fatos apresentados na ação abalaram a relação jurídica, causando repugnância e desconfiança dos usuários do Facebook. Esses fatos envolvem a obtenção de dados pessoais dos usuários sem a observância da legislação brasileira, o que viola o princípio da boa-fé objetiva.

O vazamento de dados pessoais é uma violação grave da privacidade dos usuários, e é cada vez mais comum em plataformas digitais como o Facebook. Nesse caso, a decisão do Tribunal de Justiça do Maranhão de condenar a empresa ao pagamento de indenização por danos morais aos usuários afetados é uma medida importante para garantir a proteção dos direitos dessas pessoas.

A Lei Geral de Proteção de Dados é um marco importante para a proteção dos direitos e liberdades fundamentais dos titulares de dados pessoais no Brasil. Como mencionado anteriormente, já houve algumas decisões judiciais importantes relacionadas a ela, e é fundamental que as empresas estejam em conformidade com a lei para evitar violações e possíveis sanções.

As empresas precisam compreender a importância da proteção dos dados pessoais de seus usuários e implementar medidas adequadas para garantir a

---

[13] BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Agravo de Instrumento n. 0749765-29.2020.8.07.0000, de Brasília/DF, Relator César Loyola. Data de Julgamento: 20/11/2020.

segurança dessas informações, como a adoção de políticas de privacidade claras e transparentes, a utilização de tecnologias de segurança eficazes e a realização de treinamentos e conscientização de seus funcionários.

Além disso, é importante que os usuários estejam cientes de seus direitos e saibam como exercê-los em caso de violação de seus dados pessoais, buscando reparação pelos danos sofridos.

Enfim, a proteção dos dados pessoais é um tema cada vez mais relevante e deve ser tratado com seriedade pelas empresas e pelos usuários. A LGPD veio para fortalecer a privacidade e a segurança dos dados pessoais no Brasil, e é fundamental que as empresas e a sociedade em geral estejam conscientes de suas responsabilidades nessa área.

Neste interim, é de suma importância que as empresas estejam em conformidade com a lei e tomem medidas efetivas para proteger os dados de seus usuários. Em caso de violação, os usuários têm o direito de buscar reparação pelos danos sofridos.

6. CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) no Brasil trouxe uma nova dimensão para o tratamento de dados ao disciplinar a proteção de dados pessoais como um direito fundamental, e reconhece a existência de dados pessoais sensíveis, que incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicatos ou organizações religiosas, filosóficas ou políticas, bem como dados relacionados à saúde, vida sexual, dados genéticos ou biométricos, quando relacionados a uma pessoa natural.

A referida Lei é uma legislação importante e relevante para a proteção dos direitos dos indivíduos em relação aos seus dados pessoais. Com o aumento do uso da tecnologia e da internet, os dados pessoais tornaram-se vulneráveis e a privacidade dos indivíduos foi comprometida. Esta lei busca proteger os direitos das pessoas físicas à liberdade, privacidade e proteção de seus dados pessoais, garantindo que o processamento relacionado à coleta de dados seja realizado de forma responsável e de acordo com as melhores práticas.

Assim, dados pessoais e informações pessoais são termos que se sobrepõem em algumas circunstâncias, mas têm diferenças importantes. Deste modo, a proteção de dados ou informações pessoais tem como objetivo proteger a personalidade da pessoa e não o dano em si. É importante, portanto, que haja regulamentações e medidas adequadas para garantir a privacidade e a segurança desses dados, especialmente quando se trata de categorias que representam uma ameaça maior à personalidade do indivíduo.

Assim sendo, este estudo buscou investigar a relevância das regulamentações da LGPD no contexto da saúde, destacando a importância da proteção dos dados pessoais dos pacientes e a responsabilidade dos profissionais de saúde em relação ao uso e proteção dessas informações. É fundamental que os profissionais de saúde estejam cientes das normas e regulamentações da LGPD e que implementem práticas responsáveis no uso e proteção dos dados pessoais dos pacientes. Portanto, profissionais de saúde, clínicas médicas, hospitais e centros de saúde, entre outros, que realizam o tratamento de dados pessoais sensíveis relacionados à saúde devem adotar medidas para se adequar às normas previstas na lei. O não cumprimento das disposições da LGPD pode resultar em sanções que vão

desde a aplicação de multas pecuniárias até a proibição do uso de dados pessoais sensíveis.

Uma possível solução para fortalecer a proteção de dados sensíveis dos pacientes na área da saúde é a aplicação efetiva da LGPD. Isso envolve revisar políticas internas, implementar medidas de segurança adequadas, treinar profissionais de saúde e obter consentimento informado dos pacientes. No entanto, a implementação efetiva da LGPD pode apresentar desafios, como interpretação e aplicação da lei e adaptação de práticas existentes. É importante pesquisar e buscar soluções para preencher essas lacunas, como desenvolver diretrizes específicas para a área da saúde, adotar tecnologias avançadas de segurança de dados e capacitar continuamente os profissionais de saúde.

Em suma, o grande desafio da era digital é buscar a convergência dos conceitos de ética, direito e proteção de dados, a fim de criar uma cibercultura positiva ou uma nova ética digital. Essa tarefa deve ser realizada sem comprometer os avanços tecnológicos. Vale ressaltar que o tema está longe de ser esgotado e continuará passando por várias alterações de entendimento e aplicação durante a vigência da LGPD. É provável que surjam diversas controvérsias, tanto devido ao descumprimento da lei quanto ao amadurecimento dos conceitos introduzidos por ela.

7. REFERÊNCIAS

ABDET - ACADEMIA BRASILEIRA DE DIREITO DO ESTADO. **Comentários ao Marco Civil da Internet.** Disponível em: <http://abdet.com.br/site/wp-content/uploads/2015/02/MCIABDET.pdf>. Acesso em: 10/03/2023.

ADRIEN JAMMET, **TheEvolution of EU Law on the Protection of Personal.** Issue, 2014

ALBUQUERQUE, Aline. **Direitos humanos dos pacientes**. Curitiba: Juruá, 2016.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. 1. ed. São Paulo: Malheiros Editores, 2006.

BIONI, Bruno Ricardo. **Proteção de dados pessoais e direitos da personalidade**. Revista Brasileira de Direito Civil, Belo Horizonte, v. 17, n. 71, p. 137-161, jan./mar. 2019. Disponível em: https://www.rbdcivil.com.br/artigos/17-71-bruno-bioni/. Acesso em: 27/03/2023.

BOFF, Salete Oro; FORTES, Vinícius Borges. A **Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.** Sequência (Florianópolis) [online]. 2014, n.68.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. – Brasília: Senado Federal, Coordenação de Edições Técnicas, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 10/03/2023.

_____. **Lei n. 12.965**, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 10/03/2023.

_____. **Lei n. 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 10/03/2023.

_____. **Lei n. 12.737**, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 10/03/2023.

_____. **Lei n. 12.414**, de 09 de junho de 2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm> Acesso em: 10/03/2023.

_____. **Lei n. 9.507**, de 12 de novembro de 1997. **Regula o direito de acesso a informações e disciplina o rito processual do habeas data.** Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm> Acesso em: 10/03/2023.

_____. **Lei n. 12.527**, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 10/03/2023.

_____. **Lei n. 8.078**, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em: 10/03/2023.

CASTELLS, Manoel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Zahar, 2015.

CATALA, J. **Dados pessoais: do conceito à proteção**. Revista de Direito, Estado e Telecomunicações, 2011.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. **A lei geral de proteção de dados do brasil na era da big data. In: Tecnologia Jurídica & Direito Digital** - II Congresso Internacional de Direito, Governo e Tecnologia, 2., 2018, Belo Horizonte. Anais [...]. Belo Horizonte: Fórum, 2018, v.1, p. 351-366.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos e coordenação. **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103**. Joaçaba: Unoese, 2011.

_____, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2016

DOVE, Edward S; TAYLOR. Mark J. **Signalling Standards for Progress: Bridging the Divide Between a Valid Consent to Use Patient Data Under Data Protection Law and the Common Law Duty of Confidentiality**. Medical Law Review, v. 29, Issue 3, Summer, p. 411–445, 2021.

FIGUEIREDO, Luis. **Curso de direito constitucional.** São Paulo: Saraiva, 2017.

GREGORI, Maria Stella. **Os impactos da lei geral de proteção de dados pessoais na saúde suplementar.** Revista de Direito do Consumidor. v. 127, p. 171– 196, jan./fev. 2020.

HAGE, J. R. **A aplicação dos princípios da proteção de dados pessoais no Brasil. Revista de Direito, Tecnologia e Inovação**, v. 5, n. 1, 2019. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rdti/article/view/43595.>. Acesso em: 10/03/2023.

KAMEDA, S. I.; PAZELLO, E. T. **Dados em Saúde e Regulação: a Proteção de Dados Pessoais como Paradigma na Era da e-Saúde**. Revista de Direito Sanitário, São Paulo, v. 16, n. 1, 2015.

LEMOS, F. **Direito, tecnologia e cultura: Reflexões sobre a Lei Azeredo.** Revista USP, 2014.

LÉVY, Pierre. Cibercultura. São Paulo: Ed. 34, 1999.

LUCIANO, Eliane Maria Monteiro de Castro; BRAGANÇA, Maria de Lourdes; TESTA, Maria Lucia. **Privacidade e sigilo médico: reflexões para a enfermagem**. Revista da Escola de Enfermagem da USP, São Paulo, v. 45, n. 6, p. 1516-1521, dez. 2011. Disponível em: https://doi.org/10.1590/S0080-62342011000600029. Acesso em: 28/03/2023.

MALDONADO, Vinícius Navarro. **A importância do prontuário médico na prática médica**. Revista Médica de Minas Gerais, Belo Horizonte, v. 25, n. 1, p. 97-102, 2015.

MALDONADO, Vinícius Navarro; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada.** 1. ed. São Paulo: Revista dos Tribunais, 2019.

MALDONADO, José Luiz Quadros. **Responsabilidade Civil por Dano Decorrente do Processamento de Dados: Uma Análise à Luz da Jurisprudência Brasileira e Portuguesa.** Revista de Direito do Consumidor, São Paulo, n. 126, p. 105-132, 2019.

MARTINS, Guilherme Magalhães. **O direito ao esquecimento na Internet.** In: Direito Privado e Internet. Coord: Guilherme Magalhães Martins. São Paulo: Editora Atlas, 2014.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. 156 f. Dissertação (Mestrado em Direito) -Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/handle/10482/4782. Acesso em: 28/03/2023.

MENDES, Alexandre Libório Philippi. **O uso de dados pessoais sensíveis no contexto da proteção de dados pessoais.** In: CRESPO, Marcelo (coord.) Lei Geral de Proteção de Dados Pessoais: comentários artigos por artigo. São Paulo: Thomson Reuters Brasil, 2020.

ONU (Organizações das Nações Unidas). **Declaração Universal dos Direitos Humanos**,1948. Disponível em: https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf. Acessado em 28/03/2023.

SÁ JUNIOR, Sergio Ricardo C. **A regulação jurídica da proteção de dados pessoais no Brasil.** 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 2012.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013.

SCHWARCZ, Lilia Moritz. **Brasil: Uma Biografia**. São Paulo: Companhia das Letras. 2016.

SERPA NETO. **Prontuários Médicos eletrônicos: análise secundária para melhorar o atendimento ao paciente**. TIC Saúde. Pesquisa Sobre o Uso de Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde brasileiros. Núcleo de Informação e Comunicação do Ponto BR; 2017.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Ed. Malheiros, 2013.

SOBRINHO, Pilau. **A saúde como direito fundamental e o papel do Estado na sua garantia.** Revista Direitos Fundamentais & Democracia, v. 19, n. 1, 2016.

SOUZA, Rafael Santos de. **Anonimização de dados pessoais: conflitos e desafios à proteção de dados pessoais.** In: SOUZA, Guilherme Wunsch; CORREIA, Marcelo Roque Martins (Orgs.). Proteção de dados pessoais: doutrina e casos (pp. 31-48). Salvador: JusPodivm, 2018.

TEFFÉ, Chiara Spadaccini de. **Os princípios como fundamento do sistema jurídico e a interpretação da norma LGPD.** In: Anais do IV Congresso de Direito e Inovação. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2019.

TIBÚRCIO, Caio César**. Proteção de Dados como Cláusula Pétrea**. Migalhas, 2022. Disponível em: https://www.migalhas.com.br/coluna/tecnologia/357133/protecao-de-dados-como-clausula-petrea. Acesso em: 27/03/2023.

TINTO, Ana Rita Ramos Y Rio. **Proteção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Proteção de Dados da União Europeia.** 2018. Dissertação (Mestrado). Escola Nacional de Saúde Pública. Universidade Nova de Lisboa, Lisboa, 2018.

VIEIRA, Fabio Alonso; COSTA, Carolina Barbosa Cunha. **Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil.Latin Lawyer. August 2021**. Disponível em: https://latinlawyer.com/guide/the-guide-corporate-compliance/secondedition/article/24-data-privacy-and-protection-relating-healthcare-in-europe-the-united-statesand-brazil. Acesso em: 10/03/2023