BEATRIZ MOREIRA ASSUNÇÃO

A LGPD E O DIREITO MÉDICO: CULTURA ORGANIZACIONAL COM ENFOQUE NA PRIVACIDADE DE DADOS PESSOAIS SENSÍVEIS

CURSO DE DIREITO – UniEVANGÉLICA

2022

BEATRIZ MOREIRA ASSUNÇÃO

A LGPD E O DIREITO MÉDICO: CULTURA ORGANIZACIONAL COM ENFOQUE NA PRIVACIDADE DE DADOS PESSOAIS SENSÍVEIS

Trabalho de Conclusão de Curso apresentado ao Núcleo deTrabalho Científico do curso de Direito da Universidade Evangélica de Goiás, como exigência parcial para a obtenção do grau de bacharel em Direito, sob orientação do professor M.e. Herbert Emílio Araújo Lopes

ANÁPOLIS – 2022

BEATRIZ MOREIRA ASSUNÇÃO

A LGPD E O DIREITO MÉDICO: CULTURA ORGANIZACIONAL COM ENFOQUE NA PRIVACIDADE DE DADOS PESSOAIS SENSÍVEIS.

Anápolis, _____ de Junho de 2022.

BANCA EXAMINADORA

Prof. M.e. Herbert Emílio Araújo Lopes

Professor Orientador

Profa. M.e. Áurea Marchetti Bandeira

Supervisora do NTC

“O correr da vida embrulha tudo. A vida é assim: esquenta e esfria, aperta e daí afrouxa, sossega e depois desinquieta. O que ela quer da gente é coragem” – Guimarães Rosa

AGRADECIMENTOS

Agradeço, inicialmente, a Deus, que concede sabedoria e ilumina os meus dons, entre eles o amor pelo conhecimento e o desejo do saber, Ele quem orienta e dá forças nos momentos de tempestade, me permitindo viver a plenitude da sua graça.

Agradeço aos meus pais, Fátima e Renato, que por me amarem com razões que trasncedem a compreensão, incentivam o meu desbravar, fazendo clarear em minha mente a certeza de que a melhor parte da viagem é a jornada. Aos meus amigos e familiares, faltam palavras por tamanho acolhimento e compreensão.

Agradeço à Universidade Evangélica de Goiás pelos anos de amadurecimento acadêmico, e especial ao meu estimado orientador, Prof. Me. Herbert Emílio Araújo Lopes, homem sábio e de admiráveis qualidades, que contribuiu de forma incalculável para o sucesso deste trabalho.

RESUMO

A Lei n° 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD), configurou um marco importante no que diz respeito ao direito digital brasileiro e suas respectivas aplicabilidades. Visto que, delimitou a maneira de se operacionalizar o tratamento de dados pessoais dos indivíduos, em qualquer campo que os englobe. É imprescindível destacar que, se respeitamos as definições incluídas por Patrícia Peck Pinheiro (2019), a LGPD esculpiu-se como uma legislação essencialmente técnica, abrangendo em suas disposições itens de controle, a fim de assegurar que as garantias previstas sejam plenamente cumpridas, tanto para a iniciativa pública como para a privada, de forma sustentável e eficiente.

O principal objetivo é promover a maior segurança e impor penalidades, caso suas diretrizes não sejam cumpridas. Desde que a norma entrou em vigência, o Brasil adentrou no rol dos 120 países que possuem uma legislação específica para regulamentar a proteção de dados pessoais, diretriz que já é há algum tempo regulada na Europa, com a *General Data Protection Regulation* (GDPR).

O normativo em tela, preconiza mecanismos para objetivar a, plena e certa, execução dos direitos consagrados ao titular dos dados, faz menção às medidas de segurança que deverão ser adotados. O ápice, trata-se de consolidar a cultura organizacional com enfoque no garante da privacidade de dados pessoais, atentando-se o legislador a proteger os direitos fundamentais de liberdade e privacidade, tal como o livre desenvolvimento da personalidade da pessoa natural.

É de clareza solar, reconhecer que a Lei nº 13.709/2018 assevera aos cidadãos maior controle a respeito de suas informações pessoais, razão pela qual se inclui neste debate o impacto da LGPD no âmbito da saúde, haja vista ser um ramo que, inevitavelmente, manuseia dados pessoais e, essencialmente, os sensíveis. Entretanto, a icógnita de como tais elementos têm sido tratados emergiu a necessidade em proteger o indivíduo perante o cenário de riscos que envolvem a conjuntura digital.

A partir dos questionamentos expostos, profissionais que compõem o organograma médico, bem como pesquisadores, tem se sensibilizado quanto à um dos efeitos basilares do disposto, qual seja o liame de atrasar a inovação e progressão

no uso de inteligências artificiais.

Portanto, objetivou-se, através do presente trabalho de conclusão de curso, compreender as razões pelas quais a aplicabilidade da LGPD nos ambientes clínicos-hospitalares, consultórios e operadoras de planos de saúde, se faz imprescindível, de modo a mapear as questões pertinentes, apurar riscos que englobam o vazamento das bases de uma instituição de saúde, a elaboração das políticas de proteção dados, a responsabilidade civil, bem como um comparativo de ameaças, benefícios e prejuízos aos entes que compõem o ciclo médico.

Palavras chave: LGPD. Direito Médico. Dados Sensíveis. Saúde. Privacidade.

SUMÁRIO

CAPÍTULO I – O IMPACTO DA LGPD NO ÂMBITO DA SAÚDE

O novo cenário mundial vislumbra o potencial tecnológico em constante ascensão, ainda que o ápice demonstre estar distante, considerando os impasses revelados na era pós-moderna. É válido mencionar a tendência dasinovações como necessidade, impossibilitando que exista qualquer vestígio de resistência.

Perante o avanço e instalação do mundo predominantemente digital,as formas de comunicação, processamento e armazenamento possibilitaram o surgimento de dados em proporções volumosas, que só são manejados no contexto atual com o auxílio, destacando a codependência humana em relação às máquinas. As modificações revelam a transformação no modo de comportamento do homem, incluindo ferramentas de comunicação sofisticadas e aprimorando a capacidadede armazenamento de dados e informações. (LIPPSTEIN, 2017)

Nesta linha, quando se contempla a inclusão dos anseios tecnológicos ao campo científico, primordialmente no que concerne aos potenciais ainda desconhecidos, há resistência e inevitavelmente óticas lesivas e instáveis dos horizontes elucidados. Ocorre que, as realidades das mudançasnão se configuram adstritamente às futuras gerações, fazendo-se pertinente analisar o conteúdo regulamentado, e vislumbrar o momento em que a sociedade brasileira não mais compõe os bastidores no tratamento de dados pessoais.

Em sede da abrangência aqui aplicada, vê-se que os ambientes clínicos-hospitalares lidam diretamente com o manuseio de dados, seja no momento de captação, tratamento ou armazenamento de dados, existindo um lapso temporal considerável, de modo basilar no que concerne à previsibilidadedo sigilo médico. Entretanto, até a Lei n° 13.709/2018 entrar em vigor, tal procedimento não era munido de diretrizes legais, o que abria brechas e precedentes na segurança dos dados sensíveis coletados.

Assim, objetivando proteger os dados pessoais e assegurar os direitos fundamentais concernentes à liberdade e privacidade de seus titulares, a LGPD foi estabelecida e devidamente promulgada, seguindo os preceitos já adotados pela Europa com a GDPR, de modo a estabelecer uma inovação ao ordenamento jurídico brasileiro.

A Lei n° 13.709/2018, alterada pela Lei n° 13.853/2019, regulamentou o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa naturalou por pessoais jurídica de direito público ou privado, listando no artigo 2º os fundamentos essenciais para que ocorra o regular manuseio. Considerando essa raiz, passou a legislar quanto aos dados pessoais sensíveis, os quais são concedidos, por essência, ao âmbito da saúde.

1.1 Princípios da LGPD

Sabe-se que o regimento dos princípios existe desde a primariedadehumana, revelando sua face multifacetária e polissêmica ao demonstrar que a transgressão ataca todo o sistema, de modo a provocar uma subversão aos valores fundamentais.

Conforme fora preceituado incialemente por Ronald Dworkin, tanto uma constelação de princípios quanto uma regra positivamente estabelecida, podem impor uma obrigação legal. Com isso, é certo dizer que os princípios sãoresponsáveis por nortear todo o sistema jurídico, de modo que estabelecem ideais gerais, os quais devem amparar a elaboração da lei, bem como seu entendimento e aplicação. (BONAVIDES, 1996)

O jurista e doutrinador Miguel Reale, assume posição semelhante, quanto a compreensão de que:

> [...]princípios são verdades, pois juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dadaporção da realidade[...]. (1986, p. 60)

Considerando os apontamentos acima, a Lei Geral de Proteção de Dados (LGPD), tem-se por base a *General Data Protection Regulation* (GDPR),em seu artigo 5°, em vigor a partir dos vinte e cinco dias do mês de maio de 2018, estabelece os princípios que devem a ser seguidos no tratamento de dados pessoais, e que são delimitados expressamente, sendo eles: i) ilicitude; ii)lealdade; iii) transparência; iv) limitação da finalidade; v) minimização de dados; vi) exatidão; vii) limitação da conservação; viii) integridade e confidencialidade;ix) responsabilidade. (Regulamento (UE) 2016/679 do Parlamento Europeu e doConselho).

Contudo, a proteção de dados submete-se não só aos princípios gerais

norteadores, como também aos princípios próprios delineados no artigo 6º da Lei Geral de Proteção, cravando inicialmente que o tratamento seja presidido pela boa-fé, para empós estabelecer aqueles essencialmente jurídicos.

De certo modo, pode-se extrair da LGPD sua densidade principiológica, isto é, traz em seus limites legais uma conjectura de princípios que devem ser considerados para a plena execução. O legislador, no intuito de simplificar a aplicação da regra, demarcou como sendo imprescindível a verificação de conformidade para com os itens de controle.

É imprescindível dizer ainda que, o normativo vislumbrou o amplo cenário tocado pela LGPD, não sendo possível que estabelecesse o normativo de modo taxativo, recorrendo-se assim aos princípios norteadores da ordem jurídica, adotando em conjunto os especificados, para que não pairem dúvidas ou conflitos que envolvam o cuidado com os dados nos mais diversos cenários. (PESTANA, 2020)

Por conseguinte, é factível dizer que ao conhecermos os princípios, podemos compreender a matéria sob atenção, facilitando a dissecação do objeto que se apresenta no estudo. Em reverso, quando há desconhecimento dos dogmas, caminha-se lentamente por preceptivos, sem que exista ampla e larga visão.

A linha mestra para o tratamento de dados pessoais é, por essência, o consentimento do titular, em virtude disso, é necessário que sejam observados os princípios norteadores, quais sejam a finalidade, compatibilidade do tratamento, limitação, garantia aos titulares de consulta facilitada e gratuita, atualização de dados, transparência, utilização de medidas de segurança capazes de comprovar a proteção dos dados, prestação de contas pelo agente,não discriminação, além do princípio da boa-fé. (LUGATI, 2020)

Em primo, a LGPD trata o princípio da finalidade, expondo que o tratamento de dados deve ser tomado com base em propósitos legítimos,específicos e explícitos, devidamente prestados ao titular, indicando a impossibilidade em utilizá-los para fins diversos e incompatíveis.

Já segundo o princípio da adequação, refere-se à compatibilidade do tratamento para com as informações que foram prestadas ao titular. Concluindo-se

pelo vínculo de pertinência lógica de analogia evidenciado entre o tratamento e a finalidade objetivada, tratando-se do somatório de circunstâncias que o englobe.

No campo jurídico, as circunstâncias dizem respeito a objetos e às ações do homem (não somente às condutas, que são catalogadas *a priori* por normas codificadas irradiadas a partir do contexto jurídico), consubstancia em eventos e fatos sobre os quais se admite relato apropriado, identificados de uma atmosfera particular onde tiverem lugar,sendo assim mais das vezes extremamente relevantes para o discurso sobre a prova e acerca das repercussões jurídicas que lhe serão atribuídas. O contexto do tratamento, como se observa, estabelece um sistema de referência circunstancial, a partir do qual o tratamento cogitado seriamente faça sentido. (PESTANA, 2007)

Em contrapartida o princípio da necessidade é solidificado na limitação em realizar o mínimo necessário, de modo que inclua os dados essencialmente pertinentes, e que não firam a finalidade proposta.

Já o princípio do livre acesso dispõe quanto a um dos princípios cardeais da LGPD, de modo que garante aos titulares dos dados fornecidos tenham facilitada e gratuita consulta quanto a forma e a duração do tratamento,e ainda no que concerne à integralidade dos dados pessoais).

Segundo o princípio da transparência, o qual se imbrica com o da qualidade também já explicitado, há uma validação aos assegurados de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, bem como os respectivos agentes de tratamento, resguardados os segredos industriais e comerciais. A ênfase da transparência deseja destacar a importância que a LGPD dispensa à fluidez de informações para o titular dos dados tratados, afinal, o titular, em conjunto com os dados, configuram os elementos mais importantes de todo o processo de tratamento.

O princípio da segurança disposto no inciso VII, dá o tom para a interpretação da aplicabilidade normativa da lei. Ocorre que, a LGPD extrai daqueles que tratam dados a utilização de medidas aptas a proteção de acessosnão autorizados (invasões) ou ilícitas de destruição, perda, alteração,comunicação ou difusão (como vazamentos acidentais ou criminosos). O foco aqui é a proteção prévia, englobando o primor do

inciso VIII, ou seja, não basta que operador e o controlar apliquem técnicas de mitigação de riscos, danos, oubusquem a reparação posterior dos danos. (BRASIL, 2018)

Por fim, o artigo 6°, da Lei n° 13.709/18 delimita os princípios da não discriminação e responsabilização (BRASIL, 2018). Assim, expressa a impossibilidade de armazenamento dos dados para fins discriminatórios, ilícitosou abusivos. Enquanto o princípio da responsabilização exige que seja demonstrado pelo agente a adoção de medidas eficazes e que cumpram as normas de proteção de dados pessoais.

A LGPD no decorrer de seus dispositivos prevê que quem, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano seja ele de raiz patrimonial ou moral, individual ou coletivo, será obrigado a repará-lo. E responderão solidariamente todos os envolvidos no tratamento dedados, a menos que provem que embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à LGPD; ou que o danoé decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Em linhas alhures, para fins de complementação, cabe mencionar ainda, as especificações do artigo 5°, inciso XXXIII, da Constituição Federal, noque versa ao direito de todos a receber dos órgãos públicos informações de seuinteresse particular, ou de interesse coletivo ou geral, ressalvados os casos ondeo sigilo é indispensável à segurança da sociedade e do Estado, de modo que sefaz possível a interpretação e aplicação aos órgãos de raiz privada, no tocante aos dados pessoais sensíveis fornecidos, com destaque àqueles prestados em âmbito médico. (BRASIL, 1988).

1.2 Considerações essenciais quanto a Lei n° 13.709/18

A Lei n° 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD), esculpiu um marco importante no que diz respeito ao direito digital brasileiro e suas respectivas aplicabilidades, visto que, delimitou a maneira de se operacionalizar o tratamento de dados pessoais dos indivíduos,em qualquer campo que os englobe. É imprescindível destacar que a LGPD afeiçou-se como uma legislação essencialmente técnica, abrangendo em suas disposições itens de controle, no intuito de assegurar que as garantias previstas sejam plenamente

cumpridas, tanto para a iniciativa pública como para a privada,de forma sustentável e eficiente. (PINHEIRO, 2019)

O principal objetivo é promover a maior segurança e impor penalidades, caso suas diretrizes não sejam cumpridas. Desde que a norma entrou em vigência, o Brasil adentrou no rol dos 120 países que possuem uma legislação específica para regulamentar a proteção de dados pessoais.

A Europa há algum tempo estabeleceu e segue suas próprias diretrizes no continente, com a *General Data Protection Regulation* (GDPR), e o regulamento, em qualquer localidade que seja, é primordial para custodiar os dados das pessoas e afastar as adversidades provenientes dos vazamentos.

O regulamento em tela, explicita a implantação de mecanismos que objetivem a plena e certa execução dos direitos concernentes ao titular dos dados, fazendo menção às medidas de segurança que deverão ser adotados. O ápice trata-se de consolidar a cultura organizacional com enfoque no garante daprivacidade de dados pessoais, atentando-se o legislador a proteger os direitosfundamentais de liberdade e privacidade, tal como o livre desenvolvimento da personalidade da pessoa natural. (PINHEIRO, 2019)

É de clareza solar, reconhecer que a Lei nº 13.709/2018 assevera aoscidadãos maior controle a respeito de suas informações pessoais, de modo a exigir conhecimento explícito e tácito, salvo as hipóteses em que fica desobrigado, como é o caso de obrigações legais ou regulatórias exercidas poragente de tratamento.

Além disso, institui como obrigatória a oferta de uma gama de opções que garanta ao titular o direito de acessá-lo, corrigi-lo ou, caso reconheça necessário, determinar que seja excluído. Vale ressaltar que, deve ser disponibilizado de modo ostensivo a real finalidade ainda durante a coleta de dados. (id.2019)

Neste toar, podemos incluir em debate o impacto da LGPD no âmbitoda saúde, por se tratar de um ramo que, inevitavelmente, manuseia dados pessoais e, em especial, os sensíveis, entretanto, o questionamento de como tais elementos têm sido tratados fez-se necessário perante o cenário de riscos que envolvem a conjuntura digital.

A partir dos questionamentos expostos, profissionais que compõem o organograma médico, bem como pesquisadores, tem se preocupado quanto à um dos efeitos basilares do disposto, qual seja o de atrasar a inovação e progressão no uso de inteligências artificiais.

1.3 Impactos da Regulamentação no Direito Médico

A norma abriu precedentes para solucionar indagações que, permaneceram por um longo período sem resposta, beneficiando a sociedade, de modo a preencher lacunas e equiparar o território brasileiro ao nível de desenvolvimento econômico-tecnológico das nações em ascensão.

O Direito Médico, precipuamente, o tema da segurança das informações é cabal, porquanto que na atuação profissional existe uma reunião de dados de pacientes como diagnósticos, anamnese, laudos, prescrições médicas, exames e demais protocolos.

A Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) intenta alcançar a criação de um ambiente seguro a respeito das averiguações individuais para coibir transações de dados pessoais com fins comerciais, em situações que não há manifesta autorização do indivíduo.

Resta claro já na redação do art. 1º do normativo que, a regulamentação da proteção dos dados engloba tanto pessoas naturais (pessoas físicas) quanto jurídicas (de direito público ou direito privado) e, logo, no campo do Direito Médico, sua abrangência se dá tanto a profissionaisautônomos quanto hospitais e clínicas.

No tocante às bases que referenciam a saúde, é certo que os médicose os serviços clínico-hospitalares já possuem a diretriz da circunspeção com as informações dos pacientes, considerando que este tem faculdade para com a privacidade, ao sigilo e inviolabilidade de suas informações pessoais, bem como, o histórico clínico, prontuário, tratamentos realizados e medicação ministrada.

A proteção do sigilo, no que tange aos dados e ao prontuário do paciente, já é prevista pelo Código de Ética Médica (Resolução nº 2.217 de 27 de setembro de 2018) e pela Lei nº 13.787/2018, que regula a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de

paciente. Na LGPD tais informações integram a categoria dos dados sensíveis, prenunciando as novidades garantidas pela globalização das vertentes tecnológicas intrínsecas e extrínsecas.

Ainda que a medida de vigilância digital se demonstre excessiva, emrazão de limitar a circulação de dados e reconstruir rotas de modo impositivo, é possível enxergar as ramificações e reflexos decorrentes da proteção conferidaatravés das diretrizes que fortalecem a privacidade dos titulares, tocando ainda direitos como o resguardo da honra e imagem, a inviolabilidades da intimidade edignidade da pessoa humana.

As regras explicitadas e incansavelmente dispostas na LGPD, aplicam-se a situações como no acesso a exames via plataformas digitais, na telemedicina e ainda na Troca de Informações na Saúde Suplementar – TISS (padrão obrigatório para as trocas eletrônicas de dados de atenção à saúde dosbeneficiários de planos, entre os agentes da Saúde Suplementar).

No entanto, mister se faz mencionar, que a LGPD confere destaque ao cuidado específico de dados pessoais e dados pessoais sensíveis da saúde,o que provoca a submissão de regulamentações específicas aos seus princípios gerais. É certo que, o dever de proteger as bases fornecidas é mais vasto que odever específico de sigilo médico, uma vez que a Autoridade Nacional de Proteção de Dados – ANPD, por dispor da competência em fiscalizar os direitosde exercício, tal como manutenção de dados, revela-se apta a velar pelo sigilo médico.

Ademais, é inválido o consentimento para compartilhamento de dados sensíveis sobre a saúde do titular, na hipótese de os agentes controladores almejarem por meio de tal, a obtenção de vantagem econômica,o que automaticamente traz à luz a lacuna que a redação do texto do art. 11, §4º da LGPD ao prever que esse compartilhamento pode ocorrer na assistência farmacêutica, no atendimento de saúde (inclusive de serviços auxiliares de diagnose e terapia em benefício do titular), na portabilidade solicitada pelo titular ou em transações financeiras e administrativas envolvidas na referida prestação de serviços (na portabilidade, ambos agentes manterão os seus dados no que isso for necessário ao cumprimento das suas obrigações legais e para prevenir responsabilidades).

1.4 Requisitos para a efetiva implementação e respectivas penalidades

O legislador, ao editar a Lei nº 13.709/2018 preocupou-se em delimitarcritérios para o processamento seguro de informação e tratamento de dados, sob pena de sofrerem as devidas sanções quando não observarem práticas de governança e atenderem às expectativas de controle definidos pela legislação. Atentou-se ao que passou desapercebido pela Lei n° 12.695/14, denominada como Marco Civil da Internet.

Ainda que o Marco Civil da Internet tenha incluído inúmeros assuntos de destaque em relação direta da tecnologia, a referida lei não atingiu de modo detalhado a efetivação jurídica de garantias e direitos inerentes à pessoa na era moderna. Entretanto, por não atingir de modo aprofundado a vertente protetiva dos dados, fez-se imprescindível a criação de norma posterior específica. Arespeito da proteção de dados, vejamos o que disserta Rebeca Garcia:

> "seu espírito e seu escopo são outros. De todo modo, o Marco Civil da Internet estabelece importantes princípios e coloca em posição de destaque a proteção da privacidade e dos dados pessoais do usuário. Com efeito, a lei assegura aos usuários o direito à proteção da privacidade e a informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, e garante também que os dados pessoais não serão transferidos a terceiros, salvo expressoconsentimento ou determinação legal". (2016, p.161-190)

A partir de tal perspectiva, as sanções previstas no artigo 12 da Lei nº12.695/14 não poderiam provocar a proibição da operação da empresa ou mesmo a suspensão do aplicativo. Neste toar, as sanções previstas no artigo 12, gerariam advertência, multa, suspensão temporária ou a proibição do exercício das atividades, podendo aplicá-las de forma isolada ou cumulativa

O que cumpre dizer fundamentado na análise disposta, tem-se que o processamento de dados sensíveis torna o tratamento no âmbito médico ainda mais rigoroso, uma vez que envolve o segredo e confidencialidade que exige a profissão médica.

Neste sentido tornou-se indispensável o estabelecimento de políticase normas de segurança que contribuam para a mudança de cultura e para a incorporação de

conceitos tecnológicos de proteção de dados, como o uso de antivírus, firewall e proteções de rede e monitoramento de acesso.

Ocorre que, ainda que a discussão que envolve a temática seja antiga, a construção do teor da Lei de Proteção de Dados que se deu ao longo de anos, foi aprovada em regime de urgência e publica em agosto do ano de 2018, no intento de buscar efetividade na solução dos incidentes ocorridos em cenários internacional, essencialmente no que abriga a captação e armazenamento de dados pessoais.

Com isso, a sociedade médica viu-se perante inúmeras inovações, demodo que ao titular dos dados deve ser garantido todas as informações quanto ao processamento, e, nos casos que se exigem, a colheita do consentimento a ser passível de gerenciamento. Seguindo tal lógica, a imprescindibilidade de elucidar todas as fases que compõe esse processo de transformação, de modoa especificar as ações e as alterações de rotinas e controles.

A propósito, a Lei Geral de Proteção de Dados (Lei n° 13.709/2018) estabelece dois relatórios obrigatórios, para reafirmar o comprometimento com a segurança das informações prestadas. O Relatório Geral de Processamento eo Relatório de Impactos à Proteção de Dados:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Os desdobramentos da LGPD para o processamento de dados podem ser simplificados em tratar apenas o que for necessário para uma finalidade específica, adequada a um alinhamento de processos, de forma segura e com prevenção, estimando pela transparência, de modo a não causar danos ao titular, sob pena de sanções administrativas e outras consequências previstas no rol legislativo. (SINDIMED, 2021)

As sanções podem variar de simples advertência à exclusão do bancode dados, passando por multas, multas diárias e publicização das ocorrências de violação de dados e vazamentos.

Considerando o cenário de um possível vazamento das bases, há quese afirmar o caos instalado, visto que poderá comprometer as anotações pertencentes às Instituições de Saúde, sejam referentes aos pacientes, bem como aos funcionários que compõem o quadro. A partir de tal possibilidade, é evidente que haja um plano gerenciador de crises, intentando resguardar a sensibilidade e conter o ataque.

Com a informação ocupando o centro revolucionário tecnológico, o que disparou a potencialidade de gerar danos, definir medidas de modo a mitigar os riscos e impactos torna-se uma preocupação recorrente, uma vez que aprivacidade é o cerne diretamente atingido.

Luis Grandinetti Castanho de Carvalho (2017, p.3) expõe com a ênfase o tema, “a arma dos tempos modernos não é a bomba, mas a informação. Quem detém a informação, tem o poder. O poder não é só o de influenciar os comportamentos, mas de antecipar-se a eles”.

Assim, é de pronto afirmar que a privacidade se vincula à dignidade da pessoa humana, sendo o direito que abarca o campo da personalidade. Os danos, maximizados pela tecnologia, conceberam uma nova face à privacidade,conferindo controle e liberdade aos titulares, a partir da vigência da norma, de tomar decisões referentes às informações, o que consolida a sensibilidade envolvendo a proteção de dados, essencialmente no que reporta ao Direito Médico.

Em contrapartida, é oportuno momento para que as Instituições médicas enxerguem na aplicação do que impõe a Lei Geral de Proteção de Dados, e não a enxerguem como empecilho, mas sim uma ferramenta moderna e de tendência mundial, somando ao aperfeiçoamento diário dos referidos dados, a fim de resguardar ambos os lados.

Em atenção ao delineado no presente capítulo, a disposição dos instrumentos, influem que o aparato judicial e legislativo caminha no sentido da regulação das ações no âmbito das plataformas digitais. A entrada em vigor da lei de Proteção de Dados no Brasil (Lei nº 13.709) em 2020 e suas respectivas penalidades no ano de 2021 implicou mudanças significativas aos órgãos estatais e empresariais no que se imputa às atividades de coleta e armazenamento de dados, garantindo maior segurança jurídica e eficácia na tutela dos dados pessoais na Internet. Posto isso, foi feito um

arcabouço de informações basilares para a formulação do próximo capítulo.

CAPÍTULO II – OS DADOS PESSOAIS SENSÍVEIS E A PROTEÇÃO DA LGPD

A lei n 13.709/2018, revolucionou a forma como os dados pessoais são vistos e tratados no território nacional, impactando de forma significativa a regulamentação perante os hospitais essencialmente no que diz respeito à relação estabelecida entre paciente e instituição.

Nesta linha, contemplando a vastidão de dados exigidos para a atuação de excelência, os estabelecimentos de saúde passaram a se deparar com um mar de questionamentos, ante o desconhecimento da melhor forma de adequar-se ao novo ordenamento. Uma vez que, os dados relacionados à saúde do paciente são, por essência, sensíveis.

Conforme preceitua o disposto no Art. 4º da Lei (BRASIL, 2018), tais dados referem-se a saúde física ou mental de uma pessoa natural, incluindo a prestação de serviços, que revelem informações sobre o seu estado de saúde. Por tais razões, estes, assim como os demais dados sensíveis delineados na redação legal, recebem uma proteção ampla, de modo a exigir o consentimento explícito dos pacientes e devem estar amparados sob uma finalidade específica, salvo em hipóteses excepcionais que os dispensem, como em casos em que se busca preservar a vida ou integridade física.

É imperioso mencionar que o reiterado tratamento de dados sensíveis, o revela a imprescindibilidade em adequar-se à LGPD de forma ainda mais determinante. De forma a destacar que, em um país onde os beneficiários da saúde suplementar ultrapassam 47,6 milhões, de acordo com o número mais recente, de dezembro de 2020, e se realizaram 1,62 bilhão de procedimentos em 2019, conforme dados da Agência Nacional de Saúde (ANS), demonstram-se evidentes o enorme fluxo e volume de dados pessoais envolvidos. Considerando ainda, de modo incisivo o Sistema Único de Saúde, que também deverá se adequar às disposições da LGPD, já que as regras nela previstas também se aplicam ao Poder Público.

2.1 O que são os dados pessoais sensíveis

Sabe-se que o compartilhamento de dados pessoais ante à vulnerabilidade revelada ao expor elementos sensíveis inerentes a si mesmos ou a familiares, podem tornar-se armas poderosas quando tratados indevidamente, permitindo que as informações prestadas sejam utilizadas para o comentimento de práticas ilícitas, seja no campo digital ou real.

Os dados pessoais sensíveis caracterizam-se, em regra, por todos aqueles que possam identificar a origem racial ou étnica do usuário, bem como suas convicções religiosas ou políticas, filiação a sindicato ou organização de caráter religioso, filosófico ou político. Contempla, ainda, quando vinculados à pessoa natural, os dados referentes à saúde ou à vida sexual, assim como os dados genéticos ou biométricos. Destacando-se para tanto a redação da normativa:

> Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> (...)

A tecnologia conferiu maior relevância às informações pessoais: contribuiu para que fossem transformadas em algo útil e reduziu os custos de sua aquisição e de seu trânsito. A dimensão do avanço tecnológico sobre a vida privada foi tão expressiva que levou à evidente constatação da “insuficiência da dogmática tradicional” para controlar o intenso fluxo de informações. (DONEDA, 2006, p. 22-34)

A necessidade de uma legislação específica sobre a proteção conferida aos dados pessoais emergiu da forma como está sustentado atualmente o modelo atual de negociações, a era digital, em que inevitavelmente as informações tornaram-se a principal moeda de troca utilizada pelos usuários a fim de garantir o acesso a determinados bens, serviços ou conveniências.

Ocorre que, em se tratando da sensibilidade dos dados disponibilizados ao campo da medicina, a LGPD veda expressamente a comunicação ou o uso

compartilhado entre controladores com o objetivo de obter vantagem econômica, exceto quando exige-se a portabilidade de dados, desde que haja expressa autorização do titular.

Portanto, partindo de tal pressuposto, é intrinseco que os dados sensíveis determinem uma abordagem séria e segura, haja vista que a violação de sua natureza e características podem implicar em riscos irreversíveis aos direitos e liberdades fundamentais da pessoa natural, conforme delimitado pela Carta Magna.

2.2 Abordagem quanto a relevância dos dados pessoais sensíveis para a sociedade médica

O uso da tecnologia nos mais diversos campos, revelou para a contemporaniedade um potencial mercadológico de informações, uma vez que os dados revelam poder, conhecimento, e consequentemente o aspecto econômico. A vista disso, como regra, a partir do momento em que as unidades de saúde coletam dados de pacientes, potencialmente assumem o viés de serem potenciais empresas de análise de dados, cujo produto de venda extrapolaria a mera comercialização de medicamentos e serviços.

A Constituição Federal de 1988, em seu artigo 5°, inciso X, dispõe quanto a proteção constitucional a vida privada. O direito à intimidade refere-se à proteção da esfera privada ou íntima de uma pessoa, devendo esta, ser protegida contra ingerências externas, alheias e não requisitadas (BRASIL, 1988).

Partindo por esta linha, a proteção à saúde enquanto direito fundamental garantido constitucionalmente, reforça a interdependência e a mútua conformação de todos os direitos humanos e fundamentais. Evidentemente, no caso do direito à saúde, as informações geradas devem garantir à privacidade, considerando a complexidade e o caráter sensível e pessoal firmados.

Entretanto, o significado teórico de privacidade enquanto direito a ser deixado só perdeu seu valor genérico. De modo que, na sociedade da informação tendem a prevalecer definições funcionais da privacidade que criam possibilidades de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele efetivamente conferidas. Tornando, assim, a privacidade como direito de manter o

controle sobre as próprias informações (RODOTÁ, 2008, p. 92).

A necessidade de solicitar dados pessoais e gerir os sensíveis não pode ser visto como uma obrigação negativa para a gestão médica. Pelo contrário, é importante olhar para a LGPD como uma oportunidade para aumentar efetivamente a segurança do ambiente clínico-hospitalar e zelar pela proteção de dados dos pacientes.

Assim, lidar com essas informações exige o máximo de aperfeiçoamento técnico e conhecimento a respeito das disposições impostas, ainda que seja um normativo tenreo, faz-se necessária criação de ações e políticas internas que visem aplicar as práticas de segurança de dados, através de ambientes criptografados e adaptados às normas da LGPD.

Frisa-se, aqui, que os dados não podem ser coletados sem uma finalidade específica. Devendo esta, ser comunicada antes que ocorra a coleta dos dados individuais, o que facilita valorar os critérios de razoabilidade para sua utilização, afastando abusos por parte da entidade coletora.

2.3 A cultura organizacional no garante a privacidade

O direito à privacidade na sua acepção clássica, é delineado como uma tutela restringida a questões estritamente privadas e que busca combater invasores externos, ocorre que tal definição é insuficiente. Sob essa perspectiva, o doutrinador RODOTÀ (2008, p. 25) defende uma mudança qualitativa na sua concepção, devendo reposicioná-la conforme as formas de organização de poder, levando em conta que “a infraestrutura da informação representa hoje um dos seus componentes fundamentais”.

LEONARDI (2012, p. 52-76) elenca algumas das possíveis definições da privacidade, dentre as quais estão: 1) o direito a ser deixado só; 2) o resguardo contra interferências alheias; 3) o segredo ou sigilo; 5 e 4) o controle sobre informações e dados pessoais.

Cruzando a linha da privacidade como direito meramente individualista, esta passou a se tornar um aspecto fundamental da realização e do desenvolvimento da personalidade. Proteger a privacidade, fez-se um mecanismo imprescindível na garantia da liberdade da autonomia privada frente às intervenções do Estado e da

sociedade como um todo.

Com a revelação de multifacetas na acessibilidade e de interferência na privacidade individual, por meio da facilitação no fornecimento de dados pessoais, aliada a sua mercantilização desenfreada, é essencial construir um direito que discipline não apenas as formas de acesso a dados pessoais, mas também o modo como são utilizados e por quais canais circulam, sem deixar de lado a problemática relativa a indispensabilidade de permanência dessas informações na rede. (CORRÊA; GEDIEL, 2008, p. 143)

Sem a pretensão de profetizar, o historiador Harari, através das experiências e fatos ocorridos na humanidade, lança questionamentos importantes relacionados à ética no uso da tecnologia e, especialmente, dos dados pessoais e sensíveis – frequentemente considerados o novo petróleo da internet e a nova moeda do mundo digital para a humanidade. Seguindo tal premissa, a tecnologia do século XXI é capaz de capacitar os algoritmos externos a serem —hackers da humanidade". Estes algoritmos seriam mais especialistas no conhecimento de um indivíduo do que ele próprio, transferindo a crença no individualismo para os algoritmos em rede.

2.4 O empoderamento do titular e a sua posição como ente inviolável

Considerando as hipóteses em que se dispensa o consentimento do titular, este ato será indispensável, uma vez que tal determinação está expressamente prevista no art. 5°, XII, da LGPD (BRASIL, 2018) sendo uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Em se tratando do campo médico, a complexidade provocada é maior, uma vez que em muitas situações a coleta de dados obtido para uma determinada finalidade, pode posteriormente emergir a necessidade de que esses dados sejam usados para outras aplicações.

Sendo assim, a normativa dispõe expressamente que a autorização para uma finalidade diferente daquela originalmente firmada, cabe exclusivamente ao titular, que a qualquer momento tem o direito de voltar atrás em sua decisão de consentimento. Ante tal impasse exige que as organizações criem mecanismos seguros de coleta da

autorização do titular e que estejam sempre prontas para produzir, de modo ágil e seguro, provas sobre o aceite em relação ao uso de seus dados.

É imprescindível dizer quanto a sua conceituação, sendo um ato jurídico com conteúdo existencial e revogável a qualquer tempo e, para além, um limite à tutela da saúde, estabelecido pela autodeterminação pessoal. No consentimento, o paciente previamente admite que tolerará uma intervenção ou tratamento a ser efetivado em benefício dos seus interesses existenciais psicofísicos, delineando os seus contornos ou assentirá ao que lhe for proposto. Trata-se de ato proveniente da sua autodeterminação, tendo como função adicional a legitimação da atividade do médico no atendimento que o demande, bem como a especificação das fronteiras de atuação do profissional, seguindo aa particularidade de cada caso. (PELLEGRINO, Giulio, 2015)

Conforme preceitua Danilo Pereira, no Direito Médico, há uma “relação obrigacional complexa”, que reveste uma vinculação relacional, não limitada a um dever principal, qual seja submeter o, mas também um abrangente conjunto de deveres acessórios, nos quais se encontram o consentimento do paciente, a documentação, o sigilo de informações e a proteção dos dados, delineando ainda os mais diversos figurantes que compõem a relação, médicos, pacientes, equipes de atendimento em saúde, clínicas, hospitais ou outras estruturas juridicamente formadas, para a prestação de serviços médicos ou a complementação do atendimento prestado.

Isto posto, tem-se que o pontapé que legitima a coleta de dados é o consentimento do titular. Ocorre que nem sempre essa relação é constituída com equilíbrio, em razão da expressa dificuldade em ter acesso, bem como aos possíveis danos provocados a partir das entidades coletoras.

A LGPD (BRASIL, 2018) preconiza que o consentimento poderá ser dispensado, segundo a redação dada pelo art. 13, IV, mencionando a título de exemplo, quando se estiver diante de tratamento de dados para fins estatísticos. Nessa hipótese especifica, deve-se tomar cuidado, pois atualmente há pesquisas comportamentais tendo por base dados coletados dos indivíduos com informações dissociadas.

Pode-se citar ainda, algumas hipóteses, conforme detalhado no Art. 7º, inciso VIII, “para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”. Caso essencialmente especial, que na área da saúde pode representar momentos inadiáveis para assegurar a vida, a lei permite então que se os dados sensíveis forem indispensáveis ao tratamento, poderão ser utilizados mesmo sem que subsista o expresso consentimento pelo titular ou seu responsável.

Se, como quer Harari, somos todos pequenos “chips”, partes de um enorme processador de informações que é a humanidade, nossos dados pessoais são os bits que descortinam os nossos aspectos arcanos e que possibilitam certa margem de controle sobre nós mesmos; há que se regular, portanto, quais informações circulam por esses “chips”, quem as está promovendo e com qual intento, sob pena de pôr em xeque as liberdades e a própria democracia.

Embora a legislação seja bastante clara no que tange aos elementos que devem ser conferidos ao consentimento a fim de ser expressamente considerado como informado, na prática tem se percebido entraves para a implementação deste poder decisório. Revisitando a história, persistem dúvidas em torno da racionalidade e do poder de barganha dos titulares dos dados pessoais a fim de que possam empreender um controle efetivo sobre seus dados, apesar das quais a legislação tomou o consentimento como elemento nuclear da estratégia regulatória da privacidade informacional. Assim, a aposta é na capacidade, na racionalidade e na habilidade do indivíduo para execercer efetivamente o controle de suas informações pessoais. (BIONI, Op. Cit., p. 137)

O ponto de icógnitas central é sempre checar a existência de algum tipo de subordinação, assimetria de poder, que possa minar a voluntariedade do consentimento, devendo haver uma análise casuística para se concluir se o consentimento pode ser adjetivado ou não como livre.

Apesar de a LGPD não dispor expressamente sobre esse conceito de *privacy by default* em comparação à GDPR (General Data Protection Regulation), é possível extraí-lo do princípio da necessidade, em consonância da responsabilização e prestação de contas. Interpretação que já se fazia possível pela inteleção do que deve

ser um processo genuíno de tomada de decisão desde o Marco Civil da Internet (BRASIL, 2014).

Ante o delineado em linhas alhures, é oportuno destacar a ideia de revogabilidade incondicional, cuja qual encontra fundamento no fato de estar protegendo a própria personalidade, atributos nos quais está a indisponibilidade. Partindo deste pressuposto, o consentimento será sempre revogável e a sua caracterização como ato jurídico unilateral serve a reforçar tal dinância. Nesta concepção, que poderia ser denominada extracontratual, vislumbra a possibilidade de embates futuros ao ser confrontada com a prática, uma vez que esse consentimento, de alguma forma, implica modificação significativa na esfera jurídica de quem, a partir dele, é legitimado ao tratamento dos dados pessoais e esse interesse também merece ser considerado. (DONEDA, 2019)

Para os fins de restar demonstrado o empoderamento do titular dos dados pessoais sensíveis, destaca a LGPD que a comunicação ou o uso compartilhado de dados sensíveis entre controladores, com objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. Como regra, veda-se a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica. Seguindo esta premissa, deverá ser considerado sempre excepcional, pela relevância dos valores em questão, e autorizado somente quando não houver possibilidade de utilização discriminatória das informações coletadas. (DONEDA, 2010)

Há que se pontuar a sistematização mais dificultosa de conflitos, sendo sem dúvidas, aquela que toca o tratamento de dados sensíveis, dotados de alta carga de informação existencial. Quando em “choque”, o tratamento desses dados acaba por definir qual situação existencial será a mais axiologicamente relevante.

Porém, mostra-se relevante salientar que a LGPD veda o tratamento de dados sensíveis com base no “interesse legítimo” seja do controlador, seja de terceiro, visto que essa hipótese não constou entre aquelas autorizativas do tratamento de dados previstas no art. 11 da LGPD.

Apesar dessa ausência, é possível imaginar situações nas quais o legítimo

interesse de um terceiro, ou seja, situações que tenham efetiva relevância em sua esfera jurídica, com eminente caráter existencial e pessoal (CASTRO, 2017), poderia justificar o tratamento de dados com base no seu legítimo interesse. Nessa linha racionológica, pode-se trazer à tona para fins exemplificativos, o tratamento de dados genéticos do doador de sêmen para inseminação heteróloga, feito de forma anônima. O legislador brasileiro, por meio da possibilidade de a pessoa do adotado conhecer sua origem biológica (art. 48, Estatuto da Criança e do Adolescente), legitimou o tratamento de dados genéticos do doador de sêmen, ainda que contrário ao consentimento do seu titular, que buscou o anonimato.

O caminho nessas situações atípicas, contudo, não seria o "legítimo interesse", mas sim o "exercício regular de direitos", base autorizativa ao tratamento de dados pessoais contida na alínea d do inciso II do art. 11 da LGPD, elencada no rol das hipóteses que se dispensa o consentimento expresso.

Em consonância com o exposto até aqui, no que tange ao campo do consentimento, compreende sua ligação direta à função patrimonial que é explicada pelo Direito, como pode se observar nos argumentos de Silva e Melo:

> Dessa forma, o consentimento referente a direitos de personalidade é nitidamente diferente daquele realizado em situações puramente patrimoniais e, como tal, deve ser aferido com uma diferenciada valoração quanto à hierarquia dos valores constitucionais. Assim, a prevalência do valor conferido à pessoa humana pelo nosso ordenamento jurídico constitucional condiciona a interpretação de cada ato ou atividade para que seja realizada à luz da dignidade da pessoa humana (2019, p. 372).

Por fim, à luz do princípio de limitação de uso de dados, parece evidente que o uso discriminatório, ou para algum fim ilegal, seja proibido de início, entretanto há que se refletir sobre a possibilidade de ir além do obvio quando se trata de mineração de dados, para fins de saúde pública, por exemplo. Em razão da pandemia que assola o mundo, a mineração de dados de localização permitiu ao Estado de São Paulo, por exemplo, identificar qual é o percentual de pessoas que estavam respeitando o isolamento social e ficando em casa (CATE, 2013), sendo uma clara utilização de dados para fins diversos do que foram coletados.

As noções destacadas neste capítulo travaram a percepção de uma

capacidade tecnológica de armazenamento e processamento de dados que coloca toda uma sociedade em linha de vulnerabilidade, afinal estamos diante de uma estrutura que movimenta a economia do futuro que a cada dia se mostra atual, conferindo ao titular dos dados uma percepção, por hora ilusionista, de exercer o poder de consentimento sob suas informações. Por conseguinte, será exposto posteriormente quanto ao poder estatal de regulamentação, sendo este fator preponderante na adoção de políticas de segurança de dados, bem como, da privacidade de seus cidadãos, bem como seus respectivos desafios e inoperabilidade. Subsistindo um dever de regulamentar tal atividade, tarefa inglória, efetivamente ao considerar o processos evolutivo tecnológico constante, cujo qual a mente humana não tem sido capaz de acompanhar.

CAPÍTULO III – O BANCO DE DADOS MÉDICOS E SUA (IN)VIOLABILIDADE

As inovações tecnológicas sagraram-se no cotidiano organizacional do relacionamento médico-paciente. Outrossim, ainda que o marco digital tenha revolucionado o campo da saúde, é evidente que se aliou aos inúmeros questionamentos e polêmicas ramificado a partir do armazenamento de dados, primordialmente sensíveis, em bases hospitalares, dentre tais polêmicas, cito a criação de aplicativos e elementos para firmar estrutura operacional do setor, avaliando os riscos de violação, demonstrando os riscos do *ransomware*.

3.1 A criação da ANPD e o cenário de risco que engloba a conjectura atual

Primordialmente cabe mencionar que, a informação detém uma ampla notoriedade e garantir a segurança desta, trata-se de uma prática estratégica-organizacional imprescindível de ser adotada por organizações, sejam elas de cunho público ou privado, em qualquer segmento que exerçam suas atividades. Desta feita, a segurança consiste na presenvação de um tripé de carcaterísticas indeclináveis, sendo: a confidencialidade, a integridade e a disponibilidade. E ainda, acrescenta-se a tal determinação, as propriedades essenciais que denotam a autenticidade, a responsabilidade, o não repúdio e a confiabilidade das informações (ABNT, 2013b; ISO, 2016).

O mundo hodierno experimenta diversas inovações, essencialmente no que se diz respeito às mudanças nos padrões de cuidados à saúde, que inevitavelmente se conectam à era tecnológica, assomando o uso da internet, dispositivos móveis, redes sociais e registros, que permitem o monitoramento de dados clínicos, o que forçosamente veio acompanhado de uma série de impasses no que concerne à governança da informação.

Desta feita, a Lei Geral de Proteção de Dados, com o propósito de supervisionar adequadamente o efetivo cumprimento dos requisitos impostos, cria a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, a fim de funcionar nos moldes de uma agência reguladora, para fiscalizar o tratamento de dados, aplicar sanções e regular matérias.

Imprescindível pontuar que, as autoridades, sejam públicas ou privadas, tem depositado uma expectativa irreal de garantia quanto a segurança dos dados a elas ofertados, consequência clara das ferramentas emergentes, como a anonimização. Ocorre que, gerenciar os bancos de dados pessoais, sobretudo os sensíveis, trata-se de uma tarefa adornada de desafios inerentes. Razão pela qual, enfatiza-se a necessidade de consolidar efetiva proteção, em um cenário aparentemente caótico.

Dessarte, integrando a própria estrutura da ANPD, o Conselho Nacional de Proteção de Dados Pessoais e Privacidade consiste em órgão consultivo multissetorial (art. 58), composto por 23 representantes, que tem o propósito de propor diretrizes para a elaboração e acompanhamento da execução da política de proteção de dados, bem como promover estudos/pesquisas e audiências públicas, e propor ações, inclusive aquelas voltadas à transmissão de conhecimentos, na intenção de conscientizar a população acerca de seus direitos à proteção de dados e à privacidade.

A ANPD, como uma das atribuições mais importantes, deverá dispor sobre padrões técnicos mínimos voltados aos de segurança estabelecidos pelosprincípios do "*Privacy by Design*" e do "*Privacy by Default*", de observância obrigatória aos agentes.

Nesta linha, a Lei Geral de Proteção de Dados destaca o princípio do "Privacy by Design" (art. 46, § 2º), que traduz-se na incorporação de ferramentas de privacidade a partir do momento de criação da normativa, no intento de proteção enquanto perdurar a existência, focando não apenas na adoção de medidas que previnam, garantam e comuniquem todas as possibilidades de riscos ao titular dos dados, mas também no desenvolvimento de sistemas conforme a necessidade e interesse do usuário.

Tem-se que o princípio do "Privacy by Default" (art. 55-J, inciso VIII) configura como um desenrolar do "Privacy by Design". Trata diretamente do dever de configuração de privacidade, que corresponda ao mais restrito, inerete à coleta de dados pessoais a ser realizada por aplicativos, de modo que as informações, além daquelas necessárias, devam ser previamente autorizadas pelo usuário do serviço.

A existência de uma autoridade nacional forte, eficiente e independente segue

ainda a tendência criada pela GDPR nos países europeus, visando que o órgão atenda aos interesses dos cidadãos, como observa Bezerra (2019, p. 56):

> Atualmente, há aproximadamente 120 países com leis vigentes de proteção de dados pessoais e até 2020 esse número deverá subir para cerca de 134. Destes 120 países, aproximadamente 80% editaram uma lei de proteção de dados pessoais e possuem uma autoridade nacional independente, enquanto somente 10% não contam com um órgão independente, por previsões legislativas expressas em obediência a diretivas ou orientações de outros órgãos do Poder Executivo. Nota-se que, embora os modelos de autoridades nacionais sejam os mais variados, estudos demonstram que a maioria dos países optou por um modelo em que o órgão de controle desfruta de um grau de independência bastante elevado.

Nesse contexto, e considerando todo o exposto, a instituição da Autoridade Nacional de Proteção de Dados (ANPD) denota um indispensável papel, quando bem executado, visto que se trata de um órgão regulador e responsável por proporcionar um ambiente de segurança jurídica, fiscalização e orientação a população.

3.2 Os profissionais de saúde como agentes de tratamento

Os Agentes de Tratamento de Dados, conforme prevê a legislação, correspondem ao controlador e operador, sendo responsáveis por manusear as informações prestadas à entidade, de modo que se obrigam a garantir a segurança da informação, conforme expressa previsão na LGPD, mesmo após o término da relação.

Assim, emerge, instantaneamente, a vinculação do profissional de saúde como agente de tratamento de dados, em especial aos sensíveis. De modo que desses se espera a adoção de boas práticas, como revisões e adequações de políticas internas, procedimentos e atividades que envolvam o manuseio de dados pessoais sensíveis, em estrita observância com o firmado na LGPD, independentemente do tamanho da base de dados existente.

Imprescindível sustentar que, os agentes de tratamento, ao lidarem com um base de dados sensíveis, indubitavelmente são interligados ao que preconiza o art 5°, inciso X, da Constituição Federal Brasileira, garantindo proteção da esfera privada de uma pessoa. O direito à privacidade, essencialmente à intimidade, vislumbra abrigo

quanto à interegências externas, alheias, isto é, aquelas que não foram suscitadas pelo titular, de modo que uma informação não poderá ser veiculada ou repassada, sem que haja prévio consentimento.

Segundo preconiza as ilustres doutrinadoras com Celina Bodin e Chiara de Teffé (2016, p.21), quando dispondo de dados pessoais, entidades privadas e governamentais tornam-se capazes de “rotular” e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis. Prosseguindo nesta linha de raciocínio, as autoras sustentam que um acervo suficientemente amplo de informações permite a elaboração de perfis de consumo, o que se, de um lado, pode ser utilizado para incrementar e personalizar a venda de produtos e serviços, de outro, pode aumentar o controle sobre a pessoa, desconsiderando sua autonomia e dificultando a participação do indivíduo no processo decisório relativo ao tratamento de seus dados pessoais, de seu patrimônio informativo.

Pode-se dizer, portanto, que a tônica assumida, no momento que se confere ao titular dos dados o poder de controlá-lo, denota a evidente preocupação do legislador com a privacidade informacional, possibilitando que os agentes de tratamento exerçam o manuseio dos dados, em clara assimetria com o disposto na letra da lei.

3.3 A delimitação de políticas para evitar o vazamento de dados nas bases médicas

É imprescindível pontuar uma ressalva, visto que a LGPD não delimita processos específicos para habilitar ferramentas e garantir a segurança de informações prestadas, dado que apenas desenha hipóteses legais, previstas, para tratar os dados pessoais. Desta feita, não subsiste uma exigência prévia para implementar o *Data Loss Prevention*, que visa impedir o vazamento dos dados, bem como não determina informações que podem ser veiculadas.

Ademais, como a normativa especifíca, os dados tratados são pessoais , e não comerciais. Com isso, há uma linha tênue entre a lei e o compliance, visto que no mundo hodierno isso circunscreve toda movimentação das bases de informações que

circulam no território nacional, de modo que o art. 3° da lei n° 13.708/2018, dispõe que poderá aplicar suas sanções, expondo um rol taxativo, a qualquer operação de tratamento. (BRASIL, 2018)

A LGPD, espelha um avanço extraordinário no que tange à preocupação do Estado com o meio privado do indivíduo, a fim de efetivar as ordens judiciais e uma tendência a evoluir na esfera do Direito Digital Brasileiro.

Importante ainda, trazer à baila que o sujeito moderno pode ser moldado no ambiente virtual, mas a ampla circulação, produção e armazenamento de dados gera, inevitavelmente um ambiente instável, onde as informações são massificadas e o produto desta sociedade digitalizada expropria a intimidade e a privacidade do particular, exposto e vulnerável. (PEIXOTO; PENNA, 2017)

As mudanças nos padrões de cuidados à saúde, associadas diretamente ao momento de revolução tecnológica, transparecem um dos maiores desafios das entidades de saúde que é assegurar que os dados fornecidos pelos pacientes e usuários não sejam violados, divulgados, modificados e até mesmo comercializados. (SAMY; AHMAD; ISMAIL, 2010)

Clarividente mencionar que, as empresas que atuam no segmento da saúde devem ter como foco prioritário, a adoção de mecanismos para proteger e amparar os pacientes, de modo que se sintam seguros aos fornecer seus dados, certos da inviolabilidade do sigilo médico, destacando-se a importância do consentimento, aliado à transparência durante a coleta.

Nesse sentido, o Código de Ética Médica (Resolução CFM nº 2.227/2018) elege como infração ética o ato de “Art. 73: revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente”. Ainda, ao corroborar preceito da Declaração de Genebra de 1924, prevê que o sigilo deve ser respeitado mesmo após a morte do paciente e sobre fatos que sejam de conhecimento público (Art. 73, § único, “a”)

No âmbito da segurança da informação, de acordo com o *Article 29 Data Protection Working Party* (2014), é evidente mencionar que os procedimentos devem objetivar a confidencialidade, a integridade e a disponibilidade das informações

durante todo o seu ciclo, sob pena de configurar um incidente de segurança. As medidas de segurança elencadas pelo legislador perpassam a técnica e a sede administrativa, a qual dependeria de uma estrutura organizacional efetiva dos agentes de tratamento. Considerando tais razões, para que o fluxo informacional se desenvolva adequadamente, é imprescindível a adoção de medidas de segurança com a finalidade de impedir vulnerabilidades, acessos não autorizados ou qualquer incidência que represente um tratamento inadequado dos dados pessoais, que possam provocar danos graves e até mesmo irreversíveis aos titulares do dados.

Outrossim, o setor da saúde não deve se limitar aos cuidados para evitar punições, advertências, multas, impacto de imagem e até mesmo responsabilização de danos nas esfera judicial, uma vez que a LGPD vai muito além dessas limitações. A proteção e segurança dos dados deve se preocupar incisivamente em garantir que as informações não sofram ataques cibernéticos e violações, enquanto é coletada e utilizada para os seus devidos fins.

Fato é que, a LGPD vem suprir uma lacuna das legislações setoriais e provisionar, de modo efetivo, a responsabilização quando da violação dos dados pessoais sensíveis nas mais diversas esferas.

3.4 A criação do DATASUS e a (in)segurança dos *softwares*

Evidente mencionar que a Lei Geral de Proteção de Dados sagrou-se como um marco de avanço às medidas protetivas de privacidades digitais, e um impulso teórico para efetivar as ordens judiciais de remoção do conteúdo da internet e sistemas de gestão. Urge salientar, no que concerne aos dados pessoas sensíveis, a normativa delineou um tratamento diferenciado, considerando a maior vulnerabilidade e o teor essencialmente personalíssimo das informações prestadas.

O ponto chave se encontra no âmbito tecnológico, a citar o *Big Data*, onde temos o cruzamento de dados a fim de relacionar uma série de informações e estabelecer provisionamentos comportamentais e eventos futuros. Ocorre que, tal captura de individualidades, por essência, sigilosas, trata-se de uma violação dos sistemas que direcionam publicidades, tratamentos, produtos e serviços, a fim de influenciar a vida dos usuários, demonstrando a insegurança das atuais bases.

De acordo com o renomado doutrinador Gualtieri (2019), esta base legal possui uma especificidade no artigo 11 da lei, em que é possível o compartilhamento e a comunicação entre controladores no caso da prestação de serviço de saúde, emergindo uma preocupação em como tratá-los.

A tutela da saúde dos titulares de dados, tem uma base legal necessária aos profissionais de saúde. Nesta base legal, é possível realizar o tratamento de dados sensíveis, mesmo sem a autorização do titular dos dados, se o motivo for identificável como tratamento para garantir a saúde da pessoa, a qual se assemelha com a base de interesse vital da pessoa.

A atenção aos dados sensíveis deve ter em vista a crescente importância da informação na conjectura social, o paradigma da hiperconectividade e o progresso das potencialidades tecnológicas fundadas nos dados fornecidos.

Com o desenvolvimento das mais diversas modalidades de inteligência artificial, enquanto subcampo da informática, temos por fim habilitar o desenvolvimento de tecnologias capazes de copiar a inteligência humana ao realizar tarefas, no conceito do pesquisador de Stanford, McCarthy (1956), a humanidade é conduzida a desafios sem precedentes.

A infiltração de mecanismos tecnológicos conduziu, inevitavelmente a sociedade, como bem expôs Rodotà (2019) a uma “ditadura de algoritmos”, onde o indivíduo torna-se prisioneiro de mecanismos dos quais não detém o controle. A gravidade é acentuada no momento em que esses algoritmos são falhos, embora transpareçam neutralidade.

O mundo hodierno denota uma limitação do indivíduo, que em regra deveria dispor de autonomia, como um ser limitado à seus dados, sendo indevidamente restrito, limitado em suas ações existenciais. Rodotà (2019, p.40) bem rememora ao destacar que, considerando a mineração ininterrupta de dados estabelecida entre poderes públicos e privados, as pessoas são transformadas em abstrações, subtraídas inconscientemente a um futuro determinado na era tecnológica.

Perpassando por tais contextualizações, é imprescindível destacar quanto à criação do DATASUS, que data de 30 anos de atuação, formalizado pelo decreto

nº100, de 16 de abril de 1991, a fim de fortalecer o Sistema Único de Saúde (SUS), sendo desde seu “nascimento” um grande aliado nas soluções tecnológicas e softwares. O principal intento figurou no avanço tecnológico para proceder com a coleta, armazenamento e disseminação de dados sobre a saúde no país, para proporcionar planejamentos estratégicos e operacionais no campo médico.

Ocorre que, os efeitos de uma sociedade massivamente moderna são experimentados e visíveis dia após dia. Nesse contexto, o Brasil finalizou o ano de 2021 tematizando um dos maiores ataques cibernéticos da história, a invasão à rede interna do DataSus, que comprometeu o acesso de diversas plataformas mantidas pelo Ministério da Saúde, contribuindo negativamente na capacidade de respostas dos gestores públicos à evolução do quadro pandêmico da COVID-19 no contexto brasileiro.

A invasão ao sistema articulou uma preocupação, antes não experimentada, e salientou a vulnerabilidade do sistema. Nesta linha, pode-se fazer alusão ao escrito por Hobbes, quando minuciou o Estado como o Leviatã, um monstro que se agigantava em todos os aspectos da sociedade aliadas a vida humana, parecia ser ficção. Contudo, quando o movimento de acesso à informação teve início, de fato o Estado fez-se uma criatura desconhecida que matava silenciosamente a individualidade, liberdade e privacidade, a partir de uma constante e oculta vigilância.

Por tais razões, pode-se destacar que a limitação do poder absoluto não implicou mudanças efetivas nos moldes que o Estado coleta as informações do cidadão. Sucede-se que, a partir da consicência das normas legislativas, as discussões sobre o dever informacional do Estado, em relação aos seus cidadãos, ganharam novos rumos, exigindo abertura da governança e transparência.

Conforme preceitua Laura Schertel e aqui destaca-se um recorte: “A confiança dos cidadãos em relação à proteção da privacidade nos sistemas de comunicação e informação sofreu um gravíssimo abalo, a partir do momento em que se revelou que o Estado, que deveria proteger a integridade e a confidencialidade do fluxo de informações, está, ao contrário, violandoas. Retorna, assim, o temor do Estado como o *Big Brother*, que tudo vê e tudo controla, ameaçando direitos já há muito consolidados e colocando em risco a confiança dos indivíduos na infraestrutura da

comunicação e informação, componente vital da sociedade da informação.”

Diante das inúmeras ocorrências de vazamento de dados pessoais, da comercialização de banco de dados, de falhas apontadas nos sistemas e órgãos da Administração Pública, as pessoas temem que suas informações sejam compartilhadas, sem autorização e sejam utilizadas para fins ilegítimos. Trata-se, portanto, da inequívoca necessidade em reduzir o fluxo de informação na sociedades, visto que a simples anonimização não é perfeita.

Pugliesi (2020, p. 56) destaca a importância que as instituições governamentais possuem no que diz respeito à imposição das normas jurídicas aos indivíduos, instituições públicas e privadas, a fim de erradicar os privilégios e injustiças sociais de toda a forma. Cabe aos governos, dotados de legitimidade, ferramentas jurídicas (ex. poder de polícia e poder da polícia) e estrutura administrativa própria, fazer valer as leis, resgatando o ideal de justiça, quando este estiver em perigo.

Os desafios para regular esse “Admirável Mundo Novo”, superam as mais variadas questões éticas e de políticas públicas, haja vista a velocidade com a qual a inteligência tecnológica se desenvolve. Entretanto, é imprescindível enconrajar a implantação de mecanismos que protejam os dados pessoais sensíveis, a fim de dar voz a afirmação dos direitos fundamentais do indivíduo, sem que seja necessário engessar o desenvolvimento das mais infinitas possibilidades de inovação na saúde.

CONCLUSÃO

Fato é que se vive a sociedade da informação, com isso a humanidade se revolucionou, exercendo um controle, até então não experimentado. A era informacional modificou a forma como se faz tudo, mas essencialmente a forme de pensar e agir.

O impacto gerado pelo bombardeiro de dados é múltiplo, gerando efeitos nos padrões de consumo, ideologias, interesses, bem como em um extensa série de fatores que, cabiam, até então, apenas ao círculo social que se relacionavam. Os dados revolucionaram tendências, instrumentalizou a existência do homem, o limitando a números.

A fim de considerar os impactos da informatização, em suas mais diversas facetas, o objetivo principal desta pesquisa foi analisar a lei vigente de proteção de dados (LGPD) no Brasil, bem como suas devidas implicações na relação entre o paciente e a sociedade médica.

A análise deste estudo emergiu a compatibilidade do exercício seguro da medicina, em atenção ao uso coordenado das informações prestadas pelos titulares, seguindo a risca as regras que garantem a proteção contra o uso inapropriado ou não autorizado, em face das novas tecnologias.

Diante de tais pontos, foi possível concluir que há muito a se caminhar no território brasileiro, visto que os avanços tecnológicos alcançaram dimensões distantes do que preconizam as regras jurídicas, por vezes deixando lacunas e icógnitas passíveis de solução.

Isso porque a intensificação das ferramentas inovadoras resultam em intereferências incalculáveis na esfera privada dos indivíduos, essencialmente no que diz respeito aos seus dados pessoais sensíveis e a volatilidade de sua existência informática, podendo ser a qualquer momento invadida e violada.

BIBLIOGRAFIA

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC27002** - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. 2013b. Rio de Janeiro: ABNT, 2013.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Padrão para Troca de Informação de Saúde Suplementar – TISS**. Disponível em: http://www.ans.gov.br/prestadores/tiss-troca-de-informacao-de-saude-suplementar. Acesso em: 01 set. 2021.

BEZERRA, Maria Ruth Borges. **Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei.** Caderno Virtual, v. 2, n. 44, p.1-95, 2019

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 fev. 2022.

_____. **Lei 12.925 de 23 de abril de 2014**. Lei do Marco Civil da Internet. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 mar. 2022.

_____. **Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos.Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 mar. 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Forense. 2019.

BONAVIDES, Paulo**. Curso de direito constitucional**, 6ª ed., São Paulo. 1996.

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Processo Penal e Constituição**. 2017.

CASTRO, Thamis Dalsenter Viveiros de. **A função da cláusula de bons costumes no direito civil e a teoria tríplice da autonomia privada existencial**. Revista Brasileira de Direito Civil, Belo Horizonte, v. 14, out.-dez. 2017. p. 103;106.

CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. **Notice and consent in a world of Big Data**. International Data Privacy Law, Volume 3, Issue 2, mai. 2013, p. 67–73, https://doi.org/10.1093/idpl/ipt005. p. 71. Acesso em: 14 mar. 2022

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 2.227/2018**. Aprova o Código de Ética Médica. Disponível em: . Acesso em: 11 mai. 2022.

DALLARI, Analluza Bolivar. **A LGPD na Saúde**, 1ª ed., São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo**. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 27

_____, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019. (E-book)

GARCIA, Rebeca. **Marco Civil da Internet no Brasil: repercussões e perspectivas**. Revista dos Tribunais, v. 964, 2016, p. 161-190.

KORYREFF, Alan. **A Lei Geral de Proteção de Dados no Direito Médico**. Disponível em: https://www.megajuridico.com/a-lei-geral-de-protecao-de-dados-no-direitomedico/. Acesso em: 26 ago. 2021.

LAW, Thomas. **A Lei Geral de Proteção de Dados:** uma análise comparada ao novo modelo chinês. 2020. 306 f. Tese (Doutorado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2020. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/23402. Acesso em: 28 fev. 2022

McCARTHY, J. **A proposal for the Dartmouth summer research project on Artificial Intelligence, 1956**. Disponível em:

http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf. Acesso em: 21 mai. 2022.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor:** Linhas gerais de um novo direito fundamental. Brasília: IDP, 2019.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**, v. 22, n. 1 2017.

PENNA, Bernardo Schimdt e; PEIXOTO, Juliane Egler Loureiro**.** A sociedade superinformacionista e o direito ao esquecimento: a proteção da memória individual na internet e o aparente conflito com o direito à informação e à liberdade de expressão. **Revista dos Tribunais**, vol. 981/2017, p. 97, jul. 2017.

PESTANA, Marcio. **A Prova no Processo Administrativo-Tributário**. Rio de Janeiro: Ed. Elsevier, 2007

PINHEIRO, Patrícia. **Comentários à LGPD**. 1ª ed., São Paulo: Saraiva, 2019.

_____. Nova Lei Brasileira de Proteção de Dados (LGPD) e o impacto nas instituições públicas e privadas. RT 1.000. Ano 108. Vol. 1000. São Paulo: **Revista dos Tribunais**, 2019.

PUGLIESI, Márcio. Norm as a Promise, International Conventions and Matters of Legitimacy. **In DIGE Direito Internacional e Globalização Econômica** – Vol 2. São Paulo: Edit. Arraes, 2020.

SAMY, G.N.; AHMAD, R; ISMAIL, Z. Security threats categories in healthcare information systems. **Health Informatics Journal**. v.16, n.3, p.201–209, 2010. Disponível em: https://journals.sagepub.com/doi/10.1177/1460458210377468?url_ver=Z39.882003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub++0pubmed%23articleCitationDownloadContainer&#articleCitationDownloadContainer. Acesso em : 18 maio 2022

SILVA, Tiago Vinícius Soares (2020). **O tratamento de dados pessoais sensíveis nas empresas do setor da saúde, segundo a Lei Geral de Proteção de Dados (LGPD).** Dissertação mestrado – Universidade do Vale do Rio dos Sinos.

SINDMED-MG, **Aspectos Práticos da LGPD (Lei Geral de Proteção de Dados) para médicos e clínicas**. Disponível em: https://sinmedmg.org.br/wp-content/uploads/2021/05/CARTILHA-LGPD-_-700x500px-1.pdf. Acesso em: 10 set. 2021.

TOPNEWSTECH. **LGPD:** Saiba como e a Importância de Conhecer. Disponível em: https://direitoreal.com.br/artigos/lgpd-saiba-como-e-a-importancia-de-conhecer. Acesso em: 06 set. 2021

WOLKMER, A. C., & LIPPSTEIN, D. (2017). **Por uma educação latino-americana emdireitos humanos**: pensamento jurídico crítico contra-hegemônico. Revista De Direitos E Garantias Fundamentais, 18(1), 283-301.