A LEI GERAL DE PROTEÇÃO DE DADOS E A ERA DA INTELIGÊNCIA ARTIFICIAL – APLICAÇÃO NA GESTÃO DE CLÍNICAS MÉDICAS

THE GENERAL DATA PROTECTION LAW AND THE ERA OF ARTIFICIAL INTELLIGENCE – APPLICATION IN THE MANAGEMENT OF MEDICAL CLINICS

Fábio S. Santos - Doutorado em Direito Público pela Universidade Federal da Bahia (UFBA). Pesquisador do Centro de Pesquisas em Proteção Internacional de Minorias da USP. Mestrado e Doutorado pela Universidade Salvador (UNIFACS). Pesquisador e Bolsista CAPES. Bacharel em Direito pela Universidade Estadual de Santa Cruz (UESC), Especialista em Direito Público e em Docência do Ensino Superior. Membro do Grupo de Pesquisa em Cidadania e do Núcleo de Pesquisa em Jurisdição Constitucional e Controle de Constitucionalidade (UFBA), e Educação e Desenvolvimento. Pesquisador do Instituto Geográfico e Histórico da Bahia. Professor de Ciência Política e Direito Constitucional e Direitos Fundamentais (UFBA). Professor (Cursos de Graduação e Pós-Graduação, Mestrado e Doutorado) de Direito, Metodologia Científica e Pesquisa Jurídica na Universidade Salvador (UNIFACS); Centro Universitário Maria Milza (UNIMAM); Universidade Católica do Salvador – UCSAL.E-mail: fabiosantosdireito@gmail.com

INTRODUÇÃO

Em seu crescimento como ser humano, cada indivíduo necessita se utilizar de toda informação disponível, se relacionar com ela, compartilhando-a com os outros ese colocando intrinsecamente em sociedade, buscando o desenvolvimento social de todos. Segundo Castells (2002, p. 23-24), "a construção da identidade vale-se da matéria prima fornecida pela história, geografia, biologia, por instituições produtivas, pela memória coletiva e por fantasias pessoais, pelos aparatos de poder e revelaçõesde cunho religioso".

Para Motta (2010), o fornecimento de informações no Brasil, foi amplamente divulgada no século XX, com a construção das redes de "informações e bensimateriais", denominada de redes eletrônicas. A rede eletrônica que mais se destacoue se destaca até hoje é a *internet*, pois possui baixo custo para a criação de atividadesem geral, rapidez na troca de informações, oportunidades de comercialização internacionalmente e mundialmente, além de outros benefícios.

De acordo com Castells (2011), a sociedade atual está envolvida em rede e dessa forma é vinculada por "fluxos", sendo direcionados para o capital, informação, tecnologia. Para o autor, o termo "fluxos" é definido como, "sequências intencionais, repetitivas e programáveis de intercâmbio e interação entre posições fisicamente desarticuladas, mantidas por atores sociais nas estruturas econômicas, política e simbólica da sociedade" (CASTELLS, 2011, p. 501).

E qual é a definição de rede? Nas mais distintas interpretações sobre "rede", utiliza-se nesta pesquisa a interpretação adotada por Castells (2011), o qual afirma que rede é digital e agrega várias diversidades, sendo uma dela as informações de dados. "Uma estrutura social com base em redes é um sistema aberto altamente dinâmico suscetível de inovação, sem ameaças ao seu equilíbrio" (CASTELLS, 2011, p. 566). Vale frisar que a rede digital pode ser considerada libertadora e autônoma, mas que se não utilizada de forma eficiente e eficaz, poderá "mascarar" a realidade eas relações sociais.

As relações sociais surgem como fator fundamental para o desenvolvimento dapessoa natural, entretanto, o direito à liberdade das informações de cada indivíduo, começa a ser questionado, pois é inerente a cada um. Estas informações devem ser preservadas e somente disponibilizadas de acordo com a vontade de seu detentor. Passam a serem reconhecidas como direito humano por inúmeras declarações universais e ratificado pela Constituição Federal (BRASIL, 1988) como direito fundamental, que visa buscar a inviolabilidade dos dados pessoais e consequentemente, a proteção à privacidade de cada um.

Pode-se ilustrar a necessidade da proteção de dados, com um pensamento de Rodotá (2008), onde fala que a proteção de dados, se relaciona intrinsecamente ao direito de personalidade e, não ao direito de propriedade, pois esta liga-se aos fins econômicos e aquela aos dados estritamente pessoais e inegociáveis.

A Declaração Universal dos Direitos

Humanos, em seu art. 12 já previa de umaforma implícita, que todos teriam direito a proteção de seus dados pessoais. Isso também acontecia no Pacto San José da Costa Rica, em seus artigos 11 e 12.

Em 1950, ocorreu na Europa, a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e já chamava atenção para a necessidade da proteção à privacidade (QUINTILIANO, 2021).

Com uma quantidade cada vez maior do uso de transferências de dados, os processos são cada vez mais automatizados, surgindo uma enorme preocupação daEuropa sobre o tema, e em 1981, ocorreu a primeira convenção internacional a tratar sobre o assunto. O tema fundamental desta referida convenção tratava de alinhar os valores fundamentais do respeito à vida privada e da circulação livre das informações dos seus habitantes (QUINTILIANO, 2021).

Com a Diretiva 95/46/CE, de 1995, a Europa criou os alicerces que passaram a balizar os fundamentos para a implantação da proteção de dados pessoais e que também colaboraram para que a mesma fosse adotada por muitos países do mundo, inclusive o Brasil (QUINTILIANO, 2021).

Um dos principais fundamentos para a implantação desta proteção, é identificar que independente de nacionalidade ou residência, cada indivíduo tem direito aliberdade e proteção de seus direitos individuais. E que todos os serviços que visam a proteção dos dados pessoais estão a serviço de cada indivíduo e não, de forma contrária.

Proteger os dados não pode significar a criação de barreiras para impedir o progresso econômico da sociedade. O bem-estar social deve ser priorizado, e somente a segurança criada pela proteção dos dados individuais vai gerar combustível para um aumento exponencial do comércio e do progresso social.

Esse tratamento e proteção de dados, forneceu para cada cidadão a garantia de poder se utilizar desta segurança para, por exemplo, transferir recursos ou informações para quem desejar, sem incorrer em risco de que as mesmas sejam cooptadas por quem quer que seja, sem que possua a devida autorização.

Este sentimento de segurança é que faz com que cada indivíduo sinta-se capaze confiante de disponibilizar suas informações sem que tenha receio de que as mesmas sejam perdidas ou desviadas. Ao mesmo tempo esta troca constante de informações faz com que se crie um panorama complexo com o objetivo de crescimento econômico social, na busca de um, cada vez maior, bem-estar individuale coletivo.

Diante disso as redes digitais e consequentemente as informações de dados, são capazes de evoluir no que concerne a quantidade, extensão e qualidade, apresentando um papel tanto social quanto econômico. Tem função social porque levapara uma maior parte da população acesso e em termos econômicos contribuem paraa fluidez de informações e do próprio capital.

Dessa forma, o desenvolvimento desta rede de dados gerou mudanças na sociedade capitalista, possibilitando formas diversas de produzir, comunicar, relacionar e construir conhecimento.

Deste modo, o objetivo geral deste trabalho foi refletir, a luz do direito da saúde,a Lei Geral de Proteção de dados (LGPD) em clínicas médicas. Já os objetivos específicos foram: a) verificar a importância da implantação da LGPD nas clínicas médicas; b) identificar quais bancos de dados, *softwares* e *hardwares* especiais são indispensáveis para a implantação da LGPD nas clínicas médicas; c) descrever quaisdevem ser os dados que o paciente precisa fornecer as clínicas médicas.

Para realização desse trabalho, adotou-se como procedimentos metodológicosa revisão e leitura de textos, livros e documentos oficiais sobre os assuntos relacionados à temática; o levantamento, sistematização e análise de dados disponibilizados pelos *sites* do governo brasileiro. Dentre os autores utilizados, encontram-se Castells (2002, 2011), Bioni (2019), Maldonado e Blum (2019), Gil (2002) e também a Constituição Federal (BRASIL, 1988), a LGPD (BRASIL, 2018), dentre outras fontes.

Neste trabalho, o método utilizado foi o dedutivo. O estudo apresentou caráterdescritivo e baseou-se em dados qualitativos.

O trabalho foi organizado em seções. A primeira corresponde a esta introdução; a segunda seção identificou a proteção de dados no Brasil; a terceira seção analisoua Lei Geral de Proteção de Dados no Brasil – Lei 13.709/18; já a quarta seção refletiu sobre a Lei Geral de Proteção de Dados nas clínicas médicas no Brasil. Por fim, na última seção obtiveram-se as considerações finais.

As hipóteses para este estudo foram: i) acredita-se que a LGPD deve ser implantada nos serviços de saúde; ii) pensa-se que a eficácia da LGPD nos serviços de saúde só ocorrerá a partir da implantação de banco de dados, *softwares* e *hardwares* especiais; iii) considera-se que para a implantação da LGPD nas clínicas médicas, os pacientes devam autorizar a utilização de seus dados.

O pesquisador motivou-se, em realizar esta pesquisa a partir da dificuldade dasclínicas médicas em saberem como implantar a LGPD. Devido a novidade e atualidade do assunto, não existem fartas bibliografias disponíveis sobre ele no âmbito acadêmico. A relevância social desta investigação consistiu na necessidade da LGPD para normatizar a proteção de dados para todos.

Espera-se com esta pesquisa contribuir para o esclarecimento da importância e da função de refletir sobre a Lei Geral de Proteção de Dados.

Vale frisar que as informações de dados são cruciais nesta pesquisa, pois através destas informações os princípios da igualdade, publicidade, legalidade e transparência serão efetivos.

1 A PROTEÇÃO DE DADOS NO BRASIL

As novas tecnologias de informação e comunicação - TIC trouxeram questionamentos acerca da proteção de dados sociais no mundo.

Para Castells (2011) a sociedade é definida como informacional, global e em rede destacando assimo papel da reestruturação do capitalismo e da gerência dos dados sociais.

Com o surgimento de novas legislações, vindas primordialmente da Europa, empresas

multinacionais começaram a ser obrigadas a se adaptar a estes novos princípios de proteção de dados. E o Brasil, que se utilizava muito da influência europeia e americana, passou a ser pressionado para que tornasse o seu ambiente digital mais protegido e regulado.

De acordo com Klee e Martins (2015, p. 291), o conceito de dados "*são informações. Tecnicamente, são informações que passam por algum tipo de tratamento, ainda que simples coleta, por meio eletrônico ou não". É esta coleta de dados e seu sigilo, que o Brasil começou a pensar em implementar. Os autores também afirmam que "sigilo de dados significa sigilo de informações tratadas, de forma informatizada ou não. E mais: é o sigilo de qualquer caráter nominativo, possibilitando identificar direta ou indiretamente a pessoa referida*" (KLEE;MARTINS, 2015, p. 291).

No Brasil, esta proteção de dados pessoais, chegou com atraso. Enquanto, como dito anteriormente, a preocupação para realizar a implementação desta políticavem desde 1981, no âmbito europeu, aqui, somente começou a ganhar importância na Constituição Federal de 1988.

Somente a garantia constitucional, não bastava para que estes dados fossem tratados de forma coerente e protegidos para garantir o seu sigilo. Surgiu, com isso, a necessidade de se pensar em criar uma regulamentação específica que disponibilizasse as diretrizes, em comum para todos os envolvidos, visando a implementação de práticas que tornasse possível o tratamento das informações que se colocavam cada vez mais complexas e volumosas.

A Constituição Federal/88 em seu art. 5º, incisos X, XII e LXXII diz:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
> *(...)*
> *X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*
> *(...)*
> *XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)*
> *(...)*
> *LXXII - conceder-se-á habeas data:*
> a) *para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;*
> b) *para a retificação de dados, quando não se prefira fazê-lo por*

> *processo sigiloso, judicial ou administrativo (BRASIL, 1988, [s.p.]).*

Se na Europa, já existia a preocupação em proteger os dados pessoais desde1981, no Brasil, a primeira atitude concreta neste sentido foi em 2013, onde o poder judiciário buscou – a partir da justificativa de que o desenvolvimento tecnológico e a internet são fundamentais para a sociedade – garantir os direitos individuais e coletivos dos cidadãos. Surgiu então uma resposta do próprio legislativo brasileiro quando da implementação da Marco Civil da *Internet*. Nele, existiam princípiosrelacionados a proteção de dados pessoais e à privacidade de cada cidadão.

No artigo 5º da Lei 12.965/2014 – Marco Civil da *Internet*, a *internet* é vista como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escalamundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014, [s.p.]).

O Marco Civil da *Internet*, buscava uma melhor regulamentação do ambiente cibernético no país, pois, até o momento, os cidadãos somente contavam com o CDC

- Código de Defesa do Consumidor (Lei nº 8.078/1990) para defender e manter o cadastro de registro dos consumidores em bancos de dados. O CDC se colocava muito frágil e defasada em relação a assuntos relacionados a *internet* e outros meiosdigitais.

> *"O Código de Defesa do Consumidor disciplinou, em seu art. 43, os bancos de dados e cadastros de consumidores. Note-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indomuito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidadedo consumidor (BIONI, 2019, p. 184)."*

Dessa maneira, o Código de Defesa do Consumidor trouxe a proteção de dados dos consumidores, a partir de dois princípios cruciais, a saber: os princípios da qualidade e do livre acesso. De acordo com Doneda (2015, p. 381), outros princípiosestão legitimados no CDC, são eles:

> *"[...] os direitos de acesso (correspondente ao princípio do livre acesso) e de retificação (correspondente ao princípio da qualidade), que possibilitam a ele consultar toda e qualquer informação pessoal a seu respeito armazenada "em cadastros, fichas, registros e dados pessoais e de consumoarquivados" e, no caso de encontrar alguma incorreção, solicitar a retificaçãodo dado (artigo 43, caput e § 3º). Na hipótese de lhe ser negado o exercício de tais direitos, o consumidor poderá se valer dos procedimentos judiciais ordinários (artigo 43, § 4º) ou da já citada ação de habeas data."*

Outra Lei importante para a proteção dos dados do consumidor e do banco dedados, foi a criação da Lei do Cadastro Positivo (Lei 12.414/11), sancionada pela ex- presidente da República Dilma Rousseff. Já em 2012, ocorreu

um caso muito grave com a atriz global Carolina Dieckmann, cujos dados pessoais foram *hackeados* e publicados na *internet*. Com esse fato, foi criada e sancionada a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann.

Evidencia-se a importância de se ter uma Lei que proteja realmente os dados dos cidadãos e que dê uma segurança para que estes dados sejam utilizados em distintas circunstâncias, garantindo a privacidade e transparência nas empresas, instituições, órgãos, etc.

Lemos (2015) acredita que a Lei do Marco Civil ainda não é uma Lei adequada para tantas barreiras jurídicas e técnicas que o direito brasileiro enfrenta. Para o autor, o Marco Civil é importante, contudo sofre com as imperfeições ocorridas com as transformações tecnológicas.

"O Marco Civil é um projeto de lei singular. Não apenas por causa de seu conteúdo, mas também pelo processo que levou a sua criação, debate e aprovação. O Marco Civil estabelece princípios, direitos e deveres para a rede no Brasil de forma articulada com os princípios da democracia. Esse fato pode parecer trivial, mas não é. Vivemos hoje um momento em que a internetenfrenta grande fragmentação técnica e também jurídica (LEMOS, 2015, p. 79)."

Surgiu, então, a imperiosa necessidade de se criar a Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/2018 (BRASIL, 2018), após 30 anos de promulgada a atual Constituição, com o objetivo principal de regular o tratamento de dados pessoais. Com isso, as operações que envolvem coleta, tratamento, utilização e transmissão destes dados passam a existir somente com a autorização do seu proprietário. Assim, as informações pessoais de cada cidadão passam a ter mais transparência e controle do mesmo.

Diante do exposto, a necessidade de uma regulação para usar e tratar os dados não objetiva apenas proteger a privacidade do cidadão, "mas também outros direitos fundamentais e liberdades individuais, que somente podem ser exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais" (MONTEIRO, 2018, p. 02). E quais os direitos que os indivíduos podem "não ter acesso" caso seus dados não sejam protegidos por uma Lei? Para Monteiro (2018), os seguintes direitos são: Direito à saúde; Direito à educação; Direito ao pleno emprego; Direito à informação; Direito à liberdade; e Direito à cidadania.

No que tange ao Direito à saúde, Monteiro (2018, p. 03) afirma que a proteção dos dados e seu acesso,

"[...] pode, ainda, de forma totalmente automatizada, agregar tais dados a bases públicas, como do Sistema Único de Saúde (SUS), e fazer inferências de dados a partir de outras fontes, como redes sociais e dados de locais frequentados pelos indivíduos. Quando cruzados, esses dados formam um perfil comportamental que alimentará sistemas capazes de influenciar de forma contundente o acesso a serviços de saúde de qualidade."

Vale frisar a importância de "fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais" (MONTEIRO, 2018, p. 09). E não apenas

estimular o desenvolvimento econômico, mas também proteger os dados pessoais dos cidadãos.

2 A LGPD NO BRASIL – LEI 13.709/18

Em 14 de agosto de 2018, a Lei Geral de Proteção de Dados - LGPD foi sancionada pelo então presidente Michel Temer entrando em vigor em 18 de setembro de 2020. Com o aumento dos avanços tecnológicos como a inteligência artificial e o *Big Data Bank*, tornou-se imperativo a implementação de um maior controle dos dados no país. E com a implementação da LGPD, o Brasil se colocou entre os 120 países que possuem uma legislação específica em relação a controle de dados pessoais (NONES, 2022).

De acordo com Serpro (2020), existe um grau de adequação à proteção de dados pessoais ao redor do mundo e o Brasil em 2020, se enquadrava na categoria “autoridade nacional e lei(s) de proteção de dados pessoais”, pois ainda estava em fase de implementação da LGPD.Qual o motivo que em 2020 já não se enquadrava em “país adequado”? De acordo com a LGPD (2018) deve existir um período de adaptação concedida a todas as instituições, organizações que armazenam, transferem e tratam de dados a adaptarem-se a nova legislação.

A Lei Geral de Proteção de Dados possui como principal influência para sua criação, o GDPR (*General Data Protection Regulation*), que entrou em vigor para os países europeus e se tornou a legislação mais importante sobre o assunto. Também foi inspirada na Diretiva europeia 95/46/CE, e foi uma junção do Projeto de Lei nº 5.276/2016, de iniciativa da Presidência da República e o Projeto de Lei 4.060/2012, de iniciativa parlamentar.

A LGPD tem como principal objetivo a coleta e tratamento dos dados pessoais,tanto de pessoas físicas ou jurídicas, de direito público ou privado, no território brasileiro. Com isso, toda coleta, tratamento e utilização de dados pessoais por terceiros, estão sujeitos a esta lei.

É importante salientar que a LGPD é aplicável em todos os setores da economia e entrou em vigor em 18 de setembro de 2020, estabelecendo uma série de regulamentações para as pessoas físicas e jurídicas que atuam no Brasil, que passam a ter conhecimento de como serão tratadas as suas informações privadas.

"A Lei Geral de proteção de Dados, em seu art. 2º, incisos de I a VII diz: Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a

> *livre concorrência e a defesa do consumidor; e*
>
> *VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."*

Destaca-se na LGPD alguns elementos/conceitos importantes e que são relacionados a proteção de dados, a saber: **i) dado pessoal:** informação sobre a pessoa identificada; **ii) dado pessoal sensível:** trata-se de dados sobre a origem racial, religião, opinião política, filiação política, vida sexual, etc vinculado a pessoa natural; **iii) dado anonimizado:** não pode ser identificado; **iv) banco de dados:** estruturação dos dados pessoais em meio eletrônico ou físico; **v) titular:** pessoa quese refere os dados; **vi) controlador:** pessoa natural ou jurídica que autoriza o tratamento dos dados pessoais; **vii) operador:** pessoa natural ou jurídica, de direito público ou privado, que trata dos dados pessoais que o controlador pediu; **viii) encarregado:** é o que estabelece a comunicação entre o controlador e os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); **ix) agentes de tratamento:** o controlador e o operador; **x) tratamento:** é a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração dos dados; **xi) anonimização:** um determinado dado perde a possibilidade de associação, diretaou indireta, a um indivíduo; **xii) consentimento:** o titular concorda com o tratamento de seus dados pessoais para uma determinada finalidade; **xiii) bloqueio:** suspensãode tratamento dos dados pessoais ou do banco de dados; **xiv) eliminação:** exclusãode dado; **xv) transferência internacional de dados:** transferência de dados para umpaís estrangeiro; **xvi) uso compartilhado de dados:** comunicação, difusão, transferência de dados; **xvii) relatório de impacto à proteção de dados pessoais:** documentação sobre a descrição dos processos de tratamento de dados pessoais; **xviii) órgão de pesquisa:** órgão ou entidade que inclua a pesquisa básica ou aplicadade caráter histórico, científico, tecnológico ou estatístico; e **xix) autoridade nacional:** órgão da administração pública que zela, implementa e fiscaliza o cumprimento desta Lei em todo o território brasileiro (AGUIAR, 2018).

A Lei Geral de Proteção de Dados cria nove direitos que são cruciais para o titular do sistema.

Os direitos estão expressos no artigo 18 e dão aos indivíduos titulares: 1) comprovação do tratamento dos dados; 2) o acesso aos dados; 3) correção de dados incompletos ou errados; 4) anonimização, exclusão ou bloqueio dos dados; 5) dados entregues a outros serviços; 6) ter dados excluídos; 7) informações sobre as instituições e entidades públicas e privadas sobre o compartilhamento dos dados; 8) informações

que podem negar o consentimento dosdados; e 9) revogação do consentimento (BRASIL, 2018). Salienta-se que a LGPD faz todo seu tratamento de dados exclusivamente no Brasil, ou seja, o titular precisa estar no Brasil quando for realizada a coleta dos dados. Também é preciso que as finalidades da LGPD sejam de ordem econômica, "tenha por objetivo a oferta ou o fornecimento de bens ou serviços; o tratamento de dados de indivíduos localizados e coletados por meio físicos, analógicos ou digitais, no território nacional" (GREGORI, 2020, p. 179).

Gregori (2020) frisa que não são todos os dados pessoais que são tratados na LGPD. Não são tratados os dados. Dentre todos os setores atingidos pela LGPD, o da saúde se coloca como um dos mais complexos e com inúmeros desafios a serem superados para sua implantação. Mesmo com várias acreditações e certificações, inúmeras clínicas estão fazendo um enorme esforço, primeiramente para compreender todos os requisitos necessários, para depois partirem para realizar a implantação da Lei com o intuito deevitar penalidades futuras.

Muitos destes serviços estão tendo que recorrer a consultorias externas para conseguirem se adequar a esta nova realidade. O governo central não forneceu suporte adequado para que clínicas de menor porte (principalmente as localizadas em Salvador e Região Metropolitana) realizassem esta implantação sozinhas, pois existem várias regras novas e a Lei é muito complexa. Entretanto, com relação as multas, começaram a ser aplicadas a partir de agosto de 2021 e em janeiro de 2022 foram implementadas novas regras relacionadas as pequenas empresas instaladas no país.

Entre todas as dificuldades encontradas apresentadas, novos *softwares* e *hardwares* somam-se a elas. A preparação do serviço como um todo para que as novas regras funcionem com perfeição é fundamental. Formulários e a conscientização dos pacientes para a necessidade de seu correto preenchimento também são importantes. Somente assim, o serviço atenderá as regras da LGPD.

Portanto, a LGPD não deve ser temida. É importante salientar que quando uma organização se adequa as diretrizes desta Lei, seguramente torna seus processos muito mais seguros e transparentes. Esta conformidade é fundamental para o negóciocomo um todo, na medida em que deixa muito mais seguro e alinhado com a legislação, evitando, com isso, surpresas desagradáveis no futuro.

O setor de saúde sempre necessitou de uma atenção especial, visto que os dados pessoais nesta área são muito sensíveis. Nas clínicas médicas de pequeno porte não seria diferente, pois funcionários, médicos e pacientes, se encontram envoltos em emaranhado de informações sigilosas, que precisam ser armazenadas de uma determinada forma, que proporcione agilidade e segurança no trato destas informações.

Outro fator importante a ser levado em consideração, é que segundo a Demografia Médica do Brasil, publicação da Universidade de São Paulo (USP) e do Conselho Federal de Medicina (CFM), em 2020, foram ultrapassados os 500.000 médicos no país. O que torna o desafio da implementação da LGPD, maior ainda,

visto que a maioria destes, também trabalham em clínicas médicas espalhadas por todo o país, e realizar uma padronização entre coleta, armazenamento e transferência destas informações sensíveis, será um enorme desafio (SCHEFFER *et al*., 2020).

3 LGPD E SEU REFLEXO NAS CLÍNICAS MÉDICAS

A LGPD certamente cria uma cultura com relação ao tratamento da privacidade das informações pessoais no Brasil.

Clínicas Médicas também tratam com dados pessoais em diversos níveis, entre eles, dados biométricos, patológicos, estatísticos e principalmente os prontuários médicos. Neles, se encontram os dados mais sensíveis de cada paciente que, com a devida autorização dos mesmos, precisam ser tratados de forma segura e rápida para agilizar o atendimento e não comprometer o resultado de cada tratamento.
Para isso, é fundamental que se crie uma política de proteção de dados para aclínica. Nela, todos os processos devem ser identificados e tratados de forma que os dados coletados fiquem protegidos e disponíveis para quem possui autorização paraconsultá-los.

Dados pessoais de cada paciente, como resultados de exames, prontuário médico e principalmente informações sigilosas de cada um, devem ser protegidos. Entretanto, se o paciente estiver inconsciente, devem também ser repassados para seus familiares responsáveis.

Para se adequar uma Clínica a LGPD, primeiramente será imprescindível que se desenvolva uma política de proteção de dados para a mesma. Nela, será necessário que se identifique todos os processos e cuidados necessários para que as informações sejam tratadas de forma adequada, além, da definição dos meios que serão utilizados para comunicação das mesmas.

Outro fator importante, é a criação de meios de proteção dos dados que estejam presentes em fichas e prontuários médicos, principalmente os que estejam envolvidos em situações de sigilo médico. Nestes casos, seria importante criar controles que fossem realizados através de meios tecnológicos, além de intenso treinamento dos usuários e ações que visem a conscientização de funcionários, usuários, prestadorese até mesmo dos próprios pacientes, da importância da proteção destes dados sensíveis.

Dessa forma, para que a LGPD esteja realmente sendo trabalhada pelas clínicas, os servidores precisam seguir o passo-a-passo, a saber:

"*Estudo interno para revisar as rotinas na coleta de dados e implementar instrumentos de proteção dos dados, inclusive com programas de computador, bem como adoção de medidas de segurança para: a.1) controle de acessos às informações; a2) salvaguarda dos bancos de dados; a3) combate contra invasão, perda ou vazamento de informações; b) Avaliação jurídica das responsabilidades sobre as informações de saúde coletadas, com elaboração de contratos e documentos legais para proteção da empresa, além de orientação jurídica para adequação à lei (compliance); c) Desenvolvimento de projeto de*

proteção de dados com sistema de mitigaçãode riscos, emissão de relatórios e práticas de governança corporativa; d) Designação de um líder para organização de todas as atividades da empresaligada aos dados pessoais dos clientes e de terceiros, responsável inclusive pela gestão e acompanhamento deste segmento dentro da corporação; e) Revisão da forma de comunicação e troca de informações entre a empresa e os titulares de dados pessoais fornecidos (transparência); f) Treinamento da equipe de colaboradores para divulgação das novas práticas, implicações jurídicas e responsabilizações pessoais (BATTAGLIA, 2020, [s.p.]).”

É importante também salientar que, a partir de 01 de agosto de 2021 iniciou- se a aplicação de multas para empresas que não se adequaram às diretrizes impostaspela LGPD, com multas de até 2% do faturamento bruto da empresa (limitadas a R$ 50.000.000,00 por infração).

Depois de constatadas as infrações, as empresas também poderão sofrer penalidades como bloqueio e exclusão dos dados pessoais dos clientes; suspenção do acesso ao banco de dados, não podendo tratar as informações, além de ser obrigado que a violação constatada seja divulgada para conhecimento público.

Vale mencionar também, que uma instituição de saúde se preserva a partir dosdados protegidos, através de um ciclo de vida dos dados. Dessa forma a utilização do mapeamento de dados torna-se necessário, no intuito de compreender quais os dados pessoais devem ser manipulados e por onde eles são trafegados nas clínicas médicas. “Entender a importância de cada dado pessoal dentro de fluxos e processos e entender sobre governança de dados cooperapara que o mapeamento seja completo e adequado” (GONÇALVES, 2021, [s.p]).

3.1 DATA MAPPING (MAPEAMENTO DE DADOS)

Data mapping ou mapeamento de dados nada mais é do que um documento ou planilha que mostra o caminho percorrido dos dados (da coleta ao seu descarte). O ciclo compreende sete etapas: a coleta dos dados; o processamento dos dados; a análise dos dados; o compartilhamento dos dados; o armazenamento dos dados; a reutilização dos dados; e a eliminação dos dados.

Nas clínicas médicas essa movimentação de dados incluem os dados dos clientes, colaboradores, parceiros entre outros. Destaca-se a importância de realizar o *data mapping*, pois isso mostra o quanto a clínica, empresa ou outra instituição estáem conformidade com a Lei Geral de Proteção de Dados – LGPD (GET PRIVACY, 2022).

"Sem um mapeamento correto, a tendência é que o projeto esteja fadado ao insucesso, não sobrevivendo à mais simples auditoria, por insuficiência da profundidade do entendimento sobre o cotidiano do tratamento dos dados pessoais e deixando a organização à mercê de problemas de privacidade e proteção de dados pessoais, por consequência (GONÇALVES, 2021, [s.p])."

Justifica-se o uso do *data mapping* para

diminuir os riscos de dados que a instituição poderá enfrentar, pois trará um melhor caminho para o tratamento e uso dos dados, ou seja, a gestão dos dados será melhor realizada, o que acarretará em uma proteção mais efetiva dos dados (GET PRIVACY, 2022).

O mapeamento de dados pode ser realizado por uma equipe multidisciplinar (de técnicos, profissionais da área jurídica, dentre outros presentes no ambiente clínico-hospitalar, objeto abordado neste artigo). A abordagem deve ser direcionada para cada departamento, pois cada departamento apresenta dados distintos e por issoa forma de coleta e tratamento deve ser diferente (GET PRIVACY, 2022).

Quanto ao diagnóstico desse mapeamento de dados, poderá incluir: i) uso de questionários/entrevistas para identificar os dados pessoais do cliente/colaborador etcdentro da clínica médica; ii) estudar o compartilhamento dos dados com terceiros; iii)identificar as bases legais da LGPD no momento de organizar e classificar os dados; e iv) avaliar as normas, procedimentos, processos, etc. A partir desse diagnóstico fica menos difícil de identificar possíveis riscos que podem surgir, assim a clínica médica fará com que o uso dos dados seja mais restrito, restringindo os dados a terceiros quenão estejam cadastrados no sistema (GET PRIVACY, 2022).

De acordo com Maldonado (2019), existem alguns pontos que devem ser mencionados na hora da condução do mapeamento de dados, a saber: 1) Tipos de dados: podendo ser cadastrais, trabalhistas, etc; 2) Volume de dados: alimentado diariamente, semanalmente, etc; 3) Etapas do fluxo de dados: coleta, armazenagem, sanitização, enriquecimento, processamento, segmentação, inferências, transferências, descarte; 4) Tecnologias: aplicação em um banco de dado, sistema, etc; 5) Locais de Armazenamento: o dado é armazenado internamente ou externamente; 6) Origem dos Dados: foram retirados de *sites*, estabelecimentos físicos, aplicativos, etc; 7) Campanhas de *Marketing*: como os dados são tratados influenciará nas campanhas de *marketing*; 8) Compartilhamento de dados com parceiros: indicar os parceiros que receberão os dados tratados; 9) Empresas coligadas: : indicar as empresas coligadas para receber os dados; 10) Localidades dotratamento: qual local é o tratamento dos dados; 11) Transferência internacional de dados: Plataformas de *cloud*; *Data centers* terceirizados; *Software* terceirizados; Transferência para a sede da empresa no exterior; 12) Base Legal: precisa-se indicar qual a base legal do tratamento de dados; 13) Política de Privacidade: tem que apresentar em todas as fases da coleta de dados de forma atualizada; 14) Dados de menores de idade: precisa conter em todos os registros a data de nascimento válida;

15) Retenção e extinção de dados: deve-se identificar a política adotada para a retenção e extinção dos dados; 16) Segurança da Informação: delimitar os controles de segurança da informação para proteger os dados coletados, armazenados, processados, compartilhados e transferidos; e 17) Direito dos Titulares: precisa ser avaliado na proteção de dados.

4 PRONTUÁRIO MÉDICO – FÍSICO E ELETRÔNICO

A palavra *promptuarium* vem do latim e significa o "lugar onde as coisas que pode precisar são armazenadas" ou mesmo, "ficha que contém os dados de uma pessoa" (HOUAISS, 2009, p. 1).

O primeiro relatório médico foi relatado entre 3000 a 2500 a.C., que foi feito porInhotep, médico egípcio, onde registrou em um papiro, 48 casos cirúrgicos. Em 460 a.C., Aristóteles também registrou sobre seus pacientes e as doenças que os afligia. E assim, existiu uma necessidade cada vez maior de anotar os casos de cada pacientepara conseguir uma melhor organização dos mesmos e consequentemente, maior sucesso de cura, já que os profissionais da área de saúde conseguiam seguir um caminho de tratamento já definido.

Já com relação ao Brasil, somente em 1944, na Faculdade de Medicina da Universidade de São Paulo, a utilização do prontuário médico foi implementada pela primeira vez (BACELAR *et al*., 2006).

Com isso, o prontuário médico passa a ser cada vez mais importante na conduta do paciente, pois é nele que são anotadas as informações fundamentais parase construir um melhor tratamento visto a possibilidade de continuidade das ações tomadas.

Desde Hipócrates, no século V, a utilização do prontuário médico ganhou forçae foi cada vez mais estimulado, pois, segundo ele, anotar por escrito todo o histórico de saúde do paciente tinha, principalmente, dois objetivos: acompanhar de forma precisa a evolução da enfermidade e indicar suas possíveis causas. É fundamental salientar que, não somente os médicos registravam em prontuários. Florence Nightingale, responsável por ser a precursora da enfermagem moderna, já realizava tal procedimento quando tratava os feridos da guerra da Crimeia (1853-1856), pois sabia que a continuidade do tratamento era fundamental para obter êxito na cura (SILVA, 2021, p. 1).

Conforme a Resolução CFM nº 1.638/2002, a letra do profissional responsável pelo atendimento do paciente precisa estar legível e não conter muitas abreviações, siglas e sinais impróprios, para que não haja interferência na compreensão do que fora escrito. O prontuário médico serve de matéria prima para pesquisas acadêmicase também pode ser utilizado pela própria instituição onde o mesmo se encontra para fazer uma análise do serviço que este sendo prestado (GARRITANO *et al.,* 2020).

Com a evolução dos meios eletrônicos, surgiram primeiramente sistemas visando o controle administrativo dos serviços de saúde. Após este início, surgiu a ideia de implementar também os prontuários de forma digital, sua consulta seria muitomais ágil e, já que estariam em um servidor de arquivos, poderiam ser visualizados em vários pontos do serviço, sem contar com a segurança, pois deixariam de ser escritos em papel, e passariam a ficar armazenados em lugares muito mais seguros. Surgem, com isso, em 1970, os primeiros Prontuários Eletrônicos do Paciente - PEP (ALMEIDA *et al*., 2016).

Os prontuários eletrônicos surgem com muitas vantagens diante dos que eramde papel. Segurança, unicidade, legibilidade são algumas delas, entretanto, com o número cada vez maior de informações do paciente, o desenvolvimento do prontuário também tornou-se necessário. Nele, agora não somente tinham informações escritas,mas também, imagens e resultados de exames, além de um histórico muito mais completo de sua saúde (ALMEIDA *et al*., 2016).

E em 2002, o Ministério da Saúde Brasileiro, deliberou sobre o Prontuário Eletrônico do paciente, definindo informações imprescindíveis de estarem contidas nomesmo, criando, com isso, um marco regulatório a ser acompanhado. Em consonância com estas diretrizes, o CFM também reconheceu o PEP, ratificando quese tornou a principal maneira de guardar as informações sensíveis pertencentes a cada paciente (SILVA, 2021).

Diversas diretrizes importantes foram criadas pela Lei nº 13.787/18, que se refere a meios de digitalização, guarda, armazenamento e formas de manuseio das informações contidas no prontuário do paciente.

Todo dado referente a saúde do indivíduo deve ser tratado como sensível, conforme o art. 5º, II da Lei Geral Proteção de Dados. Assim, esta disposição passaa se referir diretamente a área da saúde, passando esta, a ser uma das mais impactadas pela LGPD, pois esta lei, criou regras mais rígidas para o tratamento das informações contidas, visando agilidade e transparência para seus proprietários. Quando se fala sobre prontuário do paciente, o mesmo pode ser físico ou digital, sendo um documento pessoal e único, que possui várias informações, de todos os tipos relacionados a saúde do paciente. Ele propicia que diversos membros das equipes multiprofissionais necessárias, tenham acesso a estas informações e construam um tratamento contínuo para o paciente (RODRIGUES, 2021).

Prontuário, segundo a Resolução nº 1.638/02, é definido pelo Conselho Federal de Medicina (CFM) como

"[...] documento único, constituído de um conjunto de informações, sinais, imagens e imagens registrados, gerados a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo (CFM-BRASIL, 2002, p. 184-185)."

O Prontuário é definido pelo Ministério da Saúde como sendo um conjunto de documentos e informações que se encontram catalogados e ordenados e que contém os registros realizados por profissionais de saúde nos serviços públicos e privados (CARVALHO, 2008).

Quando o atendimento ao paciente é realizado por somente um profissional dasaúde, diz-se que o mesmo é uniprofissional, acontecendo, na maioria das vezes emum consultório ou clínica médica. Já quando se chama de multiprofissional, o atendimento está vinculado a um serviço de maior complexidade, onde o PEP fica disponível para que profissionais de diversas áreas acesse (FERNANDES, 2021).

Segundo a resolução 1.821/2007, as regras a serem observadas nos sistemas de prontuário eletrônico, são: 1) Garantir a integridade da informação e qualidade do serviço; 2) Garantir a privacidade e a confiabilidade dos dados e informações armazenadas; 3) Organizar bancos de dados seguros e confiáveis; 4) Garantir a autenticidade dos dados e informações, na medida do possível; 5) Auditar o sistema de segurança; 6) Garantir a transmissão de dados e informações em segurança; 7) Utilizar *software* certificado; 8) Exigir digitalização de prontuários existentes em meio físico; 9) Fazer cópia de segurança na medida do possível (CFM-BRASIL, 2007).

Com isso, foram aprovadas as diretrizes para coletar, e formas de utilizar e armazenar as informações do paciente, sempre preocupadas com a segurança de todo o sistema. O CFM, no art. 1º da Resolução nº 1.821/2007, deixa claro a necessidade de se aprovar através da Sociedade Brasileira de Informática, o manual de Certificação para Sistemas de Registro Eletrônico em Saúde, responsável pelas padronizações nacionais e internacionais em toda área de saúde (CFM-BRASIL, 2007).

É importante salientar que entre a Resolução nº 1.821/2007 e a Lei nº 13.787/2018 existem critérios bastante semelhantes com relação aos prontuários eletrônicos, onde a LGPD em seu art. 2º ratifica a necessidade de integridade, autenticidade e confiabilidade do mesmo. Com isso, o sistema a ser utilizado deve obedecer a previsão do §3º para a regulamentação especifica sobre o assunto e o §2ºsobre as certificações internacionais.

Todas as instituições de saúde do país passam a ser regidas pela LGPD e fiscalizadas pela Autoridade Nacional de proteção de Dados. Os profissionais de saúde envolvidos no tratamento de pacientes precisam possuir um certificado, com assinatura digital, onde será possível acompanhar todos os procedimentos realizados por ele (TEIXEIRA, 2019).

E por fim, conforme art. 5º da Constituição Federal e art. 17º da LGPD, todos os demais profissionais envolvidos na área de atendimento ao paciente, precisam respeitar os direitos fundamentais da liberdade, privacidade e intimidade de todos.

CONCLUSÃO

O surgimento das novas tecnologias de informação e comunicação propiciou um novo olhar para as questões urbanas, principalmente no que tange as questões relacionadas aos espaços de fluxos, no caso em especial ao uso e proteção de dados pessoais. A “sociedade da informação” surgiu com o processo de globalização que proporcionou um aceleramento em três meios, a saber: meio natural; meio técnico (mecanizado); e meio técnico-científico-informacional (SANTOS, 2006). O que se percebe é que a entrada destas novas tecnologias não dava a segurança de que os dados pessoais fossem protegidos neste meio informacional. Assim, Leis de Proteção de dados foram surgindo nos países europeus e na América do Norte, para que houvesse de fato uma garantia de que o cidadão tenha uma vida

privada e segura.

No Brasil antes de surgir a Lei de Proteção de Dados, vários fatores foram surgindo que, de certa forma, levaram a pensar que os cidadãos não eram pessoaslivres, como apontava a Constituição Federal de 1988. Assim, a criação da Lei13.709/2018 (Lei Geral de Proteção de Dados) foi crucial para garantir aos cidadãos uma vida mais digna e menos inquietante, quando ao uso dos seus dados nas redes.A LGPD deve ser mais aprofundada, pois ainda é muito recente fazer uma análise mais complexa. O que se sabe é que todos os setores da sociedade, devemimplementar a LGPD, pois só assim, casos de roubo de dados ou outros crimes sejam evitados.

O objeto de estudo desta pesquisa foram as clínicas médicas, ou seja, o setor da saúde. Nota-se que ainda não há uma vasta bibliografia que trabalhe sobre a temática, nem mesmo sobre aplicação da LGPD em clínicas de porte médio ou pequeno. Com o estudo de reflexão aqui proposto, pôde-se notar falhas na implementação, pois por ser uma Lei recente, muitos profissionais ainda não possuemdomínio sobre o tema. Levando a contratação de consultorias, muitas vezes caras, para implementar a LGPD nas clínicas e dar suporte técnico.

Vale frisar, que no Brasil, deve existir o *data mapping* na fase inicial da LGPD,pois as clínicas médicas precisam avaliar, a partir de planilha ou documento, como osdados pessoais estão sendo geridos, para que de fato haja uma efetiva gerência dosdados dos clientes, colaboradores, parceiros das clínicas, trazendo melhorias, menos burocracia no sistema e menos desgaste econômico e humano, pois facilitará o trabalho.

REFERÊNCIAS

AGUIAR, Antonio Carlos. **A proteção de dados no contrato de trabalho.** 2018.

ALMEIDA, Maria José Guedes Gondim; FIGUEIREDO, Bárbara Barros; SALGADO, Akayana Calegaro; TORTURELLA, Igor Moreira. Discussão ética sobre o prontuárioeletrônico do paciente. **Revista Brasileira de Educação Médica**, v. 40, n. 3, jul./set.2016.

BACELAR, Simônides da Silva; SECUNHO, Geraldo Damião; ALMEIDA, WanderleiMacedo de; OLIVEIRA, Ana Lúcia Lins. In: CONSELHO REGIONAL DE MEDICINA
DO DISTRITO FEDERAL. **Prontuário médico do paciente:** Guia para uso Prático.Brasília: Conselho Regional de Medicina, 2006. Disponível em: www.saudedireta.com.br/docsupload/1370271458PEP.pd. Acesso em: 03 jun.2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição da República Federativa/1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 de nov.2021.

BRASIL. **Lei nº 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: 24 de mai.2022.

BRASIL. **Lei 12.737, de 30 de novembro de 2012**. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 de mai.2022.

BRASIL. **Lei 12.965 de 23 abril de 2014**. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em:

24 de mai.2022.

BRASIL. **Lei 13.709/2018**. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato201 5-2018/2018/lei/l13709.htm. Acesso em:27 de nov.2021.

CARVALHO, Ivana Carolina M. **Prontuário médico e informações sigilosas-impossibilidade de divulgação**. Migalhas, 2008. Disponível em: https://www.migalhas.com.br/depeso/5 2062/prontuario-medico-e-informacoes-sigilosas---impossibilidade-de-divulgacao. Acesso em: 03 jun.2022.

CASTELLS, M. **Ruptura:** a crise da democracia liberal. Rio de Janeiro: Zahar, 2002.

CASTELLS, Manuel. **A sociedade em rede – a era da informação:** economia,sociedade e cultura; v.1. São Paulo, Paz e Terra, 2011.

CNSAÚDE – **Confederação Nacional de Saúde** (2021). Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados- Prestadores-Privados-CNSaude_ED_2021.pdf . Acesso em: 02 jun.2022.

CONSELHO FEDERAL DE MEDICINA (CFM-Brasil). Resolução CFM nº 1.638/2002.
Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, Brasília, 9 ago.
2002, Seção I, p.184-185. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 03 jun.2022.

CONSELHO FEDERAL DE MEDICINA (CFM-Brasil). Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Resolução CFM nº 1.821/2007. **Diário Oficial da União**, Brasília, 2007, Seção I, p. 252. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 03 jun.2022.

DONEDA, Danilo Cesar Maganhoto. Princípios de Proteção de Dados Pessoais. In:LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Perereira de (coords.). **Direito & Internet III – Tomo I:** Marco Civil da internet (Lei n. 12956/2014). São Paulo: Quartier Latin, 2015.p.369-384.

FERNANDES, Márcia Santana. **Prontuário eletrônico e a lei geral de proteção dedados**. Migalhas, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados. Acesso em: 03 jun.2022.

GARRITANO, Célia Regina de Oliveira; JUNQUEIRA, Felipe Holanda; LOROSA, Ely Felyppy Soares; FUGIMOTO, Mayara Sanae; MARTINS, Wallace Hostalacio Avelar. Avaliação do prontuário médico de um hospital universitário. **Revista Brasileira de Educação Médica**, v. 44, n. 1, p. 1-6, 2020.

GET PRIVACY. **Mapeamento de dados:** o que é e qual sua importância na LGPD.Disponível em: https://getprivacy.com.br/mapeamento-de-dados-lgpd/. Acesso em: 06 jun.2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

GONÇALVES, Mariana Sbaite. **Mapeamento de dados pessoais:** o coração do projeto! ConJur. 2021.

GREGORI, Maria Stella. Os impactos da Lei Geral de Proteção de Dados Pessoaisna saúde suplementar. **Revista de Direito do Consumidor**. vol. 127. Ano 29. p.
171-196. São Paulo: Ed. RT, jan.-fev./2020.

HOUAISS, A., Villar, M.S.; FRANCO, F. M. M. **Dicionário Houaiss de Língua Portuguesa**. Objetiva. 2009.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães. A Privacidade,a Proteção dos Dados e dos Registros Pessoais e a Liberdade de Expressão: Algumas Reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). In:LUCCA, Newton de; FILHO, Adalberto Simão;

LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III – Tomo I:** Marco Civil da internet (Lei n. 12956/2014). São Paulo: Quartier Latin, 2015.p. 291-368.

LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. In: LUCCA, Newton de FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III – Tomo I:** Marco Civil da internet (Lei n. 12956/2014). São Paulo: Quartier Latin, 2015.p.79-101.

MALDONADO, Viviane; BLUM, Renato. Coordenadores. **LGPD:** Lei Geral de Proteção de Dados comentada – 1ª Edição – São Paulo: Thomson Reuters Brasil,2019.

MALDONADO, Viviane Nóbrega. **LGPD:** Lei Geral de Proteção de Dados pessoais:manual de implementação. Viviane Nóbrega Maldonado (coord.). São Paulo: Thomson Reuters Brasil, 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteçãode Dados do Brasil. **Artigo estratégico**, v. 39, p. 1-14, 2018.

MOTTA, Marcelo Paiva da. **A infraestrutura informacional no espaço geográfico**. 2010.

NONES, Fernanda. **LGPD:** o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing. Resultados Digitais. 2022. Disponível em: https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/. Acesso em: 03 jun.2022.

PAGLIA E BREUNIG. **Adequação à LGPD - Mapeamento de Dados**. P&B COMPLIANCE. 2022. Disponível em: https://infographya.com/files/P_B_-_Apresentac%CC%A7a%CC%83o_-_Carto%CC%81rios_ARPEN_-_RT_24.05_(1).pdf. Acesso em: 06 jun.2022.

QUINTILIANO, Leonardo. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD)**. IAPD. 2021. Disponível em: https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/. Acesso em: 03 jun.2022.

RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Laura Secfem. LGPD na Saúde: A importância da lei nº 13.787/18para os prontuários. **Consultor Jurídico**. 2021.

SANTOS, Milton. **A Natureza do Espaço:** Técnica e Tempo, Razão e Emoção. 4ªed. 2. reimpressão-São Paulo: Editora da Universidade de São Paulo, 2006.

SERPRO. **O que muda com a LGPD.** 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 02 jun2022.

SCHEFFER, M. *et al*., **Demografia Médica no Brasil 2020**. São Paulo, SP: FMUSP,CFM, 2020. 312 p. ISBN: 978-65-00-12370-8

SILVA, Cristiane Rodrigues. História do Prontuário Médico: Evolução do prontuário médico tradicional ao prontuário eletrônico do paciente. **Research, Society and Development**, 26 jul.2021. Disponível em: //https://rsdjournal.org/index.php/rsd/article/view/18031 Acesso em: 03 jun.2022.

TEIXEIRA, Josenir. **O prontuário do paciente e a lei 13.787/18**: O que mudou?2019.