Lei Geral de Proteção de Dados - Lei 13.709/2018: na Área de Saúde

ARISTEU RATTES FILHO

RESUMO

O presente artigo propõe um estudo acerca da proteção de dados pessoais no ordenamento jurídico brasileiro de acordo com a Lei 13.709/2018 (LGPD), que entrou em vigor em 14 de agosto de 2020 no Brasil, inicialmente, trará um relato sobre a evolução das leis de tratamento de dados no Brasil – far-se-á um referencial teórico crítico abordando a previsão legal prevista na Constituição Federal - uma análise do cenário atual, no que se refere a invasão de privacidade quantos vazamentos de dados pessoais – trataremos dos principais pontos LGPD, abordando que são dados pessoais, dados sensíveis e sua abrangência - fundamentos legais para o tratamento legítimo de dados pessoais, bem como os direitos dos titulares dados e as penalidades.
Palavras-chave: Dados; Privacidade; LGPD; Proteção; Pessoais;

1. INTRODUÇÃO

O nosso tempo, se preocupa com a privacidade e também como garanti-la. O direito durante muito tempo aborda a como uma associação à busca de alguma forma do isolamento, refúgio ou segredo.

Antes da Lei Federal n° 13,709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados ou LGPD), nosso sistema judiciário já tutelava à privacidade aplicável aos dados pessoais através de várias leis esparsas, atos normativos e decisões judiciais. A partir da LGPD[1], o dado pessoal assim classificado pela LGPD ganhou a proteção legislativa propriamente dita.

Hoje a privacidade quanto a proteção dos dados, são assuntos em pautas por grandes juristas, sobre uma orientação de direitos fundamentais, isso se deve, boa parte ao desenvolvimento tecnológico e seus espaços que devem ser submetidos ao tema do judiciário.

Essa evolução se deve principalmente a facilidade de avolumar as informações e a capacidade comunicação, devido ao surgimento da internet, que nasceu no momento da Guerra Fria, em 1960, objetivo de compartilhamento de

[1] Lei Federal nº 13.709/2018 - Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

informações, utilizado inicialmente como estratégia de guerra era uma forma de *backup* de dados.

Na sequência, a aplicação da internet teve vários movimentos, porém cabe destaque é que a internet difundiu inicialmente nos meios acadêmicos, iniciando em Portugal e somente em 1988, entrou no Brasil, para fazer ligações entre universidades brasileiras e americanas.

Atualmente, o mundo vive um cenário de nunca imaginado, um cenário totalmente interconectado, isso através, do uso de aplicativos, sites, *e-commerce*, fato que isso facilitou a coleta de dados, inclusive é comum a utilização os dados ditar regras, de consumos, modos sociais, também, essa coleta facilitou para empresas fazer *marketing* direcionado, barateando assim seus custos.

Em outro sentido essa evolução, trouxe a negatividade, como a exposição de dados de forma lesiva, a *Fake News* que é utilização de informações reais para a propagação de informações falsas, conhecida como a imprensa marrom e os mais diversos crimes cibernéticos.

Na área de saúde o cenário não é diferente, com a facilidade de coleta de dados, principalmente nas grandes estruturas, ela se torna elevada, positivamente essa coleta viabiliza a comparação dados entre indivíduos, pode se dizer que essa comparabilidade fornecerá subsídios para revisões de tratamentos. Por outro lado, a base de dados quando populada com dados sensíveis se tornam um patrimônio incalculável e o seu uso indevido podem causar danos irreparáveis nos indivíduos.

Este artigo busca o entendimento do LGPD, através de uma explanação conceitual sobre alguns termos implantando por esta lei, e a principal preocupação e responder o questionamento se a privacidade dos dados na área da saúde é importante.

2. A EVOLUÇÃO DA TECNOLOGIA

O mundo que conhecemos passou de por várias etapas, teve momento da nossa história que foi a agricultura, a indústria e atualmente a o mundo digital, também denominado, como sociedade da informação.

O presente artigo torna-se relevante, pois, nas últimas décadas ouvimos falar com mais frequência em noticiários sobre a invasão da privacidade no que tange aos dados pessoais, então vem o questionamento, como a lei está se adequando a esses eventos?

Diante da evolução natural da humanidade surge sociedade da informação, e com ela também vem os problemas, cabe a lei regular os conflitos deste novo paradigma de mundo.

Neste sentido, Hugo Assmann, professor e Doutor em Teologia, com ênfase em Filosofia da Educação em seu artigo, conceituam:

> A sociedade da informação é a sociedade que está sempre a constituir se, na qual são amplamente utilizadas tecnologias de armazenamento e transmissão de dados e informação de baixo custo. Esta generalização da utilização da informação e dos dados é acompanhada por inovações organizacionais, comerciais, sociais e jurídicas que alterarão profundamente o modo de vida tanto no mundo do trabalho como na sociedade em geral (ASSMAN, 2020, p. 7-15).

Com a globalização e os avanços tecnológicos nas áreas da informação, o uso da internet e a rapidez da comunicação trouxeram muitos impactos para a vida social, econômica e política das pessoas. Contudo, as novas dimensões, a coleta e o tratamento das informações trouxeram nocividade a privacidade das pessoas quanto a seus dados.

Neste sentido, com a evolução da tecnologia acabou mudando a forma de interação entre pessoas e empresas, muitas vezes de forma lesiva, inclusive ferindo os aspectos constitucionais do direito a personalidade.

Essa comunicação geralmente é robotizada, de um lado está a pessoa o ser humano, conversando com uma máquina, inserindo os mais diversos dados, muitas vezes de foro íntimo, ao apertar um comando, facilmente todo o mundo te conhece, seus dados vão para nuvem, termo utilizado para definir um armazenamento na internet.

Como se fosse um passe de mágica tudo que você conversou com a máquina, não é mais segredo. O exemplo se concretiza mais, quando pesquisamos algo na internet, somos bombeados por *pop-up* (janelas flutuantes), de anúncios das mais diversas empresas, tudo isso, porque quando é inserido uma informação,

roboticamente através de algoritmos ela se propaga, para ramos de negócios conexos, que certamente você não autorizou.

Fato que o uso indevido de informações, como a invasão da privacidade nos dados pessoais, viola a constituição, princípios constitucionais e até leis infraconstitucionais.

No Brasil, após muitas legislações esparsas que eram até então setorizadas, que tentavam acompanhar a evolução da tecnologia e os conflitos que ela causa na vida das pessoas, em 14 de agosto de 2018, foi publicada Geral de Proteção de Dados Pessoais, prevê em seu artigo 65, que a total vigência seria em 24 (meses), ou seja, 14 de agosto de 2020 a Lei nº 13.709/2018, já conhecida como LGPD, que foi redigida com o intuito de mitigar os riscos relacionados ao tratamento indevido e/ou abusivo de dados e, ao mesmo tempo, viabilizar que novos negócios e tecnologias sejam desenvolvidos em um ambiente de segurança jurídica.

Explicitado no Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Neste sentido, está:

> a lei aprovada proporciona ao cidadão garantias em relação ao uso de seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização (MENDES E DONEDA, 2018, p. 566).

Também a importância da Lei:

> a importância da proteção dos dados pessoais está no fato de que a informação passou a ser um bem *extremamente* valorizado na sociedade e no mercado a informação é o ativo mais valioso da atual sociedade, servindo de instrumento de conhecimento, poder e controle, porque a partir dela é possível traçar perfis de porque a partir dela é possível traçar perfis de comportamento, tais como econômico, familiar, político, profissional e de consumo e fundamentar a tomada de decisões econômicas, políticas e sociais (BLUM e SCHUCH, 2019, p. 31) .

A Lei nº 13.709/18, que é a Lei Geral de Proteção de Dados do Brasil, ou, simplesmente, “LGPD”, tem exatamente esse escopo: aplica-se aos setores público e

privado e tenta estabelecer um equilíbrio entre a proteção dos dados dos cidadãos e, no caso do setor público, a utilização desses dados para a elaboração e execução de políticas públicas e a correta prestação de serviços públicos.

Com base na LGPD, faremos uma abordagem nos artigos que se referem ao tratamento dos dados quanto a sua privacidade.

3. SOBRE LGPD E PRIVACIDADE DOS DADOS PESSOAIS

3.1. UM PANORAMA DA PRIVACIDADE E DA PRIVACIDADE DOS DADOS PESSOAIS

No Brasil, o princípio da presunção de inocência, o direito à privacidade, a inviolabilidade do domicílio e a confidencialidade das comunicações gozam de proteção constitucional.

O conceito de privacidade permeia no sentido abordar elementos a necessidades diversas como igualdade e liberdade de escolha, sem ser criticado. (DONEDA, 2020).

O sentido de termos utilizados pela doutrina brasileira para representá-la, propriamente ou não, é considerável; além de “privacidade” propriamente dito, podem ser mencionados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada. (DONEDA, 2020).

A proteção a dados pessoais não é explicitamente reconhecida como um direito autônomo no ordenamento jurídico brasileiro, mas ela é derivada da garantia constitucional da igualdade, liberdade e dignidade humana, assim como da intimidade e da vida privada.

Em relação às leis e princípios internacionais que foram incorporados ao direito interno, o Brasil assinou e ratificou diversos tratados de direitos humanos que garantem o direito à privacidade, incluindo a Declaração Universal dos Direitos Humanos (DUDH), o Pacto Internacional dos Direitos Civis e Políticos, e a Convenção Americana de Direitos Humanos que por muitas décadas o STF (Supremo Tribunal Federal), os adotou.

O Código Civil brasileiro (Lei No. 10.406/2002) inclui o direito à privacidade na categoria mais ampla de direitos à personalidade, junto ao direito à proteção da imagem, da honra e da intimidade do sujeito – facetas do direito do indivíduo de excluir do conhecimento público fatos exclusivamente relacionados a sua vida privada.

Atualmente tramita nas casas legislativas a PEC 17/2019, que transforma a proteção dos dados pessoais, inclusive por meio digital, como sendo direito fundamental, fixa também a União a competência privativa para legislar sobre proteção e tratamento de dados pessoais.

3.2. EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

No ordenamento jurídico brasileiro, a temática, sobre privacidade com foco na proteção dos dados pessoais, era dotada apenas de regulamento e leis infraconstitucionais de forma muito fragmentada e insuficiente para um tema muito abrangente e que interfere na vida de todos.

Como defesa principiológica, tínhamos somente a Constituição Federal de 1998, que trata a privacidade como sendo direito fundamental e da personalidade traduz uma garantia essencial ao pleno desenvolvimento do indivíduo e ao exercício das chamadas liberdades públicas, tendo como expressão a dignidade da pessoa humana.

Diante, de tantas leis fragmentadas, surge a LGPD sigla dada para a Lei Geral de Proteção de Dados (Lei nº 13.709/18), orientada ao princípio da finalidade, visa, proteger os dados pessoais nacionalmente. Ela, foi aprovada pelo Congresso Nacional em agosto de 2018, com uma *vacacio legis,* de 24 (vinte e quatro) meses, portanto, entrou em vigor em 14 de agosto de 2020.

3.3. A NECESSIDADE DA LGPD

A Lei nº 13.709/18, ou Lei de Proteção de Dados Pessoais (LPD), estabelece normas rigorosas para a proteção dos dados pessoais.

Inspirada no também recente Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia.

Na chamada *data driven economy*, contemporânea do Big Data, da Internet das Coisas e da inteligência artificial, cada vez mais negócios e operações se baseiam em dados.

A economia orientada/baseada em dados (*data driven economy)* não é um termo novo, mas um termo em ascensão na transformação digital. Toneladas de dados são gerados diariamente por smartphones, sensores industriais e dados governamentais, conforme ilustra a figura 1, abaixo:

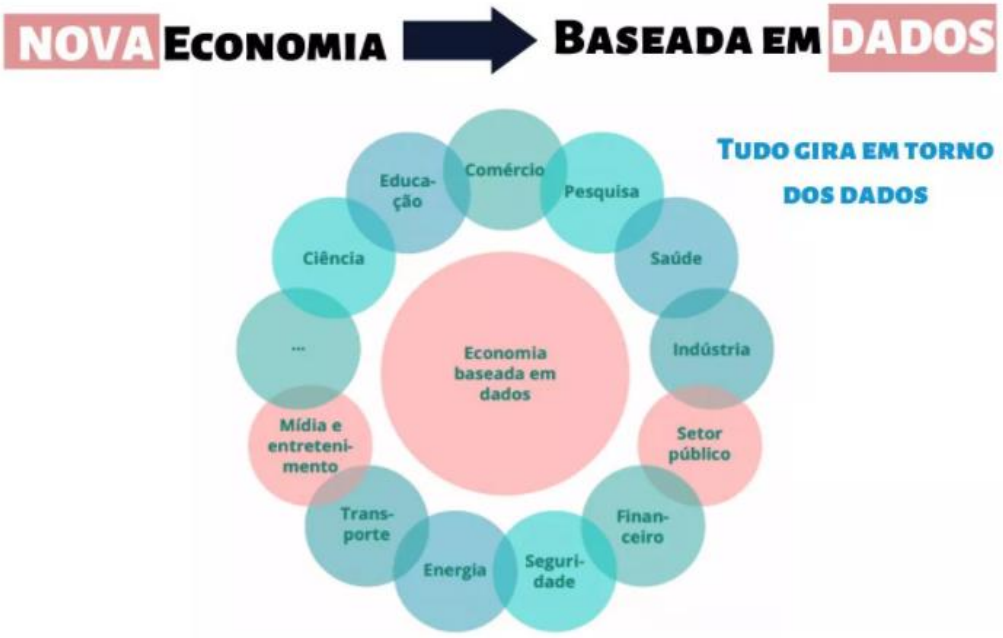

Figura 1 - Data Driven economy – FONTE[2]

A definição de Big Data é um “fenômeno de massificação de elementos de produção e armazenamento de dados, bem como o processo de tecnologias, para extraí-los e analisá-los” (AMARAL, 2016, p. 12).

Ainda, Vieira e Evangelista (2015: p. 524- 533) conceitua, quanto as aplicações de Inteligência Artificial que é definido como um recurso tecnológico que permite o desenho de sofisticados algoritmos que oferecem respostas às indagações humanas, bem como, buscam obter dados dos sujeitos e analisá-los enquanto agentes econômicos e, principalmente, agentes de consumo: ”o que desejam, o que compram, quando e como o fazem, quanto estariam dispostos a pagar por esses desejos, e assim por diante.”

[2] https://marciliodrummond.jusbrasil.com.br/artigos/833073112/incrivel-o-que-e-a-economia-baseada-em-dados, acesso em 068/10/2020 ás 15h.

Para Carvalho (2019), um forte aliado à Inteligência Artificial é a Internet das Coisas. A Internet das Coisas é a ferramenta com mais potencial de modernizar os negócios nos próximos três anos, seguida por inteligência artificial[3] que vem se expandindo rapidamente em bilhões de fontes e dispositivos de dados inteligentes interconectados, levando tudo à conectividade (OWEIS et al, 2016), deste modo, conclui-se que todos os objetos que estão conectados à Internet agem de modo inteligente e sensorial.

Com o desenvolvimento da tecnologia máquina-máquina, espera-se que uma elevada quantidade de dispositivos heterogêneos conectados à Internet das Coisas, em um futuro muito próximo.

Neste sentido a Agência Nacional de Telecomunicações (Anatel), está de acordo e estima que o Brasil já possui cerca de 20 milhões de conexões máquina-máquina. A previsão é que o número salte para 42 milhões em 2020. No mundo todo, até 2025, o total de objetos conectados deve ficar entre 100 milhões e 200 milhões. “Até 2025, cada cidadão brasileiro terá, em torno de si, sete equipamentos máquina-máquina – seja um relógio que está conectado, seja a televisão, seja o carro”[4].

Portanto, trata de dados produzidos com volume, velocidade, variedade, veracidade e valor, em diferentes formatos, em altíssima quantidade, incluindo informações digitais, vídeos e imagens.

Na contramão deste processo estão as empresas brasileiras, que segundo pesquisas do Serasa Experian em 2019, 85% das empresas[5] declaram que não se sentem prontas para atender às novas regras da LGPD. Neste levantamento, foi ouvido um universo de 508 empresas, de vários portes e segmentos, indicou, ainda, que os setores financeiro, serviços e varejo estão mais preparados para a lei. Um

---

[3] Conforme a Pesquisa da KPMG Inovação na indústria de tecnologia 2019 (*Technology Industry Innovation Survey*), com 740 líderes da indústria de tecnologia, as dez ferramentas que irão mudar as empresas a curto prazo serão: 1ª Internet das Coisas, 2ª Automação Robótica de Processos, 3ª Inteligência Artificial e Aprendizado de Máquina, 4ª Blockchain, 5ª Robótica e automação, incluindo veículos autônomos, 6ª Realidade aumentada, 7ª Realidade virtual, 8ª Rede social e tecnologias colaborativas, 9ª Biotecnologia e saúde digital e 10ª Plataformas de compartilhamento.

[4] Palavras do Secretário de Políticas de Informática, Maximiliano Salvadori Martinhão, do Ministério da Ciência, Tecnologia, Inovações e Comunicações, Brasil, 2017.

[5] https://www.serasaexperian.com.br/sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian, acessado em 06/10/2020.

dado marcante é que o setor da saúde ocupa a última posição, com apenas 8,7% das companhias em conformidade com a lei.

3.5. CONCEITOS TRAZIDO PELA LGPD

3.5.1. Principais conceitos da LGPD

Alguns conceitos e são trazidos abaixo, conforme MAGALHÃES (2019, p.10).

O que é a Lei Geral de Proteção de Dados? “Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”

De acordo com Art 5º, inciso X, a lei define o tratamento de dados como: toda operação realizada com dados pessoais, como as que se referem 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.

A quem se aplica a LGPD? A LGPD engloba todos aqueles que realizarem um tratamento de dados, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que os tratamentos sejam realizados em território nacional. Abrange também todas as empresas estabelecidas em território nacional, bem como as organizações com sede no exterior que ofereçam produtos/serviços para pessoas localizadas no Brasil ou tenham operações no País envolvendo tratamento de dados (Artigo 3º).

Quem são os Sujeitos Envolvidos na LGPD? No contexto da Lei Geral de Proteção de Dados surge a figura dos agentes de tratamento de dados. No artigo 5º da referida Lei, encontramos as definições e atribuições dos agentes de tratamento de dados, que foram classificados como Controlador e Operador.

O Titular “pessoa física a quem se refere os dados pessoais”.

O Controlador está definido como “pessoa natural ou jurídica, de direito público ou privado, e que tem com atribuição a competência nas decisões referentes ao tratamento de dados pessoais”.

O Operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador”.

Encarregado - Também chamado de Data Protection Officer (DPO), o Encarregado pela Proteção de Dados é uma pessoa indicada pelo Controlador/Operador para agir como canal de comunicação entre o Controlador e os titulares de dados, e entre o Controlador e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO pode tanto ser interno à organização como externo.

Os sujeitos estão esquematizados abaixo, conforme a Figura 2.

Figura 2 - Sujeitos previstos na LGPD

Quais são os tipos de dados regulados pela LGPD? Dado Pessoal é toda e qualquer informação relacionada à pessoa natural (física) identificada ou identificável[6]. Ou seja, dados como nome completo, e-mail, telefone, RG, CPF e endereço, e dados indiretos como endereços de IP, geolocalização de dispositivo móvel e demais identificadores eletrônicos. Com esses dados é possível monitorar o comportamento e o perfil das pessoas referidas. Portanto, qualquer informação que identifique essa pessoa em específico é considerada um dado pessoal.

[6] LGPD, art. 5º, inciso I.

Abaixo, a Figura 3, tipos de dados segundo a LGPD:

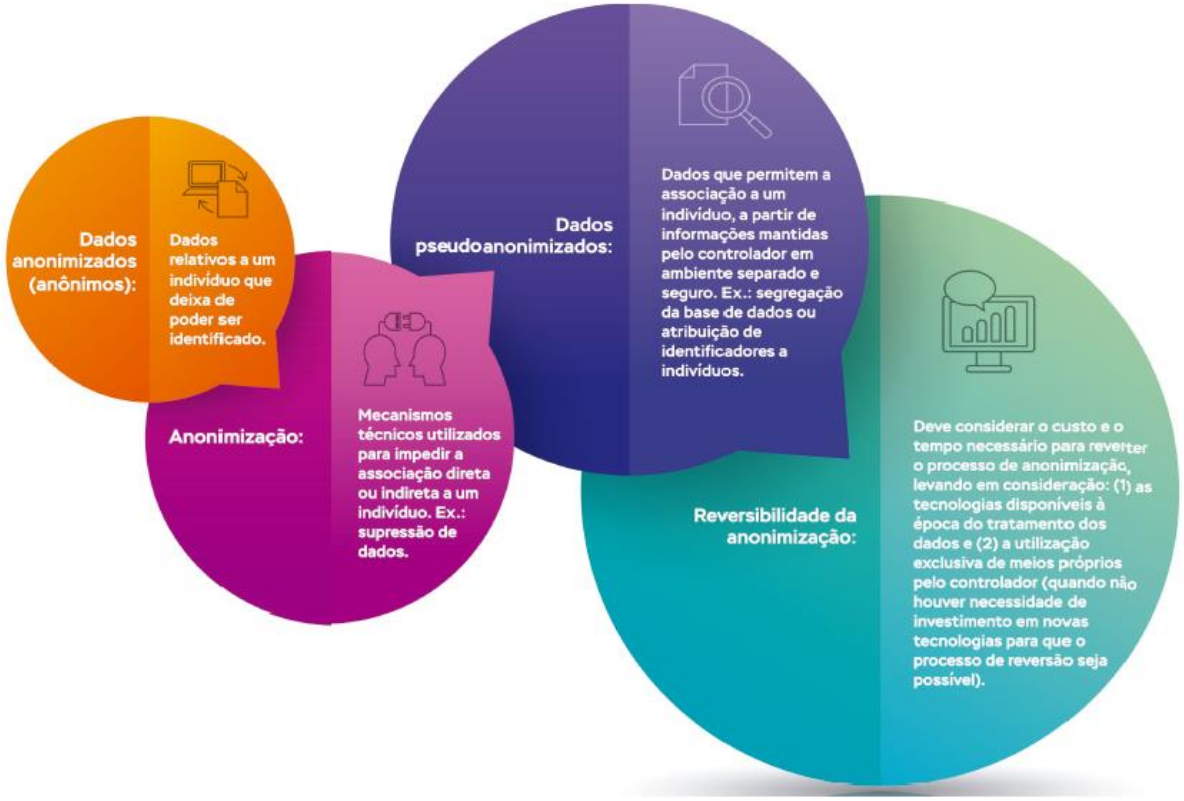

Figura 3 - Cartilha LGPD[7]

Dados Sensíveis: 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; esses dados merecem uma proteção mais rigorosa, com consentimento específico dos titulares dos dados.

Dados Anonimizados (anônimos): “processo em que um dado relativo à titular que não permite ser identificado”[8], considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Esses dados estão fora da proteção da LGPD. Exemplo: estatísticas sobre a idade de pessoas que realizaram a compra de determinado produto.

Dados Pseudo-Anonimizados: processo semelhante ao da anonimização, em que um dado perde a possibilidade de associação, direta ou indireta, a um

[7] https://www.daniel-ip.com/pt/, acessado em 08/10/2020 às 21h
[8] LGPD, art. 5º, inciso XIII

indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro[9]. O pseudo anonimato é incentivado pelo próprio regulamento como forma de reduzir os riscos. Sendo assim, é abrangido pelo LGDP. Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Exemplo: documentos salvos na nuvem.

O Consentimento? É uma das principais novidades da LGPD, está indicado expressamente nos termos expresso dos casos em que as operações de tratamento estarão em conformidade com a lei. Art. 5º, inciso XII da LGPD.

Bancos de dados? Trata-se de uma ferramenta que possibilita a sistematização de volumes de dados que podem chegar a ser gigantescos de informação e também teve seu potencial exponencialmente incrementado com o advento da informática foi, propriamente, o banco de dados. (DONEDA, 2011).

3.5.2. Aplicações

De acordo com o artigo 3º da LGPD, estão sujeitas à aplicação da lei todos os tratamentos de dados pessoais: realizadas no Brasil; que envolvam a oferta de bens ou serviços para titulares que se encontram no Brasil, - seja de modo gratuito ou oneroso -, e independentemente do país em que o tratamento ocorra, e que envolvam dados pessoais coletados no Brasil.

3.5.3. Exceções

Já o artigo 4º da Lei traz exceções expressas à aplicação da LGPD, que se resumem aos tratamentos de dados pessoais realizados para fins: particulares e não econômicos; exclusivamente jornalísticos, artísticos ou acadêmicos; exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, e que não tenham nenhum contato com o Brasil em toda a cadeia do processamento.

---

[9] Lei Federal nº 13.709/2018: “Art. 13. (...)§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.”

3.5.4. Princípios

A LGPD, como as demais leis, também estabelece baseado na boa-fé daqueles atingidos por ela. Naturalmente estamos falando dos princípios, preceituado no Art. 6º da LGPD. Estes versam sobre ações que nem sempre é possível fornecer provas inconteste de que a Lei foi obedecida.

Se aplicam este conceito, hipoteticamente, no caso de uma solicitação feita com uma finalidade pelo titular, e este, presumidamente deduz que o controlador realmente está utilizando seus dados pessoais somente para os fins acordados. Caso apareçam evidências do contrário, aí sim, caberá à Autoridade Nacional de Proteção de Dados tomar as devidas providências punitivas.

Temos como regramento base o princípio da finalidade, “tratamento de dados seja feito para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”,[10] ou seja, que todo e qualquer tratamento de dados pessoais deve ter uma finalidade específica, explicada com clareza para o titular. Nesta premissa, não é permitido coletar dados sem propósito ou que possam vir a ter utilidade para o controlador, pois tudo tem que ser explicitamente detalhado para o titular no momento de solicitação do consentimento.

Pelo princípio da adequação, estabelece “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”[11], ou seja, o tratamento deve realmente acontecer de acordo com as finalidades informadas ao titular no momento do consentimento, utilizando dados e meios adequados, formas de armazenamentos.

Outro ponto importante é o princípio da Necessidade preceitua que independentemente do fim proposto, somente os dados absolutamente essenciais devem ser tratados.

O princípio do Livre acesso o titular tem direito de solicitar certos relatórios e informações sobre o tratamento de dados realizado por sua empresa, este é complementado pelo princípio da transparência no que tange a clareza dos dados.

---

[10] LGPD, art. 6º, inciso I.
[11] LGPD, art. 6º, inciso II.

Trata-se da atualização dos dados, este é o princípio da qualidade dos dados, o titular tem direito a fazer exigências para garantir isso, como pedir a atualização de informações conforme necessário.

Importantíssimo o princípio da Segurança, pois ele narra a tutela da privacidade dos dados, ou seja, é imprescindível e dever do controlador e do operador, tomar todas as medidas para assegurar que o cumprimento dos demais princípios, destarte que isso que estamos falamos é inerente a quem tem guarda as informações.

Pelo princípio Prevenção, temos a segurança dos dados pessoais. Para garantir ainda mais a privacidade dos dados pessoais, deve estar estruturado por políticas fortes de proteção, agindo com prevenção, executando rotinas computacionais.

Não discriminação: sob hipótese alguma podem os dados coletados serem utilizados para fins discriminatórios, como recusar serviços com base em informações étnicas. Isso não impede os controladores de cumprirem as regulamentações de seus setores quanto aos clientes a quem podem ou não prestar serviços — não é ato discriminatório, por exemplo, um banco recusar crédito a um indivíduo envolvido com lavagem de dinheiro.

Pelo princípio da Responsabilização e da prestação de contas o agente deve não apenas adotar as devidas medidas de segurança para proteção dos dados, mas ser capaz de comprová-las. Em casos de incidentes e outras falhas, isso será levado em consideração pela ANPD[12].

3.5. LGPD NA ÁREA DE SÁUDE

Os dados de saúde, por sua vez, têm exigência ainda maior para o consentimento: ele deve ser concedido para finalidades específicas e destacadas. (NUNES, 2020).

Segundo PECK(2019), quando se trata de saúde, existe um ecossistema interligado, fazendo liame entre clinicas medicas, hospitais, perpassando por laboratórios, farmácias, o próprio paciente e os agentes de saúde, bem como toda a

[12] LEI FEDERAL Nº 13.853, DE 8 DE JULHO DE 2019.

esfera pública – como o sistema único de saúde (SUS), enfim a extensão do dados atinge desde o ente privado ao ente público e vice-versa.

O setor de saúde se torna atrativo, devido ao volume de informações sensíveis, para ataques virtuais principalmente os tipos de ataques envolvem o sequestro de dados (*ransomware*) com a prática da chantagem (crime de extorsão).

Vale lembrar que o SUS em 2019, foi alvo de vazamento com dados de 2,4 milhões de usuários[13], segundo informações do blog https://tecnoblog.net/285672/sus-vazamento-dados-usuarios/ acessado em 06/10/2020, a brecha para o vazamento estaria em uma API que permite acessar dados de usuários do SUS.

Segundo o Victor Hugo Silva, repórter, o vazamento envolveu um banco de dados com nome da mãe, endereço, CPF e data de nascimento de pessos cadastradas no serviço.

O Datasus, “Ao Departamento de Informática do SUS – DATASUS, órgão da Secretaria Executiva do Ministério da Saúde, compete a manutenção de bases de

[13] https://tecnoblog.net/285672/sus-vazamento-dados-usuarios/, acessado em 03/10/2020.

dados nacionais, apoio e consultoria na implantação de sistemas e coordenação das atividades de informática inerentes ao funcionamento integrado dos mesmos."[14]

Ele regula a implementação de sistemas e coletas de dados, como é o caso da portaria estabelece que o sistema de informação que permitirá a identificação dos usuários das ações e serviços em todo o território nacional será realizado por meio do Sistema Cartão Nacional de Saúde ("Sistema Cartão")[15].

Com a unificação de cadastro, que visa integrar todos os usuários, é possível de o domínio epidemiológico de acordo com o domicilio residencial, naturalmente respeitando a intimidade. O Sistema Cartão é vasta base de informações e dados dos usuários do SUS compõem a Base Nacional de Dados dos Usuários das Ações de Serviços de Saúde ("Base de Dados").

Outro sistema, instituído pelo Datasus é Sistema de Informação em Saúde para a Atenção Básica (SISAB) foi instituído pela Portaria GM/MS nº 1.412, de 10 de julho de 2013, passando a ser o sistema de informação da Atenção Básica vigente para fins de financiamento e de adesão aos programas e estratégias da Política Nacional de Atenção Básica, substituindo o Sistema de Informação da Atenção Básica (SIAB).

A Administração Pública é, sem sombra de dúvidas, a maior detentora de dados sensíveis dos usuários dos serviços, seja no âmbito do SUS, seja na Saúde Suplementar.

Conforme o site, https://www.alleasy.com.br/2020/01/20/ataques-ciberneticos-brasil-ranking-mundial/, acessado em 03/10/2020, o Brasil está em terceiro lugar no mundo em tentativas de ataques cibernéticos, sendo superados somente por China e Estados Unidos.

---

[14] http://www.ripsa.org.br/vhl/rede-de-instituicoes/ms/departamento-de-informatica-do-sus/, acessado em 03 de novembro de 2020.

[15] Portaria de Consolidação nº 1, de 28 de setembro de 2017 Art. 255. Esta Seção regulamenta o Sistema Cartão Nacio-nal de Saúde (Sistema Cartão), no âmbito das ações e ser-viços de saúde no território nacional. (Origem: PRT MS/GM 940/2011, Art. 1º)

Art. 256. O Sistema Cartão é um sistema de informação de base nacional que permite a identificação unívoca dos usuá-rios das ações e serviços de saúde, com atribuição de um número único válido em todo o território nacional. (Origem: PRT MS/GM 940/2011, Art. 2º)

Em face do nosso questionamento “é importante?”, podemos sem dúvidas nenhuma vivemos em um momento de transição onde o direito tenta acompanhar a evolução da sociedade, neste sentido, a LGPD, vem a contribuir a fim de igualar, gerar mecanismos de responsabilização, de controle, a fim de promover a privacidade dos pessoais.

5. CONCLUSÃO

A sociedade de informação passa por mudanças e a constituição do direito, ora atrás, ora na frente, tivemos na história do Brasil varias leis e normas, embora segmentadas, acompanhando a constituição no que se refere a privacidade.

Estamos otimistas, quanto ao sucesso da LGPD no Brasil, que passa a valer mesmo em 2021, que teremos mais segurança no tocante ao armazenamento das informações, sendo este o primeiro instrumento legal a contemplar exclusivamente a tutela da privacidade dos dados pessoais.

Em diversas narrativas pudemos perceber o crescente volume de informações, armazenados, e as mais diversas técnicas de coletas de dados, e a saúde não é diferente, sendo o setor público o maior detentor dos dados pessoais da população brasileira.

É importante cuidar dos dados pessoais, não economizar em estruturas técnicas para manter os dados a salvo, também primar pela tutela da privacidade dos dados pessoais, independente de qual setor, mas é importante salientar que na saúde os dados são sensíveis e estes jamais poderão vazar, invasão da privacidade e ataca diretamente a dignidade da pessoa humana.

6. BIBLIOGRAFIA

AMARAL, Fernando. Introdução a ciência de dados: mineração de dados e Big Data. Rio de Janeiro: Alta Books, 2016.

ASSMANN, Hugo. A metamorfose do aprender na sociedade da informação, Revista Ciência da Informação – IBICT, Brasília, v. 29, n. 2, p. 7-15, maio/ago. 2000.

ASSMANN, Hugo, https://www.scielo.br/pdf/ci/v29n2/a02v29n2. Acesso em 07/06/2020 às 19h 55min,

BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. Contraponto jurídico. Ed. 2019. p. RB-32.1

CARVALHO, Antonio Ramalho de Souza, Cadernos Adenauer xx (2019), nº3, proteção de dados pessoais: privacidade versus avanço tecnológico - Os dados no contexto da quarta revolução industrial - Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. isbn 978-85-7504-230-4

DONEDA, Danilo Cesar Maganhoto Da privacidade à proteção de dados pessoais. -- 1. ed. -- São Paulo: Editora Renovar , 2006.

DONEDA, Danilo. (2011). A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. 12.

DONEDA, Danilo Cesar Maganhoto Da privacidade à proteção de dados pessoais [livro eletrônico] : elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda. -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

GUTIERREZ, Teresa de Souza Dias, LGPD na saúde – o que as empresas precisam saber, 2019, www.machadonunes.com.br, acessado em 05/10/2020.

LGPD e saúde: os fins justificam os meios?, PECK, Patricia, 2019, https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude, acessado em 04/10/2020.

MAGALHÃES, Lucas Macedo de Magalhães, Machado Nunes, LGPD na Saúde – Tudo o que preciso saber – Ano 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, p. 566, 2018.

Os Agentes de Tratamento de Dados Pessoais, por Paulo Araújo (2019), http://lopesmachado.com/os-agentes-de-tratamento-de-dados-pessoais/, acessado 05/10/2020.

OWEIS, N. E. et. al. Internet of Things: overview, sources, applications and challenges. In: Proceedings of the Second International Afro-European Conference for Industrial Advancement (AECIA) 2015. Cham. 2016, p. 57-67.

Privacidade em perspectivas / organizadores Sérgio Branco, Chiara de Teffé. – Rio de Janeiro : Lumen Juris, 2018.

VIEIRA, Miguel Said; EVANGELISTA, Rafael. A máquina de exploração mercantil da privacidade e suas conexões sociais. 3o Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios. 13 a 15 de maio, 2015. Rio de Janeiro, Brasil, p. 524-533.