UNIVERSIDADE FEDERAL DE OURO PRETO
Departamento de Direito

Tainara Magalhães Cordeiro

COLETA E MONETIZAÇÃO DE DADOS SENSÍVEIS POR FARMÁCIAS:
A influência da LGPD no ramo farmacêutico

Ouro Preto
2021

Tainara Magalhães Cordeiro

Coleta e monetização de dados sensíveis por farmácias: A influência da LGPD no ramo farmacêutico

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Juliana Evangelista de Almeida.

Ouro Preto
2021

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Tainara Magalhães Cordeiro

Coleta e Monetização de Dados Sensíveis por Farmácias: a influência da LGPD no ramos farmacêutico

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 10 de janeiro de 2022

Membros da banca

Doutora- Juliana Evangelista de Almeida - Orientador(a) Universidade Federal de Ouro Preto
Doutor - Roberto Henrique Porto Nogueira - Universidade Federal de Ouro Preto
Mestre - Flávia Coelho Augusto Silva -Universidade Federal de Ouro Preto

Juliana Evangelista de Almeida, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 14/01/2022

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 14/01/2022, às 12:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0268363** e o código CRC **6DC366C5**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.000538/2022-25 SEI nº 0268363

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: 3135591545 - www.ufop.br

RESUMO

O capitalismo de vigilância ou mercado de dados tornou-se nos últimos anos um dos principais ativos econômicos da sociedade moderna, com isso, houve a necessidade de criação de uma lei que regulamentasse especificamente sobre a proteção de dados. O sancionamento da Lei Federal 13.709/2018, tem o intuito de evitar vazamento, abusos, a perda ou o uso indevido dos dados, para fins não autorizados pelos seus titulares. O principal objetivo deste trabalho é analisar em uma perspectiva histórico jurídica quais as mudanças trazidas pela Lei nº 13.709/2018 na coleta e monetização de dados sensíveis no ramo farmacêutico e demostrar como essas mudanças auxiliaram para uma maior segurança dos titulares dos dados, preservando sua privacidade evitando uma exposição negativa de informações sensíveis.

Palavras-chave: LGPD; Dados; Dados sensíveis; Capitalismo de Vigilância; Farmácia; Monetização.

ABSTRACT

Surveillance capitalism or data market has become in recent years one of the main economic assets of modern society, with that, there was a need to create a law that specifically regulates data protection. The sanction of Federal Law 13,709/2018 is intended to prevent leakage, abuse, loss or misuse of data for purposes not authorized by its holders. The main objective of this work is to analyze, from a legal historical perspective, which changes were brought about by Law No. 13.709/2018 in the collection and monetization of sensitive data in the pharmaceutical industry and demonstrate how these changes helped for greater security of data subjects, preserving their privacy avoiding negative exposure of sensitive information.

Keywords: LGPD; Data; Sensitive data; Surveillance Capitalism; Drugstore; Monetization.

SUMÁRIO

1 INTRODUÇÃO

A nova Lei Geral de Proteção de Dados (LGPD) surge em agosto de 2018, apesar de já existirem dispositivos que regem a proteção de dados como legislações esparsas, códigos de conduta e políticas internas, fazia-se necessária uma legislação específica para regulamentar o uso de dados pessoais, a fim de proteger e garantir a segurança de seus titulares.

Apesar do tratamento e monetização de dados contribuir para a qualidade de vida de pacientes e consumidores, demostra-se necessária uma lei regulamentadora com a finalidade de evitar a exposição negativa de dados sensíveis, aumentando o risco de vulnerabilidade de seus titulares.

O presente trabalho tem por objetivo analisar em uma perspectiva histórico jurídica quais as mudanças trazidas pela Lei nº 13.709/2018 na coleta e monetização de dados sensíveis no ramo farmacêutico, destacando como a Lei nº 13.709/2018 passou a tratar com mais rigor a coleta de dados sensíveis, exigindo precauções especiais dos estabelecimentos farmacêuticos.

A Lei Geral de Proteção de Dados impõe as farmácias que se utilizam de dadossensíveis uma governança clara e transparente. Sendo assim, o tratamento e monetização dos dados pessoais pelas farmácias apesar de exigir após a entrada em vigor da lei precauções especiais por tratar-se de dados sensíveis, não é ilícita, desde que efetive o que está assentado no art. 11, inciso I da Lei 13.709/2018.

A monografia em comento estabelece que a coleta desses dados identificáveis passa a ser realizada apenas com o consentimento do titular ou seu responsável legal, de forma específica e destacada, para finalidades específicas com a devida orientação sobre as finalidades do uso dos dados.

Essas mudanças têm o objetivo de trazer mais segurança no uso e armazenamento de dados, afinal, todos esperam que seus dados sejam tratados com responsabilidade e segurança sem prejudicar a privacidade, devendo o indivíduo saber para quem seus dados estão sendo encaminhados e qual o tratamento será dado para cada informação.

A fim de analisar a temática proposta, esta monografia foi pautada na investigação a respeito do tema proposto. Trata-se de uma pesquisa jurídico, dogmática e teórica, foi utilizado como procedimento a análise de conteúdo, mediante

o estudo da Lei nº 13.709/2018, de artigos científicos elencados na presente pesquisa, doutrinas sobre a Lei Geral de Proteção de Dados bem como estudo de casos.

Após o levantamento do material necessário a fim de estabelecer uma avaliação prática do que propõe o estudo, houve a busca do conhecimento teórico referente a contextualização do objeto estudado. Na contextualização foi definido o que é o capitalismo de vigilância, o conceito e a classificação de dados, o que é monetização de dados e as mudanças trazidas após a entrada em vigor da Lei nº 13.709/2018 e por fim como é feita a monetização de dados sensíveis pelo ramo farmacêutico.

Com isso, o trabalho divide-se em 4 (quatro) capítulos, sendo o primeiro reservado a explicação da alteração da nossa sociedade e como os dados hoje são o maior ativo das empresas.

O capítulo 2 (dois) se encarrega de conceituar e classificar um termo essencial para compreender o presente trabalho, os dados pessoais.

Por sua vez, o capítulo 3 (três), visa especificar o que é a monetização de dados e como ela se modificou após a entrada em vigor da Lei nº 13.709/2018.

Por fim, o capítulo 4 (quatro), assume a tarefa central do presente trabalho, explicando como a monetização de dados é feita pelas farmácias após a entrada em vigor da Lei Geral de Proteção de Dados.

2 CAPITALISMO DE VIGILÂNCIA

Ao longo da história, a sociedade sofreu diversas transformações, organizando-se de diferentes formas. Inicialmente, a sociedade era agrícola e os recursos naturais eram o centro da economia, posteriormente na segunda metade do século XVIII a Inglaterra dá início a um período de grande desenvolvimento tecnológico, e surgem as indústrias. Esse desenvolvimento alastrou-se por todo o mundo fazendo com que a economia em escala mundial sofresse grandes transformações, consolidando o capitalismo (BIONI, 2019).

A partir da segunda metade do século XX, houve uma grande expansão das tecnologias digitais em escala global, a internet surgiu e passou a ser fundamental no dia a dia das pessoas e das empresas, que começaram um processo de digitalização muito forte e, com o crescimento exponencial da tecnologia da informação o fluxo imenso de dados pessoais passou a ser visto como um produto. As empresas que detinham essas informações passaram a compartilhar e comercializar dados pessoais entre outras empresas, vez que, esse compartilhamento facilitaria a oferta de produtos de consumo (SANTOS, 2019)

Dessa forma, uma nova ordem econômica surgiria, o Capitalismo da Vigilância. Essa nova estrutura econômica tem como principal atividade a coleta e a análise de dados, principalmente no que se refere as preferências dos consumidores.

O termo Capitalismo da Vigilância (*Surveillance Capitalism*) foi criado pela acadêmica norte americana Shoshana Zuboff e citado em seu livro A era do Capitalismo de vigilância, com base em seus estudos acerca da monetização do *big data* e suas aplicações na sociedade.

Segundo a autora, o capitalismo de vigilância é uma mutação do capitalismo iniciada pelas grandes empresas de tecnologia do Vale do Silício. Zuboff, (2021, p.15) define o capitalismo de vigilância como “uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas”, sendo o *big data* a matéria-prima para empresas preverem comportamentos e, com isso, lucrar.

O que essas grandes empresas faziam/fazem até os dias atuais é utilizar a grande quantidade de dados pessoais que usuários fornecem gratuitamente a elas e transformar esses dados em matéria prima e produto altamente lucrativos.

> O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como *superávit comportamental* do proprietário, alimentando avançados processos de fabricação conhecidos como “inteligência de máquina” e manufaturado em *produtos de predição* que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. (ZUBOFF, 2021, p. 22)

A princípio é importante definir o que são dados pessoais, sobretudo os dados sensíveis. Conforme preceitua a Lei 13.709/2018 em seu artigo 5º trata-se de “qualquer informação relacionada a pessoa natural identificada ou identificável” (LGPD, art. 5º). Deste modo, o dado pessoal pode ser definido como um conjunto de informações, se caracterizando por não ser uma simples informação vaga, mas sim, por estar relacionada a uma pessoa natural, em suma, é a atribuição de qualquer informação a um indivíduo. (COSTA, 2020, p.90).

O dado pessoal sensível, por sua vez, está expresso no art. 5º II, da Lei 13.709/2018:

> 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.

Observa-se por tanto, que os dados pessoais sensíveis são descritos de uma forma taxativa, sendo eles dados de origem racial, étnica, religiosa, opinião política, filiação a sindicato, organizações religiosas, filosóficas ou políticas, dados referentes a vida sexual, genéticos e dados referentes a saúde.

Esse volume complexo de dados coletados que especifica seus usuários é processado e armazenado, dando origem ao *big data.* Laney (2001) associa o *big data* a três “Vs”, são eles: volume, velocidade e variedade.

> Volume se refere à grande quantidade de dados, velocidade seria aquela com a qual as informações são captadas e transmitidas - muitas vezes em tempo real e ininterruptamente, e variedade seria a multiplicidade de tipos de dados e fontes para obtenção destes em larga escala” (GOMES, 2017, p. 20).

O big data coletado passa por análises algorítmicas gerando os chamados *insights,* que segundo Lorena Ferreira Alves (2020) é um termo utilizado por empresas prestadoras de serviços tecnológicos, para se referir às descobertas que são feitas

através da utilização do *big data*. Estes *insights* descobrem padrões de comportamentos dos indivíduos e direciona a esses indivíduos produtos que eles podem vir a desejar e a necessitar, o que aumenta a probabilidades de ganhos econômicos das empresas.

Segundo Zuboff (2021) as empresas de tecnologia extraem as informações e as tratam, aperfeiçoando-as a cada usuário, a fim de antecipar o comportamento humano e vender essas informações aos anunciantes a “preço de ouro”.

> Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de *mercados de comportamentos futuros*. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro. (ZUBOFF, 2021, p. 22).

São inegáveis os benefícios econômicos e sociais advindos com a aplicação da inteligência artificial, a coleta, tratamento e monetização de dados contribui para a melhoria e maior eficiência de medicamentos, tratamentos, qualidade de vida de pacientes e consumidores. Entretanto, a privacidade deve ser preservada, a fim de evitar a exposição negativa de informações sensíveis aumentando a vulnerabilidade dos titulares desses dados.

> Revela-se que os dados pessoais se tornaram um novo tipo de ouro digital, a possibilidade da coleta e do processamento de dados pessoais proporciona à empresas e governos a capacidade não só de entender o comportamento dos indivíduos, como também podem os influenciar tomando ações sutis para criar uma ilusão de escolha para a pessoa, uma vez que todos os seus dados tornaram-se acessíveis por meio de seu “gêmeo digital”, essas entidades usam seu poder de processamento para seus próprios interesses. Esse novo mercado trilha uma linha perigosa entre o legal e a vigilância, fato que não deixou de ser notado, principalmente na atual Era da Informação. (BEZERRA, 2019, p.13).

O ordenamento deve estabelecer controles rigorosos sobre a forma que os dados pessoais são utilizados, visto o risco do vazamento dos mesmos, buscando uma governança clara e transparente.

3 DOS DADOS PESSOAIS: CONCEITO E CLASSIFICAÇÃO

Inicialmente, devemos entender o que é um dado. O dado é o estado primitivo da informação, vez que, não gera informação por si mesmo. Eles são fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação. (BIONI, 2019).

3.1 Dado pessoal

O conceito de dado pessoal é bastante abrangente, o ordenamento brasileiro seguindo a orientação Europeia adotou um conceito amplo de dado pessoal (MACHADO; DONEDA, 2018, p.11), conforme preceitua a Lei 13.709/2018 em seu artigo 5º trata-se de “informação relacionada a pessoa identificada ou identificável” (LGPD, art. 5º, I):

> Art. 5º Para os fins desta Lei, considera-se:
> I- dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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; [..]. (LGPD, 2018)

Em suma, dado pessoal é qualquer informação que permita identificar, direta ou indiretamente, uma pessoa viva, como nome, RG, CPF, data de nascimento, telefone, endereço, fotografia, prontuário de saúde, renda, hábitos de consumo, entre outros.

> Deste modo, o dado pessoal pode ser definido como um conjunto de informações, se caracterizando por não ser uma simples informação vaga, mas sim, por estar relacionada a uma pessoa natural, em suma, é a atribuição de qualquer informação a um indivíduo. (COSTA, 2020, p.90).

A diversidade de informações que identifica um indivíduo pode ser dividida em duas categorias, os dados pessoais e dados pessoais sensíveis, sendo estes dotados de proteção especial e sigilo.

> A especificação dos termos utilizados no contexto dos dados pessoais é particularmente importante e visa resolver os problemas de conceituação e até mesmo categorização que as informações coletadas sofriam. A partir da LGPD, passa a ficar claro e apontável o que é ou não dado pessoal [..]. (PINHEIRO,2020, p.31)

Em outras palavras, a partir da Lei Geral de Proteção de Dados, conseguimos diferenciar com maior clareza o que é dado pessoal e o que é dado pessoal sensível, visto que, o tratamento de dados goza de uma proteção especial para preservação do sigilo, quando trata-se dos dados sensíveis.

3.2 Dado pessoal sensível

No que concerne aos dados pessoais sensíveis que são o objeto central deste estudo, Bioni (2019) entende que são "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação" (Bioni, 2019, p. 84).

Os dados sensíveis são definidos pela Lei Geral de Proteção de dados (Lei 13.709/2018) como como (art.5º, II).

> III- 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;

Conforme o artigo supracitado, os dados sensíveis são informações relacionadas a religião, política, etnia, saúde, dado genético ou biométrico que permitem a identificação de uma pessoa natural.

> Existe a iminência de Dados Sensíveis em Dados Pessoais, no entanto nem todo Dado Pessoal é sensível e, tampouco, nem todo Dado Sensível é pessoal. Nesta relação, se faz necessário o esclarecimento de que Dados Sensíveis tanto ocorrem por meio de dados de pessoas naturais, quanto de pessoais jurídicas (VIGNOLI; VECHIATO, 2019).

Alguns autores como Bioni, defendem que o dado pessoal sensível devido a sua especialidade das restrições impostas ao seu tratamento apresenta um conceito taxativo na Lei Geral de Proteção de Dados (Lei 13.709/2018).

> Sua delimitação é feita por propriedades pontuais descritas em uma lista taxativa, ou seja, que não admite inclusão de outras categorias por extensão conceitual ou similaridade. Assim, por exemplo, o dado “católico romano” é Sensível; ”covarde “não é. (BIONI,2019, p.92).

Lado outro, a autores como Caitlin Mulholland (2019) que defendem que a definição de dados sensíveis não é taxativa, ela apenas enumera algumas hipóteses e isso não significa que outras hipóteses não previstas no artigo 5º da Lei Geral de Proteção de dados não possam ser abarcadas.

> Ressalte-se que esta definição não é, de forma alguma, taxativa ou exaustiva. Trata-se de conceito que enumera de maneira exemplificativa algumas das hipóteses em que serão identificados os dados pessoais que tenham natureza considerada sensível. Isto quer dizer que não somente o conteúdo dos dados previsto neste inciso merecerão a qualificação como dados sensíveis, podendo abarcar outras situações não previstas. (MULHOLLAND, 2019, p. 1)

Caitlin Mulholland (2019) entende que os dados pessoais, propriamente ditos, passarão a ser considerados sensíveis sempre que expor seu titular a algum tipo de situação constrangedora ou discriminatória, bem como informações sobre remuneração, notas acadêmicas, faturas, dados médicos, acordos conjugais, declaração de imposto de renda. Desta forma, o caráter extensivo dos dados sensíveis existe desde antes da vigência da Lei Geral de Proteção de Dados.

Mulholland (2019) destaca em seu artigo que mais importante que identificar a natureza do dado é constatar se o tratamento do dado ensejaria em uma discriminação do indivíduo, afinal, os dados sensíveis não poder ser usados de forma que gere discriminação e um tratamento não igualitário. Por tanto, a autora destaca que mesmo que o dado não seja estruturalmente de natureza sensível ao observar o art. 5º II, ele pode ser considerado como dado sensível a depender da finalidade e o uso feito deles no tratamento de dados.

Por tanto, o tratamento dos dados pessoais sensíveis exige cautela e atenção aos princípios e direitos dos titulares, vez que, o vazamento desses tipos de dados pode trazer consequências mais graves, ferindo o direito e a liberdade dos titulares.

O tratamento dos dados são as operações realizadas com os dados pessoais, elas estão elencadas no inciso X, do Artigo 5° da Lei 13.709/2018.

> Art. 5º Para os fins desta Lei, considera-se:
> X - Tratamento: 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 princípio, o tratamento dos dados pessoais deve ter o consentimento do titular, caso contrário não será legítimo esse tratamento, podendo ter sanções contra quem utilizar os dados sem consentimento do titular.

Os princípios supracitados que devem ser observados para o tratamento de dados, especialmente para o tratamento dos dados pessoais sensíveis, a Lei Geral de Proteção de Dados as estabelece no artigo 6º.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

No que se refere a finalidade, a partir da vigência da Lei Geral de Proteção de Dados não é mais possível haver o tratamento de dados com finalidades genéricas e indeterminadas. O tratamento deve ter finalidade específica, legítima, explícita e informada a seu titular.

A respeito da adequação, os dados pessoais devem ser compatíveis com a finalidade informada pela empresa.

Quanto à necessidade, devem ser utilizados apenas os dados estritamente necessários para alcançar a finalidade desejada

O livre acesso por sua vez diz respeito ao direito do titular dos dados de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito.

Com relação a qualidade dos dados, deve ser garantido aos titulares que as informações sobre eles sejam verdadeiras e atualizadas.

No tocante ao princípio da transparência, as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.

A segurança refere-se à responsabilidade das empresas que coletam e tratam os dados de garantir a proteção dos dados pessoais de acessos por terceiros.

Quanto ao princípio da prevenção as empresas devem adotar medidas a fim de evitar a ocorrência de danos em virtude do tratamento de dados pessoais.

No que concerne ao princípio da não discriminação, os dados pessoais não podem ser usados para discriminar ou promover abusos contra os seus titulares.

Por fim, o princípio da responsabilização e prestação de contas refere-se a cumprir integralmente a Lei, as empresas devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.

3.3 Dados anonimizados

São denominados como dados anonimizados aqueles dados que não possuem um meio de identificação, o inciso III, do Artigo 5° da Lei 13.709/18 preceitua que “dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”.

A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto (HOUAISS; VILLAR, 2009, p. 140).

Segundo Patrícia Pinheiro (2018, p.26), “são os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento”.

Para Martins e Faleiros Júnior (2019) a anonimização de dados é um processo técnico que representa a dissociação entre determinado dado pessoal e o seu respectivo titular. Para seu implemento, inúmeros procedimentos específicos podem ser utilizados, quase sempre a partir da eliminação de determinados elementos identificadores que constam de uma base de dados, por meio de supressão do dado, generalização, randomização ou pseudonimização.

> Importante se ter em mente, porém, que essa conceituação também estabelece, consequentemente, a linha divisória do que é e não é informação pessoal. Se os dados não são relativos a pessoa identificada ou identificável, desde a origem ou após ulterior tratamento, são dados ditos anônimos ou que foram anonimizados. Nos termos do artigo 5º, III, da LGPD, dado anonimizado é “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. (DONEDA; MACHADO, 2019, p. 11)

Por tanto, conforme preceitua José Augusto Fontoura Costa (2020), informações abstratas, genéricas e relativas a pessoas jurídicas ou qualquer outra coletividade estão fora do alcance da conceituação dada pelo artigo em comento.

> Além disso, a noção de dado pessoal não se caracteriza por uma simples informação, mas depende do vínculo desta com uma pessoa natural; caracteriza-se por tanto, como a atribuição de qualquer informação (texto, imagem, fotografia, etc.) a um indivíduo. (COSTA, 2020, p. 90)

Para mais, de acordo com os autores Danilo Doneda e Diego Machado (2019) se o dado não puder ser associado com uma pessoa física identificada ou identificável de forma permanente e irreversível o estatuto de proteção dos dados pessoais não se aplica.

3.4 Definição de big data

Após definir os dados pessoais e os princípios fundamentais para o tratamento de dados, vejamos como esses dados são transformados em produto.

Definimos como *Big Data* o grande volume de dados brutos, esses dados são gerados em grande quantidade, variedade e velocidade e para que esses dados sejam valorados eles precisam ser organizados e tratados (DE FARIAS, 2020)

O big analytics é o processo de análise e transformação do big data com o objetivo de encontrar padrões e tirar conclusões sobre a informação (DE FARIAS, 2020, p.17)

Perante esse grande volume de dados, surge a necessidade de análise destes dados. Neste seguimento, o autor Taurion (2013) aduz que:

> O Big Data e Analytics permitem encontrar padrões e sentido em uma imensa e variada massa amorfa de dados gerados por sistemas transacionais, mídias sociais, sensores etc.Portanto, Big Data cria valor para as empresas descobrindo padrões e relacionamentos entre dados que antes estavam perdidos [...]. (TAURION, 2013, p. 134)

Após esse processo, surge o *Data Insight*, que nada mais é que a análise do comportamento do usuário cujo resultado que é capaz de influir no mercado.

> Os dados precisam, portanto, ser processados e trabalhados para que possam gerar valor. Se tal constatação não afasta a importância em si dos dados isolados ou “crus”, tem o importante papel de realçar o fato de que de nada adianta o acesso a dados sem a possibilidade efetiva e eficiente de transformá-los em informação. Daí a progressiva importância que se dá ao big analytics, ou seja, a possibilidade de extrair, a partir dos dados, correlações, padrões e associações que possam ser consideradas informações e conhecimento. Para tal objetivo, é grande a importância dos algoritmos e das máquinas responsáveis por tal processamento. (FRAZÃO, 2017, p.2)

Nesta perspectiva, observamos que a qualidade do tratamento dos dados é ainda mais importante do que a velocidade em que ela é realizada, pois é o tratamento que define a relevância dos dados.

4 DA MONETIZAÇÃO DE DADOS

Como vimos anteriormente, com o desmedido crescimento da tecnologia de informação o fluxo imenso de dados pessoais passou a ser visto como um produto.

4.1 O que é?

Posto isso, a monetização de dados nada mais é que a utilização dos dados pessoais para obtenção de benefício econômico (ZUBOFF, 2021).

> O conceito de monetização possui várias dimensões, não sendo limitado ao âmbito das informações pessoais e internet, entretanto, nesse contexto, a monetização de informações seria a transformação de coisas que, a princípio, não possuem nenhum valor agregado, em coisas com algum valor, de modo que as informações pessoais podem ser utilizadas como um instrumento para facilitar transações e, ainda, como o próprio objeto dessas transações (ADJEI, 2015, p. 01).

Com essa utilização dos dados pessoais para obtenção de benefício econômico, as empresas passam aproveitar do fenômeno big data para tratar dados pessoais e extraírem lucro desse conjunto de informações. Para Adjei (2015), a monetização de informações é o processo pelo qual ocorre a transformação dos dados em mercadorias que gerem interesse de terceiros e sobre os quais haverá rentabilidade para o responsável pela sua coleta e/ou tratamento.

> Observa-se que, diante da diversidade de tarefas executadas por usuários da rede, apenas um baixo percentual de ferramentas (programas e aplicativos) são efetivamente remunerados pelos que o utilizam, assim os desenvolvedores criaram métodos alternativos de custeio do negócio, como a cobrança de funcionalidade avançadas, a venda de marketing direcionado e a monetização de dados pessoais (DE FARIAS, p.20, 2020).

Primeiramente, antes da monetização, os dados passam pela fase de tratamento. Nesta fase, as empresas ou controladores de dados extraem as informações pessoais do usuário (MALHEIRO,2017). As informações nem sempre eram coletadas com conhecimento do indivíduo, entretanto, após a entrada em vigor da Lei Geral de Proteção de Dados o tratamento de dados pessoais somente pode ocorrer com o fornecimento de consentimento pelo titular, salvo, situações em situações específicas em que a Lei expressamente afasta o consentimento do titular, conforme será apresentado adiante.

Após a fase de tratamento, os dados pessoais passam pela fase de processamento, nesta etapa, os dados pessoais são submetidos a várias técnicas de “lapidação” para transforma-los em informações úteis para as empresas.

> É nesse momento que ocorre a classificação dos usuários e sua segmentação em grupos diversos. Em se tratando da relação de consumo, por exemplo, é aqui o momento em que a empresa atribui valores diferentes para seus clientes, analisa as opções de demanda e conhece os diferentes segmentos para direcionar sua publicidade. Técnicas como mineração de dados (data mining), construção de perfil (profiling) e sistema de avaliação (scoring) são utilizadas nessa fase de tratamento. (MALHEIRO, 2017, p.24).

Segundo Luíza Fernandes Malheiro (2017) a mineração de dados tem o objetivo de extrair padrões, permitindo a classificação de pessoas ou objetos. A construção de perfil por sua vez, possibilita a reunião de uma diversidade de dados sobre o usuário a ponto de definir sua personalidade. Por fim, o sistema de avaliação é a técnica da fase de tratamento de dados que define quais os usuários têm maior valor para a empresa, para que eles sejam alvos de promoções e estratégias de fidelização de clientes. (MALHEIRO, 2017).

> [...] com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma “economia de vigilância” que tende a posicionar o cidadão como um mero expectador das suas informações (BIONI, 2019, p.39).

Por fim, a última fase do tratamento de dados seria a difusão ou cessão de dados, a chamada “indústria de bancos de dados” (MALHEIRO, 2017).

> Essa monetização se dá no âmbito do "*Big data*" — conceito que envolve a captação, armazenamento, processamento e capitalização de dados e informações. Através do tratamento desses dados, é possível aprimorar, por exemplo, a publicidade dirigida, baseada em padrões de acesso e consumo, e até mesmo influir no hábito do usuário da internet, escolhendo o que mostrar e o que não mostrar, capitalizando também em cima disto (e até mesmo influenciando o resultado de processos políticos, como sugerem alguns estudiosos). (GUIMARÃES, 2018, p.382).

Neste seguimento, são produzidos os chamados insights automatizados, que são o mapeamento que possibilita a definição do perfil do usuário, como suas preferências de consumo, gostos pessoais, dentre outros (DE FARIAS, 2020).

> A partir da produção desse insight pode-se alcançar, por exemplo, o aumento da retenção de clientes e diferenciação competitiva. Acrescido da mudança de comportamento dos consumidores, que desejam não mais serem vistos como números, mas como indivíduos, as propostas personalizadas chamam a atenção. Através dessa demanda do mercado, muitas empresas se empenham em tornarem-se especialistas na coleta de dados, desenvolvendo, assim, a expertise para descrever de modo fidedigno seus usuários, no que tange a gostos pessoais, opiniões, hábitos de consumo, dentre outras características (DE FARIAS, 2020, p.20).

Existem formas diferentes para utilizar as informações coletadas como fonte de lucro. Uma organização pode coletar e tratar os dados de seus clientes a fim de personalizar o serviço prestado ou o produto vendido a esses mesmos clientes, assim as informações são utilizadas como um meio para facilitar e aprimorar as transações dessa organização. Lado outro, pode haver a coleta e o tratamento de dados com objetivo de repassar para um terceiro, mediante contraprestação, de modo que as informações tornam se o próprio objeto da transação. (MODESTO, 2020).

> O caminho, como visto, é se utilizar dos dados coletados para vender produtos ou serviços de forma mais direcionada ao usuário específico, aperfeiçoando os relacionamentos entre os empresários e seus clientes, bem como compartilhar esses dados com terceiros que busquem ampliar a sua base de dados para além da sua própria carteira de clientes. (MODESTO, 2020, p. 6).

O grande problema que surge com a monetização dos dados pessoais diz respeito a maneira como as informações serão protegidas e utilizadas.

> Percebe-se que a evolução das técnicas no tratamento de dados pessoais possibilitou a combinação de dados em seu estado bruto, a princípio sem muita importância, para a criação de novas informações úteis e valiosas. Contudo, ao passo que essas técnicas ampliaram as oportunidades de ação dos indivíduos, elas também ampliaram os riscos a que os indivíduos podem ser submetidos. (MALHEIRO, 2017, p. 25).

Muitas vezes falta transparência/informações por parte das empresas e também a negligência dos usuários ao ignorarem os termos de uso, os termos de consentimento tornaram-se eivados de vícios. Sendo assim, surge a necessidade de criação de normas legais capazes de garantir a tutela do usuário quanto aos seus direitos (DE FARIAS, 2020).

4.2 Monetizações antes da LGPD

A proteção de dados pessoais já era mencionada em regulamentos anteriores, entretanto, os países europeus passaram a ter uma preocupação de fato com a proteção de dados e o instituto do consentimento em 1980 (KRIEGER, 2019).

Na perspectiva de Krieger (2019), no Brasil a proteção é tratada desde a Constituição Federal de 1988, visto que, o seu artigo 5º estabelece nos incisos X e XIV:

> 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; XIV é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

De acordo com Lugati e Almeida (2020), o Código de Defesa do Consumidor também estabelecia proteção de dados. O artigo 43, expressa que os cadastros dos consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, além disso a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor.

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)

Por sua vez, o Marco Civil da internet (lei nº12.965/2014), é uma lei de 2014 que foi sancionada a fim de estabelecer ditames para o uso da internet no Brasil, e até a entrada em vigor da Lei Geral de proteção de Dados, foi a principal lei usada para garantir a proteção de dados pessoais (CARVALHO, 2019).

Segundo Chaves e Vidigal (2021), alguns artigos do Marco Civil da Internet deveriam ser considerados tacitamente revogados, posto que, são incompatíveis com a LGPD, dentre eles, artigos referentes a bases legais para o tratamento de dados pessoais.

> Artigo 7º: VII não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> Artigo 7º: IX consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> Artigo 16: Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no artigo 7º" .

Conforme será apresentado no tópico posterior deste trabalho, o artigo 7º da Lei Geral de Proteção de Dados prevê 10 hipóteses para o tratamento de dados pessoais, o consentimento é apenas uma delas, contrariando o disposto pelos artigos supracitados do Marco Civil da Internet.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - Mediante o fornecimento de consentimento pelo titular;
> II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019).

> IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No ano de 2016, com intuito de regulamentar o Marco Civil da Internet, foi criado o Decreto nº 8771/2016, no entanto, ambas as legislações não trataram de forma efetiva a questão da proteção de dados pessoais e seu tratamento, por isso, posteriormente o ordenamento jurídico brasileiro teve a necessidade de criar uma legislação que disciplinasse de maneira mais abrangente a proteção e o tratamento de dados. O Decreto completou a proteção de dados, trazendo definições importantes, como a de dado pessoal, tratamento de dados pessoais e dados cadastrais. (CARVALHO, 2019).

> Dado pessoal, disposto no decreto, é o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016), e tratamento de dados pessoais seria "toda operação realizada com dados pessoais" (BRASIL, 2016), elencando no bojo do art. 14 as possibilidades de operações. Entretanto como se trata de uma definição ainda bastante genérica de dado pessoal, a efetiva proteção vai depender de interpretações que podem colocar em risco a privacidade do usuário da internet.
> Já os dados cadastrais seriam uma espécie de dado pessoal que teriam tratamentos diferenciados. Seriam os dados que qualificariam o indivíduo – nome, prenome, estado civil, profissão, filiação e endereço70, e, em razão da sua natureza seriam menos sigilosos e se encontrariam numa esfera mais pública (CARVALHO, 2019, p.63).

Segundo Krieger (2019), o Marco Civil da Internet também estabelece o direito de os titulares dos dados requererem a exclusão definitiva de suas informações pessoais após finalizada a relação com aqueles que coletaram seus dados devidamente.

> Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação. (BIONI, 2018, p. 132)

Por tanto, conclui-se que o Marco Civil da Internet e o Decreto contribuíram para a proteção de dados na internet, entretanto, não afastou a necessidade da criação de uma Lei que regulamentasse de forma efetiva a proteção de dados

pessoais, a fim de que o titular dos dados seja protegido em todo o processo desde a coleta até a possibilidade de monetização dos dados.

Consoante ao exposto anteriormente, o tratamento e compartilhamento de dados a terceiros gratuita ou onerosamente, só poderia ocorrer mediante consentimento livre, expresso e informado, por tanto, as demais hipóteses apresentadas pela Lei Geral de Proteção de Dados não eram permitidas, entretanto, observamos que o consentimento continua sendo a base para o tratamento e monetização de dados.

De acordo com Coimbra (2020), a Lei Geral de Proteção de Dados surge para complementar o Marco Civil da Internet, tratando de direitos e garantias fundamentais, trazendo maior proteção e segurança a privacidade dos dados. Ademais, a Lei nº 13.709/2018 visa a autodeterminação informativa, conferindo ao titular dos dados a palavra final sobre como seus dados serão tratados.

4.3 Monetizações após a LGPD

Após a entrada em vigor e aplicação da Lei Geral de Proteção de Dados houveram algumas mudanças significativas, vez que, a mesma impõe a necessidade de revisões de processos e procedimentos internos de coleta e monetização de dados.

Neste sentido, várias disposições devem ser observadas pelos agentes de tratamento, em todo o processo da utilização dos dados pessoais, desde a coleta até a fase de monetização, como as hipóteses em que o tratamento de dados é legal, os princípios a serem seguidos em todos os procedimentos, bem como os direitos dos titulares dos dados (MODESTO, 2020).

Como já visto anteriormente, antes da monetização os dados passam pela fase de tratamento, fase na qual as empresas ou controladoras de dados extraem as informações pessoais do usuário, podendo usá-las para fins lucrativos.

No que concerne a hipóteses em que a lei autoriza o tratamento e a possível monetização de dados pessoais, o art. 7º da LGPD elenca hipóteses em que o tratamento de dados pode ser realizado, estas hipóteses, são todas de alguma forma relevantes para o tratamento de dados (COSTA, 2021, p.96), dentre elas, a mais importante está expressa no inciso I que preceitua que o tratamento de dados pode ocorrer “mediante o fornecimento de consentimento pelo titular”.

Existem também hipóteses que independem do consentimento do titular, no caso de situações específicas, como quando necessário ao cumprimento de obrigação legal ou à execução de políticas públicas (MODESTO, 2020).

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - Mediante o fornecimento de consentimento pelo titular;
> II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019).
> IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O consentimento é definido, conforme o artigo 5º, inciso XII, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. O art. 8º da LGPD dispõe que o consentimento deverá ser fornecido por escrito ou por outro meio capaz de demonstrar a manifestação de vontade do titular. (FERNANDES, 2020, p.33). Assim, o consentimento passou a ser instrumento da manifestação da vontade individual. “Se por um lado ele revela o aspecto da autodeterminação, já exposto ao longo deste trabalho, também passa a figurar como instrumento de legitimação” (DONEDA, 2006, p. 56)

Com isso, as autorizações genéricas dadas pelo titular para o tratamento de dados pessoais são consideradas nulas e cabe ao agente controlador dos dados o ônus da prova de que o consentimento do titular foi obtido conforme a Lei Geral de Proteção de Dados. A nulidade de autorizações genéricas, prevista no §4º, art.8º tem grande relevância para a eficácia do consentimento visto que pode configurar vício de vontade (DE FARIAS, 2020, p.52).

A nulidade também pode ser verificada nos casos em que as informações dadas pelo controlador de dados a seu titular tenham conteúdo enganoso ou não ocorrido de forma transparente, clara e inequívoca. (MODESTO, 2020). Quando se trata do tratamento de dados de crianças e adolescentes, este deve ser feito com consentimento específico e destacado de um de seus representantes legais.

> E, em se tratando do tratamento de dados pessoais de crianças e de adolescentes, este deverá ser realizado em seu melhor interesse, com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, bem como os controladores não deverão condicionar a participação desses indivíduos em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (art. 14). (MODESTO, 2020, p.9).

Em relação ao principal objeto de estudo deste trabalho, a lei dispõe que, em se tratando de dados pessoais sensíveis, conforme expresso no artigo 11 da Lei Geral de Proteção de dados, devem haver precauções especiais para esse tratamento, por se tratarem de dados sensíveis, podendo ele ocorrer somente “quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas” (LGPD, art.11, I, 2018). A Lei 13.709/2018 dedica um regime jurídico mais protetivo em relação a dados sensíveis, a fim de coibir práticas discriminatórias e assegurar que o titular dos dados pessoais sensíveis possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto (BIONI, 2019).

> Nesse sentido, as organizações que intencionem coletar dados pessoais devem se adequar a esse quadro normativo, embutindo em seus sistemas soluções que assegurem ao titular dos dados a possibilidade de manifestar inequivocamente seu consentimento de maneira livre e informada. Outrossim, aquele que desejar coletar dados pessoais deverá informar ao titular a forma, a duração e a finalidade do tratamento dos dados, além dos riscos a serem suportados pelo titular. Também, em caso de alteração na finalidade específica do tratamento dos dados, o titular deverá ser informado, com destaque de forma específica do teor das alterações, de modo que, nos casos em que o seu consentimento é exigido, poderá revogá-lo caso discorde da alteração (MODESTO, 2020, p.10).

Destarte, caso o titular não concorde com alterações ou queira revogar o consentimento dado anteriormente, a ele é garantido este direito, a qualquer tempo, através de uma manifestação expressa do titular e através de um procedimento gratuito e facilitado, conforme preceitua o artigo 7º, § 5º da Lei n° 13.709/2018.

> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. (LGPD, art.7, § 5º, 2018).

O artigo 7º da Lei Geral de Proteção de Dados apresenta mais nove hipóteses além do consentimento para o tratamento e consequentemente a possível monetização de dados, dos incisos II ao X. Neste sentido, a segunda hipótese para o tratamento de dados, expressa no artigo 7º, inciso II, seria para o cumprimento de obrigação legal ou regulatória pelo controlador.

> O cumprimento de obrigação legal ou regulatória pelo controlador é a segunda hipótese de tratamento, refere-se à obrigação oriunda de requisições judiciais (força de lei ou regulamento administrativo), nesse sentido, o agente de tratamento se vê obrigada a tratar os dados pessoais objeto da requisição. (FERNANDES, 2020, p.34).

O terceiro pressuposto para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (FERNANDES, 2020, p.34).

A quarta hipótese, por sua vez, seria para a realização de estudos por órgão de pesquisa, neste caso garantindo, se possível, a anonimização dos dados pessoais;

> A quarta hipótese é para a realização de estudos por órgãos de pesquisa. O art. 7º, IV da LGPD estabelece que os órgãos de pesquisa podem utilizar os dados para pesquisa, mas não estão exauridos de cumprir com os princípios da proteção de dados. Ressalta-se que as pessoas jurídicas de direito privado com fins lucrativos não podem valer-se desta hipótese de tratamento, tendo em vista a existência de previsão expressa em sentido contrário (FERNANDES, 2020, p.34).

A utilização de dados para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular dos dados, é a quinta hipótese. Por exemplo, no caso de um contrato de compra e venda realizado online, o controlador depende de diversos dados pessoais do consumidor como o endereço, documentos pessoais para a emissão de nota fiscal, etc (FERNANDES, 2020, p.34).

A sexta possibilidade apresentada no artigo sétimo para o tratamento de dados, é seu uso para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

A proteção da vida ou da incolumidade física é a sétima hipótese, com o intuito de proteger a vida do sujeito é permitido o tratamento dos seus dados para salvar-lhe. (FERNANDES, 2020, p.35)

A oitava hipótese é a tutela da saúde, no mesmo deslinde da proteção a vida, essa hipótese deverá ser utilizada em casos de risco urgente. (FERNANDES, 2020, p.35)

A nona possibilidade de tratamento diz respeito a necessidade de uso de dados para atender aos interesses legítimos do controlador ou de terceiros, com exceção aos casos que devem prevalecer os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

> O art. 10, do mesmo dispositivo, estabelece que o legítimo interesse do controlador somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, considerando as que seguem: (I) o apoio e a promoção de atividades do controlador; (II) a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviço que o beneficiem, respeitadas as legítimas expectativas dele, e os direitos e liberdades fundamentais. O legítimo interesse também é citado no art. 37 e dispõe que tanto o controlador quanto o operador devem manter os registros das operações de tratamento de dados pessoais que realizarem. O legítimo interesse possui um elevado grau de subjetividade, mas é de extrema importância para garantir a perpetuação do empreendedorismo e da inovação. A sua importância dar-se-á pelo fato da existência de bancos de dados extensos e gerais, estes poderiam tornar-se inutilizáveis com o advento da LGPD. Para preservar a inovação, o legislador criou a base legal do legítimo interesse, que permite o tratamento dos dados dos consumidores mesmo sem o seu expresso consentimento. (FERNANDES, 2020, p.35)

Por fim, a décima e última hipótese refere-se à proteção do crédito, inclusive quanto ao disposto na legislação pertinente. A doutrina diverge se a presente hipótese abrangeria somente o scoring de crédito ou o histórico negativo do titular, espera-se que a matéria seja elucidada pela Autoridade Nacional de Proteção de Dados (ANPD). (FERNANDES, 2020, p.35).

Portanto, as organizações que intencionem coletar dados pessoais de indivíduos devem adequar-se a essa normativa. Dessa forma, observa-se que as organizações não podem mais coletar dados pessoais sem informar ao titular quais dados estão sendo coletadas, ademais, elas devem previamente informar ao titular qual a finalidade para utilização dos dados (TEFFE; VIOLA, 2020).

Ademais, não basta apenas a manifestação inequívoca e informada pelo titular, a Lei Geral de Proteção de Dados também exige consentimento livre do titular, cabendo ao controlador o ônus da prova de que o consentimento foi obtido em

conformidade com o disposto na Lei, e a Autoridade Nacional de Proteção de Dados a avaliar a validade nos moldes da LGPD. (TEFFE; VIOLA, 2020).

O artigo 6º da Lei n° 13.709/2018 por sua vez, estabelece alguns princípios, os quais devem ser observados para que ocorra o tratamento de dados pessoais, além da boa fé.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Sendo assim, conforme Modesto (2020) os princípios da necessidade, da finalidade e da adequação do tratamento de dados, demostram uma mudança de comportamento significativa por parte de muitas organizações empresárias, visto que, estas só poderão coletar os dados pessoais estritamente necessários ao fim para o qual foram coletados, não podendo realizar procedimentos que visem uma finalidade diferente da informada ao titular dos dados em sua coleta.

Além disso, uma grande mudança que surge com a vigência da Lei geral de Proteção de dados é a observância do princípio da não discriminação (LGPD, art. 6º,

inciso IX), este artigo preceitua que dados pessoais não poderão ser monetizados de maneira abusiva ou que leve a fins discriminatórios ilícitos.

> Ademais, de acordo com o princípio da não discriminação, os dados pessoais não poderão ser monetizados de maneira abusiva ou que leve a fins discriminatórios ilícitos, como, por exemplo, a venda de um mesmo produto ou serviço, no mesmo dia e horário, por preços diferentes a duas pessoas distintas motivada apenas pela análise de informações pessoais (MODESTO, 2020, p. 48).

Modesto (2020) afirma que além da observação destes princípios, há também uma série de direitos dos titulares dos dados a serem observadas elencados do artigo 17 ao artigo 22 da Lei Geral de Proteção de Dados, a fim de que se realize o tratamento e a possível monetização de dados.

> Buscando assegurar a realização desses princípios, a Lei Geral de Proteção de Dados Pessoais garante, ainda, uma série de direitos ao titular dos dados pessoais, a saber, a confirmação da existência de tratamento; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; portabilidade dos dados a outro fornecedor de serviço ou produto; eliminação dos dados pessoais tratados com o consentimento do titular; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento; e revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. (MODESTO, 2020, p.48).

O inciso VI do artigo 6º da Lei n° 13.709/2018 estabelece que a transparência nas atividades de tratamento de dados pessoais deve ser garantida aos titulares, as informações devem ser claras, precisas e facilmente acessíveis (COSTA, 2021).

Desta forma, o titular de dados deve ser informado sobre quais seus direitos, como pode exercê-los em cada fase do tratamento, bem como tomar conhecimento que suas informações estão sendo monetizadas e para qual finalidade. (MODESTO, 2020).

Sobre isso, o artigo 7º, § 5º, da Lei geral de Proteção de Dados estabelece:

> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Logo, o compartilhamento dos dados para fins gratuitos ou oneroso que são objeto desse estudo, sofre restrição, devendo obter o consentimento do titular das informações para a cessão.

No que se refere a monetização de dados pessoais sensíveis, a Lei Geral de Proteção de Dados em seu artigo 11, § 3º, determina:

> § 3º A comunicação ou o uso compartilhado de dados pessoais 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.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência
> I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência
> II - As transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Isto posto, vejamos que a Autoridade Nacional de Proteção de Dados ANPD tem o dever de controlar a comunicação ou o uso compartilhado de dados pessoais sensíveis, podendo até mesmo coibir o uso de dados pessoais para fins econômicos. Todavia, tratando-se de dados pessoais sensíveis referentes à saúde, a Lei veda expressamente a comunicação ou o uso compartilhado entre controladores que objetivam usar desses dados para obter vantagem econômica. (MODESTO, 2020).

No entanto, o § 4º do artigo 11 enumera algumas possibilidades que os dados sensíveis relacionados a saúde podem ser compartilhados com objetivo de obter vantagem econômica, sendo eles hipóteses relativas a prestação de serviços de saúde; de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º que veda operadoras de planos privados de assistência à saúde tratar dados sensíveis relacionados a saúde a fim de prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

De acordo com o artigo 16 da Lei n° 13.709/2018, o agente de tratamento não poderá manter os dados pessoais em sua base para fins de monetização após terminar o tratamento de dados.

Angela Kung e Nicole Aun (2021) estabelecem que, o término e consequentemente eliminação de dados pessoais decorrerá necessariamente da

ausência dos princípios da finalidade, necessidade, adequação do tratamento, exercício do direito do titular, ou ilicitude do tratamento reconhecida pena ANPD. (KUNG e AUN, 2021).

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - Cumprimento de obrigação legal ou regulatória pelo controlador;
> II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Os dados só poderão ser mantidos se forem anonimizados. Por tanto, a anonimização torna-se uma ferramenta de suma importância para que as organizações empresárias concretizem seus modelos de negócio (MODESTO, 2020, p.51), posto que, essa situação seria mais protetiva para os titulares, uma vez que o dado anonimizado não permite a identificação do titular, ou seja, uma vez anonimizado, o dado deixa de ser pessoal, conforme o art. 12 da LGPD. (BIONI, 2020).

Constata-se que a Lei Geral de Proteção de Dados trouxe consigo significativas mudanças, as organizações empresárias que monetizam dados pessoais devem se adequar a essa nova lei, ou correrão riscos de sofrer sanções administrativas, além de estarem sujeitas à responsabilidade civil.

5 DA MONETIZAÇÃO DE DADOS SENSÍVEIS POR FARMÁCIAS

De acordo com a Lei Geral de Proteção de Dados, os dados pessoais sensíveis são todos aqueles relacionados a uma “pessoa física identificada ou identificável”. A Lei 13.709/2018 define os dados sensíveis em seu artigo 5º, inciso II como:

> 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;

Como já visto anteriormente, os dados sensíveis são "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação" (BIONI, 2018, p. 84).

Ante a esse tipo de dados, que expressa características sobre a personalidade dos indivíduos, surge a preocupação da não exposição desses dados, visto que, sua exposição pode gerar descriminação de seu titular.

Bioni (2018) demonstra que, é possível identificar individualidades sensíveis dos titulares dos dados, até mesmo com informações triviais.

> Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado “trivial” pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional. (BIONI, 2018, p. 119).

Segundo Bioni, o mesmo pode suceder com outros “registros digitais”, tais como o histórico de navegação, os termos de pesquisa ou mesmo as compras realizadas por um consumidor. (BIONI, 2018, p.119).

O tratamento de dados, como já citado, é permitido no Brasil com algumas regras específicas para os dados sensíveis, dentre eles, os dados da saúde. Existe por exemplo uma proibição específica expressando que os dados da saúde não podem ser compartilhados entre controladores de dados para a obtenção de vantagem econômica para o fornecedor de produtos ou prestador de serviços, o que gera um conflito, vez que, este meio sempre foi rodeado de interesses lucrativos e econômicos.

> Importante destacar que a saúde é um dos setores que mais tratam dados sensíveis pela LGPD, que, desse modo, vem regular normas em um setor complexo, permeado por interesses lucrativos e econômicos (BOAS; SILVA; ROSA e AVOGLIA, 2020, p. 282).

Assim como o tratamento de dados geral, expresso na Lei n° 13.709/2018 no artigo 7º e seguintes, o tratamento de dados pessoais sensíveis explicitado no artigo 11 da mesma lei repete várias disposições sobre o tratamento, como o consentimento do titular, além das hipóteses já expostas, em que o consentimento é dispensado. (KONDER, 2019).

Conforme já apresentado, no artigo 11, § 3º da Lei n° 13.709/2018 a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo econômico pode ser vedado ou sofrer regulamentação por parte da autoridade nacional. Isso significa que as limitações taxativas da Lei não excluem a possibilidade de surgirem novas limitações. (KONDER, 2019).

No que se refere ao tratamento de dados sensíveis, principalmente os que envolvem informações sobre a saúde, para finalidade econômica, essa é uma das áreas mais delicados para Campos (2020, p.100), tendo em vista a tensão existente entre a importância do uso das informações para otimizar processos de produção e reduzir os custos e a redução de benefícios dos consumidores, vez que, a coleta de dados pode gerar uma precificação seletiva na área da saúde.

> Encontrar a dosagem adequada entre o uso de dados e o respeito a eles é certamente um dos desafios enfrentados na implementação de um programa de governança de dados, garantindo o cumprimento com a LGPD e a proteção de dados pessoais. (RICCO e CRESPO, 2021, p. 203). Embora desafiador, o esforço diário em conciliar esses aspectos é extremamente importante para propiciar oportunidade de benefícios, melhoria de tratamentos e qualidade de vida de pacientes e consumidores, mas, ao mesmo tempo, respeito à tutela dos detentores de seus dados, principalmente dados sensíveis de pessoas. (RICCO e CRESPO, 2021, p. 204).

Referente a monetização de dados pessoais sensíveis, a Lei Geral de Proteção de Dados em seu artigo 11, § 3º, estabelece:

> § 3º A comunicação ou o uso compartilhado de dados pessoais 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.

Vejamos que a Autoridade Nacional de Proteção de Dados (ANPD) tem o dever de controlar a comunicação ou o uso compartilhado de dados pessoais sensíveis, podendo até mesmo coibir o uso de dados pessoais para fins econômicos.

Quanto a monetização de dados sensíveis referentes a saúde, esta é vedada, exceto se o compartilhamento dos dados for consentido pelo titular ou quando necessária para prestação de serviço de saúde suplementar, conforme expressa o artigo 11, § 4º da Lei Geral de Proteção de Dados.

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

Ademais, o tratamento desse tipo de dado, conforme o artigo 13 da Lei nº 13.709/2018 é permitido para estudos em saúde pública, entretanto, não é permitida a transferência desses dados a terceiros, eles são tratados exclusivamente dentro do órgão e sempre que possível, esses dados devem ser anonimizados.

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

No tocante as Farmácias e Drogarias, estas possuem uma política de coletar dados que nunca se atentou muito para os limites da privacidade e proteção de dados dos titulares, vez que, a maioria mantém seu banco de dados cadastros com todos os medicamentos e produtos que seus clientes utilizam e, ainda, com que frequência consomem os medicamentos e produtos. (PERROTI, 2018).

> Ressalta-se que o consumidor, objeto de análise dos algoritmos com base em seus dados pessoais, poderá ter todas as suas doenças, infecções, DST's, psicoses, insônias, manias e hipocondrias expostas, correndo o risco do uso desses dados para efeitos de discriminação, planos de saúde ou análise de créditos.

> É evidente que boa parte dos dados coletados dos consumidores de Farmácias e Drogarias são de conteúdo sigiloso, uma vez que esses dados expõem fatos íntimos dos clientes e, por tais razões, são considerados pela regulamentação como dados sensíveis. (PERROTTI, 2018, p.1).

Pelo fato de coletar vários dados pessoais inclusive dados pessoais sensíveis (relacionados à saúde), seja para formação de cadastro, aquisição de descontos ou mesmo para que o indivíduo obtenha certo medicamento, como nos casos em que as farmácias retêm receitas dos clientes. O ramo farmacêutico acaba chamando a atenção dos consumidores com relação à proteção de dados oferecida pela nova lei (MARCONDES, 2021).

> Existem casos em que a farmácia é obrigada a coletar dados pessoais dos seus clientes, conforme determinado pela Portaria 344 de 1998 da ANVISA. Por exemplo, no caso da compra de medicamentos que possuam como base substâncias entorpecentes, psicotrópicas, retinóicas para uso sistêmico e imunossupressores. Estes somente podem ser comercializados mediante o fornecimento de nome, número do documento de identificação, endereço completo e telefone do comprador, obrigando as farmácias a coletar essas informações dos seus clientes. (MARCONDES, 2021, p.1)

Quando se trata de outros tipos de produtos, como por exemplo, cosméticos, é comum que as farmácias solicitem e armazenem dados pessoais bem como o histórico de compras, afim de traçar perfis de preferências de seus clientes, podendo oferecer descontos e ofertas personalizadas a eles. Ademais, esses dados podem ser usados também com o propósito de direcionar campanhas de Marketing a cada titular, conforme seus gostos pessoais. Nessa situação, a obtenção do consentimento do consumidor é obrigatória, e o titular dos dados deve estar ciente da finalidade da coleta de seus dados (MARCONDES, 2021).

Nos casos em que a lei (Portaria 344/1998) permite a retenção de receita médica pelas farmácias para vender determinados medicamentos, as informações contidas podem ser tão reveladoras quanto um prontuário médico, por isso seu conteúdo deve ser mantido sob sigilo, exigindo das farmácias maior atenção, pois expostos estes dados, serão divulgados fatos íntimos do titular (LEITE, 2020).

> Embora haja hipótese legal para o tratamento os dados pessoais supracitados, seja mediante o fornecimento de consentimento pelo titular ou para o cumprimento de obrigação legal ou regulatória pelo controlador, ou ainda outros embasamentos legais, percebe-se que o cuidado deve ser redobrado, uma vez que a área farmacêutica lida diariamente com dados confidenciais dos pacientes (LEITE, 2020, p.1).

Recentemente, algumas farmácias foram denunciadas e multadas pela falta de transparência para com seus consumidores. Em Mato Grosso, o PROCOM Estadual aplicou multa de 572. 680, 71 a Rede de Farmácia Droga Raia após comprovada a coleta de dados pessoais sensíveis dos consumidores e a autorização do tratamento desses dados sem a devida explicação e informação de quem teria acesso a esses dados.

No mesmo sentido, em 2018 uma reportagem da globo.com expunha a investigação feita pelo MP sobre a coleta de CPF por algumas redes de farmácias para obtenção de desconto para os clientes. A suspeita do Ministério Público era que os dados sensíveis dos clientes eram repassados para empresas de plano de saúde e de análise de crédito, sendo feito um mercado paralelo.

A monetização dos dados pessoais sensíveis pelas farmácias, como já visto, apesar de exigir precauções especiais, por se tratar de dados sensíveis, não é ilícita.

> Aliás, existe a probabilidade desses dados serem comercializados e compartilhados com empresas interessadas no acesso a essas informações, podendo gerar impacto no custo de planos de saúde, e até mesmo na fixação de juros em contratos de financiamento, em razão dos riscos representados pela condição de saúde à capacidade do financiado para honrar seus pagamentos. (PERROTTI, 2018, p.1).

Entretanto, deve efetivar o que está assentado no art. 11, inciso I da Lei 13.709/2018, ou seja, é permitida desde que haja consentimento do titular ou responsável legal dos dados e definição clara, específica, adequada e necessária da finalidade da coleta e tratamento desses dados.

> Os cadastros registrados nos sistemas das farmácias, com o intuito de oferecer descontos e promoções para os clientes, devem observar os princípios da finalidade, da adequação (tratamento compatível com a finalidade) e da necessidade. Neste caso, deve haver sempre o consentimento do titular (de forma livre e expressa) para elaboração de um cadastro, caso contrário, a exigência de tais dados será abusiva aos olhos da LGPD. (LEITE, 2020, p.1).

Além disso, a pedido do titular ou de seu representante legal (quando menor), os dados devem ser eliminados ou anonimizados, de modo que não o identifiquem, exceto se for legalmente permitido ou obrigatório serem mantidos armazenados pela farmácia para cumprir com suas obrigações legais de acordo com as definições da Lei Geral de Proteção de Dados Pessoais

Caso as farmácias não se adequem a Lei Geral de Proteção de Dados quanto a observância do ordenamento nos processos de coleta, tratamento, armazenamento, compartilhamento de dados pessoais, sobretudo, os dados pessoais sensíveis objeto desse estudo, a ANPD tem competência para determinar a adoção de medidas, inclusive sancionatórias para a empresa farmacêutica. (PERROTI, 2018).

Para mais, a Lei Geral de Proteção de Dados também prevê o dever de reparação dos danos causados aos titulares de dados.

Segundo Meinberg (2018), no capitalismo não existe obsessão de graça, as farmácias demostram uma verdadeira obsessão para a coleta de dados pessoais sensíveis e isso demonstra um interesse por trás.

Dado exposto, se por um lado, observamos positivamente o avanço da tecnologia e como a coleta, tratamento e monetização de dados contribuiu para a melhoria e maior eficiência de medicamentos, tratamentos, qualidade de vida de pacientes e consumidores, lado outro, a coleta de dados pode gerar a exposição negativa de informações sensíveis aumentando o risco de vulnerabilidade dos titulares desses dados.

Adequar-se às normas de proteção de dados não é uma tarefa fácil para o ramo farmacêutico. A LGPD não impede nenhuma empresa de realizar o tratamento de dados dos consumidores, mas estabelece que a coleta seja precedida de transparência, para que o cliente saiba com quem seus dados são compartilhados e o que, de fato, é feito com eles.

A Lei Geral de Proteção de Dados Pessoais trouxe importantes diretrizes a serem seguidas pelas organizações que resolvam monetizar esses dados, e sem dúvidas, as mudanças que surgiram podem gerar algumas dificuldades de adaptação para os entes que realizam esse tipo de atividade. (MODESTO, 2020).

Jéssica Modesto (2020) entende que uma alternativa que pode ser tomada pelos agentes que tratam e monetizam os dados é utilizar da técnica de anonimização dos mesmos, posto que, com isso haveria o impedimento de identificação dos indivíduos. De tal modo, essas técnicas retiram o vínculo entre o dado e o seu titular (DONEDA, 2019, p. 140).

Os dados anonimizados são aqueles dados que não possuem um meio de identificação, conforme estabelecido pelo inciso III, do artigo 5° da Lei 13.709/18. É aquele dado incapaz de revelar a identidade de uma pessoa. Diante do próprio

significado do termo, anônimo seria aquele que não tem nome nem rosto (HOUAISS; VILLAR, 2009, p. 140).

O artigo 12 da Lei Geral de Proteção de Dados estabelece:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Logo, anonimizar os dados significaria afastar a incidência da LGPD, dado que, o fornecimento do consentimento do titular ou a caracterização do interesse legítimo deixaria de ser necessário à realização do tratamento de dados. Entretanto, com os dados anônimos, nem todos os procedimentos de monetização podem ser realizados, sendo assim, o agente de tratamento deverá observar todas as disposições previstas na Lei 13.709/18. (MODESTO, 2020).

6 CONSIDERAÇÕES FINAIS

Ao longo da história, a sociedade organizou-se de diferentes formas. A sociedade tinha inicialmente como cerne econômico a agricultura, após a revolução industrial houve a consolidação do capitalismo e com isso uma grande expansão tecnológica, sobretudo, de tecnologias digitais.

Com a grande expansão das tecnologias digitais e o surgimento da internet houve um grande processo de digitalização e, com o crescimento exponencial da tecnologia da informação o fluxo imenso de dados pessoais passou a ser visto como um produto.

As empresas que detinham dados de titulares passaram a compartilhar e comercializar dados pessoais a fim de facilitar a oferta de produtos. Por tanto, com essa nova moeda de troca, os dados, surge uma nova ordem econômica denominada Capitalismo da Vigilância.

O capitalismo de vigilância nada mais é que a utilização que empresas fazem de dados pessoais fornecidos a ela, transformando os mesmos em matéria prima e lucro.

Os dados se subdividem em dados pessoais, dados pessoais sensíveis e dados anonimizados. Os dados pessoais então expressos na Lei 13.709/2018, em seu artigo 5º trata-se de informações relacionadas a pessoa natural, seja identificada ou identificável. O dado pessoal sensível, por sua vez, está expresso no art. 5º II, da Lei 13.709/2018, trata-se de informações relacionadas a religião, política, etnia, saúde, dado genético ou biométrico que permitem a identificação de uma pessoa natural e por fim, os dados anônimos, conforme exposto no artigo 5º III, da referida Lei, são aqueles dados referentes a uma pessoa, porém incapazes de identifica-la.

Os dados reunidos em grande volume, variedade e velocidade são definidos como *Big Data* e para que haja a valorização destes eles devem passar pelo processo de tratamento onde a grande quantidade de informações é reunida e em seguida processada para que haja uma “lapidação” e a abundância de informações coletadas se tornem úteis para as empresas.

Após isso, pode ocorrer a monetização destas informações, que é o processo pelo qual os dados tornam-se mercadorias altamente rentáveis para as empresas.

Posto isso, com a entrada em vigor da Lei 13.709/201 algumas mudanças ocorreram, no que se refere ao tratamento e monetização de dados pessoais, uma vez que, ela impõe a necessidade de revisões de processos e procedimentos internos.

Antes da entrada em vigor da Lei Geral de Proteção de Dados, haviam códigos de conduta, políticas internas e algumas legislações específicas que regulamentavam a coleta e monetização dos dados pessoais, entretanto, fazia-se necessária uma legislação específica a fim de fortificar e regulamentar o uso de dados pessoais, a fim de proteger e garantir a segurança dos seus titulares.

Após a entrada em vigor da Lei nº 13.709/2018, algumas mudanças ocorreram, sobretudo na coleta de dados sensíveis pelas farmácias, objeto deste estudo.

O tratamento e a monetização de dados pelo ramo farmacêutico passaram a exigir precauções especiais das organizações por se tratarem de dados sensíveis, além disso, a coleta desses dados identificáveis passa a ser realizada apenas com o consentimento do titular, conforme preceitua o art. 11 da Lei nº 13.709/2018 com a devida orientação sobre as finalidades do uso dos dados.

Essas mudanças tem o objetivo de trazer mais segurança no uso e armazenamento de dados, afinal, todos esperam que seus dados sejam tratados com responsabilidade e segurança sem prejudicar a privacidade, devendo o indivíduo saber para quem seus dados estão sendo encaminhados e qual o tratamento será dado para cada informação.

Diante disso, observa-se que a coleta, tratamento e monetização de dados nos moldes atuais da Lei Geral de Proteção de Dados contribuiu para a melhoria e maior eficiência de medicamentos, tratamentos, qualidade de vida para os consumidores, entretanto, a coleta de dados deve ser feita de forma que não gere a exposição negativa de informações sensíveis dos titulares.

REFERÊNCIAS

ADJEI, Joseph K. **Monetização de Pessoal Identidade em formação: Tecnológica e Regulatório Estrutura.** IEEE Computador Sociedade Washington, Washington DC / EUA, 14 dez. 2015.

ALVES, Lorena Rodrigues. **Capitalismo de vigilância: um estudo sobre a reprodução de conhecimentos estereotipados pelos algoritmos**. 2020.

BATISTA Morellato, Ana Carolina, e André Filipe Pereira Reid dos Santos. **"A Capitalismo De vigilância E a Lei Geral De proteção De Dados: Anonimização E Consentimento"**. *Revista Brasileira de Sociologia do Direito* 8, no. 2. (4 maio 2021): p. 184-211.

BEZERRA, André Luís; WEBERBAUER, Paul Hugo (Orient**.). A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade.** 2019. 42 f. TCC (graduação em Direito) - Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019

VIGNOLI, Richele; VECHIATO, Fernando. **Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação**. 2019.

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

CARVALHO, Mariana Amaral. **Capitalismo de vigilância: a privacidade na sociedade da informação.** 2019. 102 f. Dissertação (Mestrado em Direito) - Universidade Federal de Sergipe, São Cristóvão, SE, 2019.

CHAVES, Luiz Fernando Prado; VIDIGAL, Paulo. **A LGPD revogou tacitamente dispositivos do Marco Civil da Internet.** Revista **Consultor Jurídico**, 29 de março de 2021. Disponível em: <https://www.conjur.com.br/2021-mar-29/chaves-vidigal-lgpd-revogou-tacitamente-dispositivos-mci>. Acesso em: 17 nov. 2021.

COSTA, José Augusto Fontoura. **Tratamento e transparência de dados de saúde: Limites ao compartilhamento de dados sensíveis**. LGPD na Saúde [livro eletrônico] / coordenação Analluza Bolivar Dallari, Gustavo Ferraz de Campos Monaco.1.ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade.** TEPEDINO, Gustavo (Coord.). Problemas de direito constitucional. Rio de Janeiro: Renovar, 2000.

DONEDA, D. (2011). **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], 12(2), 91–108.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

FARIAS, Thalyta Soares de. **Privacidade, monetização de dados pessoais e a LGPD: desafio e impactos da Lei Nº 13.709/2018**. 2020. Monografia (Bacharelado em Direito) - Faculdade de Ciência Jurídicas e Sociais, Centro Universitário Brasília, Brasília, 2020.

FERNANDES, Pabline Santos. **O direito do consumidor e o mercado digital: uma análise sobre o tráfego digital dos dados dos consumidores frente à legislação brasileira.** 2020. 51 f. Monografia (Graduação em Direito) - Escola de Direito, Turismo e Museologia, Universidade Federal de Ouro Preto, Ouro Preto, 2020.

FRAZÃO, Ana. **Big data e concorrência Principais impactos sobre a análise concorrencial.** 2017. Acesso em: 20 out. 2021.

GOMES, Rodrigo Dias de Pinho. **Big data, desafios à tutela da pessoa humana na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2017.

HOUAISS, Antônio; VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Objetiva, 2009.

NEGRISOLI, Lucas. **Farmácias que pedem CPF podem estar repassando dados de clientes, diz MP.** Estado de Minas, 2018. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/08/17/internas_economia,980868/farmacias-que-pedem-cpf-podem-estar-repassando-dados-de-clientes-mp.shtml>. Acesso em: 22 nov. 2021.

LUÍS, Gabriel. **CPF em troca de desconto: MP investiga venda de dados de clientes por farmácias.** G1 Distrito Federal, 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml>. Acesso em: 15 nov. 2021.

KONDER, Carlos Nelson de Paula; SOUZA, Amanda Guimarães Cordeiro de. **Onerosidade do acesso às redes sociais**. Revista de Direito do Consumidor, vol. 121/2019, p. 185-212, jan – fev. 2019, DTR/2019/26061.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18).** Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019.

KUNG, Angela Fan Chi; AUN Nicole Recchi. **Conservação, anonimização e eliminação de dados na área da saúde: obrigação legal e regulatória, viabilidade técnica e observância da LGPD.** LGPD na Saúde [livro eletrônico]/ coordenação Analluza Bolivar Dallari, Gustavo Ferraz de Campos Monaco.1.ed. São Paulo: Thomson Reuters Brasil, 2021. Acesso em: 28 nov. 2021.

LANEY, D. **3D data management: Controlling data volume, velocity and variety.** META Group Research Note. V.6. n. February 2001.

LEITE, Fernanda. **Lei Geral de Proteção de Dados Pessoais na área farmacêutica.** Blog LGPD, out 2020. Disponível em: <https://www.bloglgpd.com.br/post/lei-geral-de-prote%C3%A7%C3%A3o-de-dados-pessoais-na-%C3%A1rea-farmac%C3%AAutica>. Acesso em: 18 nov. 2021.

LUGATI, L. N.; ALMEIDA, J. E. de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito, *[S. l.]*, v. 12, n. 02, p. 01-33, 2020. DOI: 10.32361/2020120210597. Acesso em: 19 nov. 2021.

MACHADO, Diego; DONEDA, Danilo. **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudoanonimização de dados.** Revista dos Tribunais. vol.998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016.** Trabalho de Conclusão de Curso (graduação) – Universidade de Brasília, Faculdade de Direito, 2017.

MARCONDES, Lucélia Bastos Gonçalves. **LGPD nas farmácias: adequação do setor às novas normas deve seguir algumas particularidades**. Migalhas, ago. 2021. Disponível em: <https://www.migalhas.com.br/depeso/350527/lgpd-nas-farmacias-adequacao-do-setor-as-novas-normas>. Acesso em: 30 nov. 2021.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. **A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

MODESTO, Andrade Jéssica. **Breves considerações acerca da monetização de dados pessoais na economia informacional à luz da lei geral de proteção de dados pessoais**. Rev. de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Evento Virtual | v. 6 | n. 1 | p. 37-58 | Jan/jun. 2020. Acesso em: 5 dez. 2021.

MULHOLLAND, Caitlin**. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais.** 2020. Este texto, com algumas alterações, foi originalmente publicado na Revista da AASP, número 144, novembro de 2019, pp. 47-53. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-devulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 20 out. 2021.

PERROTTI, Paulo. **A LGPD e o ramo farmacêutico.** LGPD Solution, 2021. Disponível em: <https://lgpdsolution.com.br/a-lgpd-e-o-ramo-farmaceutico>. Acesso em: 29 nov. 2021.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD.** São Paulo: Saraiva Educação, 2020.

ROSA, Helena Rinaldi; SILVA Marilene Alves da; BÔAS, Eliéte Ferreira Villas; AVOGLIA, Hilda Rosa Capelão.**Bancos de dados de saúde e pesquisa: prós e contras da LGPD.** LGPD na Saúde [livro eletrônico]/ coordenação Analluza Bolivar Dallari, Gustavo Ferraz de Campos Monaco.1.ed. São Paulo: Thomson Reuters Brasil, 2020. Acesso em: 03 dez. 2021.

SANTOS, Luiza Mendonça da Silva Belo. **O direito da concorrência na economia movida a dados: uma análise dos impactos do Big Data no controle de estruturas do setor digital**. 2019. 69 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) —Universidade de Brasília, Brasília, 2019.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados como direito fundamental e a incivilidade do uso de cookies.** 2018. 65f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2018.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed.São Paulo: Atlas, 2014

TAURION, Cezar. **Big Data**. Rio de Janeiro: Brasport, 2013.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. civilistica.com**, v. 9, n. 1, p. 1-38, 9 maio 2020.

VIGNOLI, Richele; VECHIATO, Fernando. **Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação Dados relativos no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação**. 2019.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância a luta por um futuro humano na nova fronteira do poder.**1 ed. 2021.