

Rian Pablo dos Santos

Fatec - Faculdade de Tecnologia de Assis

riano.opablo@gmail.com

Claudio Fazano Guazeli Junior

Fatec - Faculdade de Tecnologia de Assis

guazeli@gmail.com

RESUMO

Com a Quarta Revolução Industrial e a expansão da Internet das Coisas (IoT), a coleta e o uso de dados em sistemas e bancos de dados tornaram-se cada vez mais frequentes. Nesse contexto, surgiram novas práticas comerciais, como a venda de dados para gerar insights e orientar produtos e serviços. Diante da intensificação e invasividade dessa comercialização, muitas vezes realizada sem o consentimento dos titulares, torna-se essencial discutir a privacidade e a proteção de dados pessoais. Fundamentado na LGPD, este estudo, por meio de análise bibliográfica comparativa, examina a crescente e opaca comercialização de dados e sua relação com os princípios de transparência, finalidade e autodeterminação informativa.

Palavras-chave: LGPD. Dados pessoais. Comércio de dados. Privacidade.

ABSTRACT

With the Fourth Industrial Revolution and the expansion of the Internet of Things (IoT), the collection and use of data in systems and databases have become increasingly frequent. In this context, new commercial practices have emerged, such as the sale of data to generate insights and guide products and services. Given the intensification and invasiveness of this commercialization, often carried out without the consent of the data subjects, it becomes essential to discuss privacy and the protection of personal data. Based on the LGPD (Brazilian General Data Protection Law), this study, through comparative bibliographic analysis, examines the growing and opaque commercialization of data and its relationship with the principles of transparency, purpose, and informational self-determination.

Keywords: LGPD. Personal data. Data trading. Privacy.

1 INTRODUÇÃO

Com o advento da era da informação, a geração de dados tem sido crescente e exponencial. Esses dados, quando não tratados a primo momento, podem não indicar uma informação precisa ou direta de fácil entendimento, mas quando tratadas por organizações que utilizam destes dados para obtenção de lucros, podem gerar informações valiosas que outras empresas podem utilizar para direcionamento de propagandas ou propostas de vendas. Estas informações geradas após tratamento podem indicar comportamentos, hábitos e rotinas, informações íntimas e valiosas, o que indica um problema de violação de privacidade e também uma falha na garantia da integridade digital de todo usuário da Internet.

Este trabalho tem por objetivo averiguar sobre o aspecto das leis orientadas pela LGPD sobre comercialização de dados pessoais, desde os momentos de coleta, tratamento e venda e qual a base jurídica que as organizações deste ramo devem ser submetidas, assim como os direitos que os proprietários dos dados possuem.

A importância da abordagem deste tema dá-se pelo crescente envolvimento da humanidade com os meios digitais e a constante integração do social ao virtual, o que faz com que depositemos grandes quantidades de informações na internet sem indagar sobre como estes dados serão protegidos ou como serão tratados e quais as bases legais destas ações.

A base desta presente pesquisa será realizada através de uma análise sucinta das leis da LGPD e de bibliografias que abordam sobre os dados pessoais nos aspectos jurídicos e comerciais, junto da análise e pesquisas sobre empresas que realizam as atividades de coleta, tratamento e venda de informações e qual amparo jurídico que elas possuem.

2 REVISÃO DE LITERATURA

2.1 Definição de dados e classificação

Segundo a Lei nº 13.709/2018 (BRASIL LGDP, 2018, art. 5º, inc. I e II), considera-se dado pessoal “informação relacionada a pessoa natural identificada ou identificável” e dado pessoal sensível aquele “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato [...]”.

Estes dados são identificadores que podem em um primeiro momento não parecerem importante para uma visão desatenta, mas com o devido tratamento após a coleta por meio de registros e cadastros em lojas, comércios ou sites, eles se tornam ativos valiosos que transmitem informações precisas sobre aspectos de consumo, atividade cotidiana e crenças que são vistos como oportunidades de geração de lucros.

Nosso hábito de uso da internet, que tipos de sites visitamos, quanto tempo passamos em cada um deles, quais as nossas preferências quando compramos algo on-line e até mesmo a nossa localização geoespacial são também exemplos de dados e informações que geramos diariamente. Alguns dos serviços utilizados por usuários da web, oferecidos por empresas como Google, Facebook, Twitter, WhatsApp, entre inúmeras outras, utilizam em proveito próprio os mais variados dados e informações deste "rastro digital" que deixamos no ciberespaço, monetizando-os— pelo tratamento, cruzamento e análise deles ou na construção de modelos de negócio neles baseados, gerando retornos financeiros consideráveis. (BARROS, 2018, p75)

Verifica-se, assim, que os dados pessoais, mais do que elementos de identificação, são reconfigurados como commodities digitais e inseridos em ecossistemas analíticos que os traduzem em oportunidades de monetização e em insumos informacionais para estratégias de geração de lucro.

2.2 O mercado de dados pessoais e seus impactos

Conforme visualizado por Gianclaudio Malgieri e Bart Custers (2018), os dados pessoais são fundamentais para diversos modelos de negócios na economia digital. Entre os modelos são descritos os que estão à venda direta de dados pessoais, em que empresas ou intermediários comercializam informações como listas de contatos e dados demográficos, a publicidade baseada em dados, que utiliza perfis detalhados de consumidores para segmentar anúncios personalizados, como fazem plataformas como *Google* e *Facebook*, modelos de assinatura e licenciamento em que empresas oferecem acesso contínuo a dados por meio de assinaturas e a monetização indireta, em que os dados são usados para aprimorar produtos e serviços, como recomendações em plataformas de *streaming*.

Além disso, destacam-se os mercados de dados pessoais, onde indivíduos podem vender diretamente suas informações, e o uso de dados em pesquisas e desenvolvimento, especialmente em setores como saúde e inovação tecnológica.

Ao passo que vamos nos digitalizando e acompanhando os desenvolvimentos tecnológicos em busca de praticidade, nos vemos fazendo cadastro em diversos *sites* aceitando seus *cookies* e fazendo registros simples para acessarmos serviços “gratuitos”, tanto para realizarmos tarefas cotidianas, acadêmicas ou profissionais, tendo um crescente aumento da aquisição de dados, como visto em um estudo feito pela ABES (Associação Brasileira De Empresas De Software). “Em 2024, o universo de dados no mundo ultrapassará 157 *ZetaBytes*, ou 157 trilhões de *Gigabytes*, podendo dobrar até 2027. Quase 25% desse volume já está na nuvem, que cresce com o dobro da velocidade em relação ao que não está em *Cloud*.” (ABES, 2024).

Como visto pela ABES (2024), as soluções de dados na nuvem, que fazem parte do

modelo PaaS, devem atingir um valor de US\$ 1,5 bilhão no Brasil em 2024, refletindo um crescimento acelerado. Além disso, esse avanço impulsionará o mercado de serviços de TI, que deverá consumir aproximadamente US\$ 1,4 bilhão em 2024 com consultoria, integração e suporte de projetos relacionados a dados.

A coleta e o manuseamento de grandes volumes de dados pessoais desafiam alguns dos princípios fundamentais da privacidade: autodeterminação informativa, minimização dos dados, consentimento e direito de acesso aos dados pelo próprio. Por outro lado, devido à globalização da economia e ao facto de muitas empresas estarem estabelecidas em outros países, como os Estados Unidos e, por isso, não estarem sujeitas às regras da União Europeia e às obrigações legais de proteção de dados, assiste-se à coleta e utilização de grandes volumes de informação em violação da privacidade das pessoas. (ESTRADA, 2016, p87)

Visto o crescente aumento na criação e concentração de dados e observado que surge uma preocupação com a transparência, legitimidade e vigilância sobre o tratamento e comercialização de informações pessoais, frente à utilização massiva de dados (pessoais e não pessoais) que o paradigma arquitetônico "big data" materializa, preocupações sobre legitimidade para tratamento de dados, vigilância e transparência aos titulares ganham importância como contrapartida à renderização de comportamentos por softwares de grandes empresas (Lage, 2024, p. 3).

2.3 Princípios da LGPD aplicáveis a comercialização de dados

Observando as movimentações econômicas que esta fatia do mercado de TI possui junto com o crescimento da geração de dados, surge um novo modelo de mercado aplicado na era digital da humanidade chamado de "Capitalismo de Vigilância", uma nova ordem econômica que reivindica a experiência humana como uma matéria-prima gratuita, utilizada em práticas comerciais dissimuladas de extração, previsão e vendas (ZUBOFF, 2021).

A LGPD não possui artigos que agem diretamente no tema de comércio de dados e informações, mas possui leis que se destacam garantido transparência, privacidade e controle aos titulares dos dados. Segundo a LGPD, o tratamento de dados pessoais deve ter finalidades legítimas, específicas, explícitas e informadas ao titular, garantindo que não haja tratamento posterior que seja incompatível com essas finalidades (BRASIL, 2024).

O titular dos dados pode ter conhecimento sobre eles, forma de tratamento e bloqueio, conforme descrito no artigo 18:

"O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - Confirmação da existência de tratamento;
- II - Acesso aos dados;
- III - Correção de dados incompletos, inexatos ou desatualizados;
- IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.” (BRASIL, 2018).

A LGPD também aborda sobre o tratamento dos dados sensíveis, que também é utilizada para extração de informações importantes que podem ser utilizadas para direcionamento de propagandas, serviços ou produtos. No caso o artigo 11 refere-se ao tratamento desses dados pessoais sensíveis sem o consentimento do titular. Segundo a lei, esse tratamento pode ocorrer em algumas situações específicas, entre elas, destacam-se o cumprimento de obrigação legal ou regulatória, a realização de estudos por órgãos de pesquisa com a garantia de anonimização e a necessidade de execução de contrato em que o titular seja parte. Além disso, o tratamento pode ser justificado para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, bem como para a proteção da vida ou da incolumidade física do titular ou de terceiros.

A LGPD também menciona que o tratamento pode ocorrer para a tutela da saúde, exclusivamente em procedimentos realizados por profissionais ou serviços de saúde, e quando necessário para atender aos interesses legítimos do controlador ou de terceiros, desde que não prevaleçam os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Um ato de poder do titular da informação e o consentimento do mesmo sobre a disponibilização dos dados, transcritos no artigo 8 da LGPD, que estabelece que o tratamento de dados pessoais baseado no consentimento do titular, deve ser realizado de forma livre, informada e inequívoca. Além disso, o controlador é responsável por manter um registro do consentimento, incluindo a data da manifestação. O titular tem o direito de revogar o consentimento a qualquer momento, e essa revogação deve ser facilitada pelo controlador.

Também é necessária uma série de medidas protetivas, como visto no artigo 46, que determina que tanto o controlador quanto o operador devem implementar medidas de segurança, tanto técnicas quanto administrativas, para proteger os dados pessoais contra acessos não autorizados e situações de destruição, perda, alteração, comunicação ou difusão. As medidas de segurança devem ser revisadas e atualizadas periodicamente, e o controlador deve comunicar à autoridade nacional e ao titular sobre qualquer incidente de segurança que possa causar risco ou dano relevante aos titulares.

De acordo com a LGPD no artigo 46, tanto o controlador quanto o operador têm o dever de implementar medidas técnicas e administrativas que garantam a proteção dos dados pessoais contra acessos não autorizados e incidentes, como destruição ou perda de informações. Essas medidas devem ser revisadas e atualizadas regularmente, e, em caso de incidentes que possam

gerar riscos ou danos significativos aos titulares, é obrigatória a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados (BRASIL, 2018). A lei incentiva controladores e operadores a desenvolverem regras de boas práticas e governança no tratamento de dados pessoais como descrito no artigo 42, onde essas regras devem incluir normas de segurança, mecanismos de mitigação de riscos, ações educativas e procedimentos para atender solicitações dos titulares. A formulação dessas regras deve considerar fatores como a natureza e o porte do controlador, além da quantidade de operações realizadas. A ANPD também possui competência para editar normas complementares que orientem essas práticas (BRASIL, 2018).

Conforme a LGPD, controladores e operadores são responsáveis por reparar danos patrimoniais ou morais, individuais ou coletivos, causados em decorrência de violações à legislação de proteção de dados. A responsabilidade solidária entre controladores é prevista para garantir a reparação ao titular, enquanto os operadores podem ser eximidos de responsabilidade caso comprovem que não realizaram o tratamento atribuído, que não houve violação ou que o dano foi causado exclusivamente por culpa do titular ou de terceiros como previsto no artigo 50 (BRASIL, 2018).

3 METODOLOGIA

Neste presente artigo será utilizado como metodologia a análise bibliográfica de artigos referentes a área de direito em Tecnologia da Informação, junto da Lei Geral de Proteção de Dados (LGPD) como base de análise sobre o tema relacionado às leis que atuam na área de comércio de dados. Além de artigos da área jurídica, houve a realização de pesquisas e textos especializados da área de T.I com relação ao tema de dados e comércio do mesmo para uma apresentação e discussão sobre ele no cenário brasileiro.

Foi selecionado como fonte buscadora sites especializados em publicações como *Scielo* e *Google Scholar*. Neste artigo também foi utilizado de IAs especializadas em busca de artigos sobre o tema e correlatos sobre LGPD e comércio de dados e informações como as IAs *Perplexity*, *Consensus* e *Mônica*.

Para selecionar as fontes de inclusão para a seleção de artigos, serão utilizados como critérios artigos publicados na última década, em inglês e português sobre o tema “Dados pessoais como produto: Análise da atuação da LGPD na comercialização de dados pessoais”. As rejeições dos trabalhos excluíram os que não possuíam relevância direta para o objetivo do estudo.

4 ANÁLISE DE RESULTADOS E DISCUSSÃO

Como visto, a LGPD não possui artigos que mencionam diretamente o comércio de dados. Ela trata, de forma geral, sobre o compartilhamento e o tratamento de dados, além das respectivas responsabilidades do titular dos dados e dos operadores envolvidos.

A falta de abordagem específica pode ser interpretada como uma tentativa de não transformar os dados em um produto, preservando-os como um direito dos titulares, algo inegociável. Ainda assim, os dados são frequentemente vistos como *commodities* por grandes corporações da área de T.I., especialmente aquelas relacionadas às redes sociais. As informações são negociadas entre essas empresas, e seus setores de gerenciamento de informações podem ser considerados como um terreno fértil para a captação de dados sobre o comportamento e os hábitos de seus clientes/usuários.

Mesmo que estas empresas tenham amparo na lei para coleta e tratamento de dados, há brechas que permitem que elas, além de utilizarem esses dados para melhorias de serviços e produtos que oferecem, os utilizem para outros fins comerciais. Para essas corporações, as informações que possuem, são uma fonte rentável. De acordo com Barros (2018), os dados coletados com um propósito específico, mas utilizados de forma distinta, podem impactar significativamente a vida, a consciência e as decisões das pessoas, muitas vezes sem que elas tenham plena percepção disso. A discussão sobre como os dados, na forma de produto, é algo recente, mesmo que o primeiro conjunto de leis que aborda a proteção das informações no meio digital tenha sido criado em 1970, na Alemanha, no estado de Hesse, e seja conhecido como Hessisches Datenschutzgesetz.

Mesmo sendo recente esta discussão e também a legislação brasileira sobre proteção de dados, torna-se necessário um maior aprofundamento sobre o tema, tendo em vista que o processo de globalização e de hiper conexão do mundo à rede mundial de computadores é escalável à fabricação de dados por cada novo usuário conectado, mesmo que estes não tenham conhecimento sobre seus direitos referentes às informações pertinentes a si mesmo e considerando que muitos veem essas informações como sem valor algum.

5 CONSIDERAÇÕES FINAIS

Este estudo realizado evidencia que, embora a LGPD não atue explicitamente sobre o comércio de dados como categoria jurídica autônoma, ela estabelece uma série de padrões normativo robusto capaz de disciplinar, de forma indireta, porém eficaz, as práticas de coleta, tratamento, compartilhamento e monetização de dados pessoais. Ao afirmar princípios como a finalidade, a transparência, a minimização e a autodeterminação informativa, bem como ao positivar direitos dos titulares (acesso, correção, eliminação, portabilidade e revogação do

consentimento) e deveres de segurança e governança para controladores e operadores, a LGPD cria freios e contrapesos que tensionam a lógica econômica do capitalismo de vigilância e a opacidade dos mercados de dados.

Ainda assim se torna necessário que seja realizado uma revisão dos artigos, criação de novos artigos ou aditivos jurídicos junto de órgãos fiscalizadores independentes para que possam atuar diretamente neste ambiente comercial e tecnológico que possui capacidade realizar a modelagem de ideias e opiniões para benefício das grandes corporações de TI.

6 REFERÊNCIAS

ABES - Associação Brasileira das Empresas de Software. *Mercado Brasileiro de Software: Panorama e Tendências*. São Paulo: ABES, 2023.

BAPTISTA LUZ ADVOGADOS. Data Protection: regulamentação e mercado. São Paulo: Baptista Luz Advogados, 2019. Disponível em: <https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>. Acesso em: 29 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 mar. 2025.

CARVALHO, Victor Miguel Barros de. O direito fundamental à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória. 2018. Dissertação (Mestrado em Direito) — Universidade Federal do Rio Grande do Norte, Natal, 2018.

COELHO, Karolainy Vitória Ferreira. A tutela constitucional à privacidade frente à Lei Geral de Proteção de Dados: o impacto do uso indevido e da comercialização de dados pessoais na democratização das redes sociais. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) — Pontifícia Universidade Católica de Goiás, Goiânia, 2023.

LAGE, Daniel Dore. Monetização de dados pessoais como alternativa regulatória no Brasil: explorando possibilidades e desafios. *Revista Vertentes do Direito*, v. 11, n. 1, 2024, p. 84-108. DOI: 10.20873/uft.2359-0106.2020.v11n1.p84-108.

MALGIERI, Gianclaudio; CUSTERS, Bart. Pricing privacy: the right to know the value of your personal data. *Computer Law & Security Review*, v. 34, n. 2, p. 289-303, 2018. DOI: 10.1016/j.clsr.2017.08.006. Disponível em: <https://doi.org/10.1016/j.clsr.2017.08.006>. Acesso em: 23 mar. 2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância*. Rio de Janeiro: Intrínseca, 2021.

ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. In: EINLOFT, Denis; TOSS, Luciane; SEVERO, Valdete Souto (orgs.). *Direito do trabalho e pensamento crítico*. Porto Alegre: HS Editora, 2016. p. 79-95.