http://dx.doi.org/10.18623/rvd.v23.5877

MONETIZAÇÃO ILÍCITA DE DADOS PESSOAIS E A ECONOMIA PARALELA

ILLICIT MONETIZATION OF PERSONAL DATA AND THE PARALLEL ECONOMY

Artigo recebido em: 12/5/2025
Artigo aceito em: 3/4/2026

Fillipe Azevedo Rodrigues*
***Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil
Lattes: http://lattes.cnpq.br/1405096557504168
Orcid: https://orcid.org/0000-0002-8397-5094
rodrigues.cgern@gmail.com

Juliana de Lira Gomes*
***Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil
Lattes: http://lattes.cnpq.br/7702981145422226
Orcid: https://orcid.org/0009-0001-6278-7676
juliana.gomes.129@ufrn.edu.br

Patrícia Borba Vilar Guimarães*
***Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil
Lattes: http://lattes.cnpq.br/3134219236556237
Orcid: https://orcid.org/0000-0001-9130-3901
patricia.borba@ufrn.br

The authors declare that there is no conflict of interest

Resumo

O debate acerca da proteção de dados pessoais se acentuou diante dos avanços tecnológicos, que expandiram os riscos à privacidade e à intimidade. Nesse sentido, a monetização ilícita de dados pessoais é preocupante não apenas para a tutela de informações pessoais, mas também para a prevenção de crimes, como a lavagem de dinheiro. Diante disso, questiona-se como a comercialização ilícita de dados pessoais pode impulsionar a prática desse crime. O artigo propõe descrever a relação entre monetização ilícita de dados pessoais e o crime de lavagem de dinheiro, averiguando o debate sobre proteção de dados pessoais e suas características, analisando a monetização de informações pessoais e sua vulnerabilidade na exploração econômica e verificando o desenvolvimento do crime de lavagem de dinheiro mediante o uso de dados pessoais. A pesquisa possui abordagem bibliográfica e documental, de natureza qualitativa e de nível descritivo. Justifica-se em razão do histórico de vazamento de dados pessoais e o acesso irregular a essas informações, que possibilita a sua utilização para fins ilícitos. Por fim, acredita-se que a monetização ilícita de dados pessoais pode contribuir para o aperfeiçoamento do crime de lavagem de dinheiro, ocupando um preocupante papel nesse contexto digital.

Abstract

The debate surrounding the protection of personal data has intensified in light of technological advancements, which have expanded the risks to privacy and intimacy. In this sense, the illicit monetization of personal data is concerning not only for the protection of personal information but also for the prevention of crimes such as money laundering. Therefore, the question arises as to how the illicit commercialization of personal data can fuel the practice of this crime. This article proposes to describe the relationship between the illicit monetization of personal data and the crime of money laundering, examining the debate on personal data protection and its characteristics, analyzing the monetization of personal information and its vulnerability to economic exploitation, and verifying the development of the crime of money laundering through the use of personal data. The research employs a bibliographic and documentary approach, of a qualitative and descriptive nature. It is justified by the history of personal data leaks and unauthorized access to this information, which allows its use for illicit purposes. Finally, it is believed that the illicit monetization of personal data can contribute to the improvement of money laundering, playing a worrying role in this digital context.

Palavras-chave: Dados Pessoais. Economia Paralela. Lavagem de Dinheiro. Monetização de Dados Pessoais.

Keywords: *Personal Data. Parallel Economy. Money Laundering. Monetization of Personal Data.*

1 INTRODUÇÃO

A tutela de dados pessoais confirma a importância de se discutir sobre a proteção de informações em uma sociedade cada vez mais guiada pela governança de dados, possuindo essas informações um trabalho significativo, tanto na perspectiva social como econômica.

O avanço tecnológico não trouxe apenas benefícios, como otimização, crescimento, eficiência etc., mas também apresentou alguns aspectos preocupantes, como a monetização ilícita de dados pessoais, possibilitando o desenvolvimento de um mercado ilegal, capaz de auxiliar na prática de crimes, como a lavagem de dinheiro. Nesse sentido, a inovação tecnológica apresenta um caráter ambíguo, pois é capaz tanto de combater crimes como de favorecer a sua ocorrência.

Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) seja o amparo legal na tutela da privacidade, organizando a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais na atuação de empresas privadas e órgãos públicos, é preciso considerar as dificuldades de se atingir um cumprimento integral da norma, em razão da existência de lacunas que criam oportunidades para a realização de ilícitos, assim como as próprias tentativas de se subverter as instruções da norma.

A utilização de dados pessoais para a realização de transações e negócios ilegais ocorre por meio do aproveitamento ilícito dessas informações, sem o consentimento do titular dos dados para essa finalidade, muito menos sob o seu conhecimento. Diante disso, questiona-se: como a comercialização ilícita de dados pessoais pode impulsionar a prática do crime de lavagem de dinheiro?

Dessa forma, o artigo propõe como objetivo geral descrever a relação entre monetização ilícita de dados pessoais e o crime de lavagem de dinheiro. Já de forma específica, na seção inicial, pretende-se averiguar o debate sobre proteção de dados pessoais e suas características. Em seguida, objetiva-se analisar a monetização de informações pessoais e sua vulnerabilidade na exploração econômica. Por fim, propõe-se

verificar o desenvolvimento do crime de lavagem de dinheiro mediante o uso de dados pessoais.

Para tanto, aproveitou-se da pesquisa bibliográfica ao utilizar produções nas áreas de Proteção de Dados Pessoais e Direito Penal Econômico, assim como serviu-se de revisão documental ao aproveitar da legislação acerca de dados pessoais (LGPD), e da Lei nº 9.613/1998, que trata sobre os crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores. Da mesma forma, foram consultadas notícias jornalísticas e informações públicas que tratam sobre a temática, sendo essas últimas referências concedidas pelo próprio governo mediante divulgação em sítio eletrônico oficial.

Além disso, o artigo possui uma pesquisa qualitativa, à medida que descreve características dos dados pessoais, sua relevância na sociedade moderna e a manipulação indevida para a realização de negócios ilegais. Da mesma forma, o estudo apresenta um nível de pesquisa descritivo ao abordar sobre o controle ilícito de informações pessoais, investigando como essa ocorrência possibilita a realização do crime de lavagem de dinheiro.

Este artigo foi produzido por meio das discussões promovidas pelo componente curricular do Seminário Jurídico Avançado em Constituição, Regulação e Desenvolvimento III, do Programa de Mestrado em Direito da Universidade Federal do Rio Grande do Norte (PPGD/UFRN). Nesse contexto, foram abordados temas como o crime do colarinho branco, corrupção e ética nos negócios globais, crime organizado e mercados ilegais etc., que contribuíram para a ampliação do debate associado a temas diversos, como o que será abordado neste artigo.

A pesquisa se justifica em razão do histórico de vazamento de dados pessoais e o acesso irregular a essas informações, que possibilita a sua utilização para fins ilícitos e distinto do conhecimento dos titulares. Da mesma forma, a lavagem de dinheiro é uma prática ilegal que vem se aperfeiçoando com a ascensão da tecnologia, valendo-se de lacunas regulatórias e do aspecto prejudicial dessa nova era para a prática de crimes.

Por fim, acredita-se que a monetização ilícita de dados pessoais pode contribuir para o aperfeiçoamento da prática delitiva da lavagem de dinheiro, ocupando um preocupante papel nesse contexto digital, tanto para a tutela de dados pessoais como para a prevenção criminosa.

2 PROTEÇÃO DE DADOS PESSOAIS E SEUS ATRIBUTOS

Informações pessoais carregam um valor individual, pois relacionam-se com a privacidade e intimidade de cada indivíduo, mas, não apenas isso. Dados pessoais são capazes de caracterizar o sujeito, pois não atuam apenas como identificador, mas também dispõem de aspectos sociais, econômicos e jurídicos.

Nesse sentido, ao reconhecer a relevância de dados pessoais na vida particular, o direito constitucional brasileiro elegeu a privacidade como um direito fundamental (Finkelstein; Finkelstein, 2019). O direito à privacidade tem sua compreensão ampliada fundamentada na evolução das formas de disseminação e apropriação de dados pessoais que expandiram as possibilidades de violação da vida privada (Modesto, 2020).

A legislação infraconstitucional tratou de abordar especificamente sobre a proteção de dados pessoais por meio da promulgação da LGPD, que foi profundamente influenciada pelo Regulamento Geral sobre a Proteção de Dados (RGPD), a legislação de privacidade da União Europeia.

Essa influência entre legislações evidencia como a proteção de dados pessoais não é uma preocupação exclusiva do estado brasileiro, mas também apresenta discussões no âmbito internacional, especialmente diante do contexto digital (Tomelin; Amaya, 2024), demandando a implementação de novas previsões legais ou a modernização das já existentes, possuindo mais de cem países marco regulatório acerca da proteção de dados pessoais (Cavallaro, 2023).

Embora a LGPD possua influência direta da legislação europeia, sua produção ocorreu através da elaboração de uma primeira versão do projeto de lei, realizada pelo Ministério da Justiça, em 2010, percorrendo 8 anos de debate sobre o assunto e duas consultas públicas (Aragão; Schiocchet, 2020), demonstrando uma longa caminhada para a determinação própria da tutela de informações pessoais.

Já no período da *vacatio legis* da norma, treinamentos, cursos e *lives* foram realizados, a fim de disseminar sobre o tema e o texto normativo nas organizações públicas e privadas, assim como para a área jurídica como um todo (Silva; Silva; Rehbein, 2023), evidenciando a relevância do debate sobre o tema.

Sendo assim, a LGPD se aplica a qualquer organização que processe dados pessoais no Brasil, independentemente de estar sediada ou não no país (Neto; Demoliner, 2018), e trouxe consigo um rol de princípios, diretrizes e bases de tratamento, voltando

sua atenção tanto para a figura do titular de dados como para o controlador e operador. Isso reflete o aspecto social da LGPD, tendo em vista que, de acordo com Freund *et al.* (2023), o titular de dados ocupa o papel de principal figura protegida pela norma.

Embora os dados pessoais não disponham apenas do aspecto social (utilização para identificação e interação), a característica econômica se traduz na transformação de dados pessoais em valor, que nasce da utilização das informações coletadas na prática de vendas direcionadas a usuários específicos, estreitando o relacionamento entre empresas e clientes, assim como nasce do compartilhamento desses dados com terceiros que buscam ampliar a sua base de dados para além da clientela já existente (Modesto, 2020).

Verifica-se que a incorporação de um significado econômico às informações pessoais está profundamente associada a atividades empresariais e negociais, assim como o avanço tecnológico, que enxerga dados como um meio de desenvolvimento ou como o próprio produto de atividade, não limitando essas informações a uma mera identificação, mas enxergando potencial em diferentes aspectos.

Dessa forma, o tratamento de dados pessoais está atrelado não apenas a digitalização das atividades, mas também se refere às relações de consumo, que são muito aprimoradas mediante a utilização de dados pessoais. Isso demonstra como a informação pode ser utilizada como um ativo ou um instrumento de suporte a decisões (Cohen, 2002).

Portanto, o valor econômico dos dados pessoais foi intensamente impulsionado pela modificação na dinâmica da relação entre empresas e consumidores. Isso porque as instituições costumavam dirigir-se aos indivíduos para apresentar o seu serviço ou produto, mas a tecnologia modificou isso, pois agora os consumidores são levados até as empresas (Estrada, 2016), e a utilização de dados para a criação de uma relação de consumo é parte disso.

Nesse contexto, Lage (2024) observa que, independentemente da possibilidade ou não da comercialização de dados pessoais, eles possuem valor econômico. O novo modelo de negócio (baseado na tecnologia e uso de dados) centraliza também o debate acerca da privacidade dos titulares de dados pessoais, tendo em vista que suas informações são utilizadas como insumo, o que gera o desafio de avaliar o desenvolvimento econômico e a proteção à privacidade, buscando formas de minimizar os impactos prejudiciais (Adjei, 2015).

Pode-se deduzir que o aspecto econômico dos dados pessoais supera qualquer outro valor, pois não se limita apenas ao alcance do titular de dados, mas possui força para modificar empreendimentos e relações negociais.

Desse modo, Lage (2024) observa que a comercialização de dados já faz parte do mundo real, e que os modelos de negócios que se baseiam na atribuição de valor aos dados têm se tornado predominantes, especialmente nos negócios digitais (Malgeri; Custers, 2017), como o sistema de cookies[1]. Ainda, a sociedade da informação (momento mais recente da sociedade) é qualificada pela valorização econômica de dados pessoais (Vianna; Costa; Léda, 2025).

A discussão em torno da proteção de dados é resultado de uma sociedade cada vez mais digitalizada, onde a coleta de informações é uma prática comum e demasiada (Tomelin; Amaya, 2024). Desse modo, a segurança de dados relaciona-se tanto com informações armazenadas em ambiente físico como aquelas cujo seu armazenamento depende de alguma tecnologia da informação e comunicação (TICs) (Silva; Silva; Rehbein, 2023), o que influencia diretamente na tutela de informações pessoais.

A inclusão do debate na Constituição de 1988, por meio da EC 115/2022, elevou mais uma vez o patamar da discussão sobre privacidade, intimidade e proteção de dados ao teor constitucional, pois a tutela da privacidade não se restringe mais ao "direito de ser deixado só", mas também se transforma no direito de manter o controle sobre as próprias informações (Schereiber, 2014). Além disso, o caráter constitucional da proteção de dados pessoais fortalece o desenvolvimento do tema, sendo capaz, inclusive, de abrir precedentes para outras discussões, como monetização de dados e economia.

A abordagem constitucional sobre a proteção de dados pessoais reflete também a relação da temática com a revolução tecnológica. Isso porque, como apontam Finkelstein e Finkelstein (2019), o avanço da tecnologia atuou como um marco no tema da privacidade, pois reforçou a sua vulnerabilidade à exposição.

Considerando isso, Lage (2024) enxerga a LGPD como uma norma ainda em construção, existindo margem para discussão própria acerca da monetização de dados pessoais. Dessa forma, ainda pode-se enxergar espaço para a inclusão de outros temas em conjunto a promoção da proteção de dados.

[1]O sistema de cookies se utiliza de arquivos de textos armazenados nos dispositivos de usuários da internet para registrar informações sobre acesso e navegação, com o objetivo de aprimorar experiências online e personalizar conteúdo.

Em conclusão, as informações pessoais possuem um alto valor social e econômico, que deve ser considerado para a tutela dos dados e, ao mesmo tempo, buscar equilibrar a proteção de direitos fundamentais e um desenvolvimento social e econômico, que pode ser aperfeiçoado pela força dessas informações.

3 MONETIZAÇÃO DE INFORMAÇÕES PESSOAIS

Tendo em vista o caráter econômico de dados pessoais e a possibilidade de sua exploração como parte de uma nova forma de economia, informações pessoais representam um poder nesta era digital, especialmente quando exploradas para o desenvolvimento de empreendimentos.

A monetização de dados pessoais pode ser entendida como a transformação de coisas que não possuem valor agregado ou a modificação de algo que dispõe de algum valor, de modo que as informações pessoais podem ser utilizadas na facilitação de transações ou como o próprio objeto de transação (Adjei, 2015).

Observa-se que a comercialização de dados já era prevista como possível e, inclusive, indispensável para o desenvolvimento de negócios e estruturas diante das novas possibilidades trazidas pelo avanço da tecnologia. De acordo com Adjei (2015), essa prática é um dos principais aspectos dos modelos de negócios modernos, que foi modificado em razão do surgimento de novos mecanismos.

O avanço tecnológico abriu caminho para a monetização de dados pessoais (Barros; Santos, 2024). Com isso, novas possibilidades de remuneração para as empresas nasceram, e a monetização dos dados possui duas abordagens: interna (transformação dos dados em inteligência capaz de impulsionar os resultados) e externa (transformação dos dados pessoais em produto próprio, com relevância e valor de mercado, sendo uma nova fonte de receita para os negócios) (Modesto, 2020).

Todavia, ressalta Cohen (2002) que não houve transformação nas regras gerais de economia, ocorrendo apenas a modificação na forma como a informação é utilizada, resultando na adoção do termo “economia da informação”, que se caracteriza pelo aproveitamento dos dados como um bem econômico essencial, sendo essa a configuração da sociedade moderna. Além disso, dados pessoais representam uma importante nova fonte de receitas para organizações, estando suscetíveis como ativos buscados em situações de fusão e aquisição de organizações (Modesto, 2020).

Nessa perspectiva, Vianna, Costa e Léda (2025) apontam que para compreender a ascensão do mercado de dados ao patamar de economia é importante observar a contextualização histórica, tendo em vista que cada época possui um elemento principal de desenvolvimento e estruturação social. Por exemplo, a agricultura, a industrialização e a prestação de serviços foram recursos essenciais para a era que antecedeu a sociedade da informação (Vianna; Costa; Léda, 2025).

A economia tem sido cada vez mais marcada pela utilização de dados pessoais em modelos de negócios. Dessa forma, utiliza-se o máximo de dados possíveis, inclusive, sem a certeza se tais informações serão realmente necessárias (Modesto, 2020). Observa-se que, embora a LGPD disponha do princípio da necessidade como um dos norteadores no tratamento de informações pessoais, dados ainda são coletados de forma excessiva, recolhendo-se, assim, informações desconectadas com o propósito de tratamento, o que resulta em afronta direta à previsão normativa.

Essas informações em excesso acabam sujeitas à distorção da utilidade a que foram propostas inicialmente no momento de sua concessão. É nesse contexto que os dados pessoais são explorados para fins distintos e até ilícitos, situações desconhecidas pelos titulares das informações.

A permissão para a coleta e o tratamento de dados pessoais pode passar a ideia de que é possível usufruir de forma irrestrita dessas informações, gerando ausência de transparência na administração desses dados (Modesto, 2020). A falta de clareza no tratamento de dados pessoais para o titular da informação também se configura como um prejuízo grave, pois distancia o indivíduo do controle de suas informações. Tendo isso em vista, a inadequação legal no tratamento de dados pessoais pode suceder a comercialização de informações a terceiros e a utilização de plataformas online ampliam ainda mais esse risco (Tomelin; Amaya, 2024).

Nesse contexto, o principal exemplo de acúmulo de informações pessoais são as redes farmacêuticas, pois são empresas que possuem um amplo e detalhado histórico de dados coletados ao longo de vários períodos, e esse acervo de informações pode estar suscetível a monetização (Tomelin; Amaya, 2024), inclusive de forma ilícita, sem o consentimento do titular.

Mesmo a exploração econômica de dados pessoais apresentando-se como um novo meio de economia e empreendimento, podendo ser utilizado de forma legal através do consentimento do titular, observa-se que a LGPD não aborda de forma expressa no texto

da lei sobre a permissão ou proibição de tal prática, compreendendo apenas que qualquer utilização sem a concordância e o conhecimento do titular dos dados pessoais deve ser considerada ilegal[2]

Todavia, tramita no Brasil um Projeto de Lei acerca da monetização de dados que objetiva a criação de um ecossistema para a comercialização de dados de pessoas físicas e jurídicas. Dessa forma, o PL 234/2023 busca equilibrar proteção de dados pessoais e a exploração econômica. Contudo, o referido projeto provocou preocupações legítimas, como a tutela de direitos individuais e dados sensíveis, que exige uma proteção ainda mais incisiva.

Preocupações acerca da legalização da comercialização de dados pessoais são legítimas, pois informações pessoais já são exploradas através do vazamento de dados, o que resulta no acesso e na comercialização indevida de diversas informações. Observa-se que a venda de dados obtidos através de invasão à sistemas federais já foi alvo de investigação pela Polícia Federal do Brasil, por meio da operação I-Fraude, que objetivou combater os crimes de invasão de dispositivo informático, lavagem de dinheiro e organização criminosa.

Nesta operação, apurou-se que dados de autoridades e pessoas publicamente conhecidas estavam disponíveis para acesso. Sendo assim, era ofertado um painel de consulta, por meio das redes sociais, que poderia ser obtido por meio de planos de mensalidade e dentre os usuários foi possível identificar membros de facção criminosa e até mesmo integrantes das forças de segurança (GOV, 2024).

Nesse contexto, a Polícia Federal observa que “A utilização e comercialização de sistemas de pesquisa ilícitos cujos insumos são dados pessoais, ilicitamente obtidos, fomenta a indústria de intrusão em bancos de dados [...] incentivando a ação de grupos especializados nesse tipo de crime” (GOV, 2024). Dessa forma, essas práticas ilegais incentivam a aquisição e a comercialização de informações pessoais para fins ilícitos, o

[2]Em janeiro de 2025, a Agência Nacional de Proteção de Dados (ANPD) determinou a suspensão de incentivos financeiros por meio de coleta de íris, atingindo diretamente a empresa Tools for Humanity (TFH), que coletava dados biométricos para a criação da chamada World ID. Nesse contexto, entendeu-se que a contraprestação pecuniária oferecida pela empresa pode interferir na livre manifestação de vontade dos titulares desses dados. Além disso, a ANPD identificou que o tratamento de dados pessoais realizado pela empresa é grave, pois manuseia dados pessoais sensíveis, sem possibilidade de exclusão dos dados biométricos coletados e irreversibilidade da revogação do consentimento do titular. Estes pontos são muito preocupantes, pois demonstram uma clara afronta à LGPD, configurando-se totalmente em desacordo com o teor da norma legal. Saiba mais em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos-financeiros-por-coleta-de-iris

que se apresenta como um desafio na promoção da proteção de dados pessoais e na prevenção de crimes contra a ordem econômica.

O comércio ilegal de dados pessoais pode prejudicar não apenas a ordem econômica, tendo em vista a possibilidade de sua utilização como ferramenta na prática de crimes dessa natureza, mas, sobretudo, pode atingir de forma direta a dignidade da pessoa humana, infringindo a privacidade dos indivíduos.

Mesmo no acesso às plataformas digitais de forma simples mediante cadastro, ressalta-se que o fornecimento de dados pessoais em troca da utilização de serviços "gratuitos" (Modesto, 2020) não se mostram tão voluntários assim, tendo em vista que o titular de dados fornece suas informações pessoais em troca de tais serviços e acessos. Nessa relação, esses dados valem como moeda de troca, pois o indivíduo fica livre para acessar o conteúdo ou serviço que deseja, e o provedor mantém seus dados para aplicações.

Por isso, a monetização de dados pessoais pode resultar também em rentabilidade para o responsável pela sua coleta ou tratamento (Adjei, 2015), pois pode ser comercializado para movimentar negócios e definir estratégias, revelando aspectos para além da identificação, propriedade e sensibilidade das informações pessoais.

Tendo isso em vista, Lage (2024) acredita que explorar o aspecto econômico de dados pessoais significa uma tendência capaz de auxiliar para a chegada de um estágio maduro de ecossistema de proteção de dados pessoais, que poderá abrir novas oportunidades econômicas. Ou seja, não se pode caracterizar a comercialização de dados pessoais como algo totalmente ruim, pois essa prática, especialmente quando realizada de forma legal, pode resultar em vantagens econômicas e sociais.

No entanto, é preciso definir formas e meios para que essa monetização ocorra em conformidade com as previsões da LGPD e, acima de tudo, mantenha o titular de dados como figura prioritária nessa relação, objetivando proteger a pessoa humana, sua privacidade e autodeterminação informativa. Ainda, a digitalização de dados possui uma dimensão coletiva que não pode servir de fundamento para uma monetização irrestrita dos direitos de privacidade dos usuários (Tomelin; Amaya, 2024).

Por fim, ressalta-se que a ausência de previsão explícita quanto a comercialização de dados pessoais pela LGPD é uma preocupante lacuna, pois permite que controladores e operadores de informações pessoais se utilizem desses dados de forma indiscriminada,

em desconformidade com a norma e desrespeitando os direitos dos titulares, subvertendo o mercado econômico e desenvolvendo negócios ilícitos.

4 UTILIZAÇÃO DE DADOS PESSOAIS NO CRIME DE LAVAGEM DE DINHEIRO

Com frequência, dados pessoais são utilizados de forma indiscriminada, sem o conhecimento e consentimento do titular, explorando-se a característica econômica dessas informações, manuseando esses dados para o desenvolvimento de negócios, e até mesmo para a ocultação de práticas ilícitas. Desse modo, a utilização de dados pessoais tem sido um meio para o branqueamento de capitais, expondo uma nova forma de se praticar o crime de lavagem de dinheiro por organizações criminosas.

Isso ocorre porque o processo de formação do crime organizado usualmente se desenvolve por meio da exploração de mercados ilícitos e, inclusive, suas operações não se limitam apenas a áreas ilegais, mas também atuam em campos legítimos de exploração econômica (Rodrigues, 2014).

Por sua vez, a lavagem de dinheiro nada mais é do que o processo pelo qual busca-se conceder aparência lícita a recursos resultantes de práticas ilícitas. Portanto, a configuração da lavagem de dinheiro depende da existência de um crime distinto e anterior (Lima; Vaz; Lini, 2022). Assim sendo, a lavagem de dinheiro apresenta-se como uma atividade complementar, pois costuma estar associada à prática de um crime principal.

Isso foi impulsionado pela evolução dos mecanismos de disfarce das atividades ilícitas que progrediu para a criação de empresas de fachada, surgindo o método de lavagem de dinheiro como uma alternativa para o desfrute dos rendimentos oriundos de atividade criminosa (Rodrigues, 2014).

Além disso, na prática do crime da lavagem de dinheiro, também ocorre a conversão dos bens, valores ou direitos adquiridos de forma ilegal em ativos ilícitos. Sendo assim, essas aquisições podem ser adquiridas, negociadas, trocadas etc. (Lima; Vaz; Lini, 2022).

O desenvolvimento do crime de lavagem de dinheiro ocorre por etapas, iniciando-se pela fase de colocação, em que os bens ou dinheiro de origem ilícita são inseridos no sistema financeiro, que pode ocorrer por meio de depósitos bancários, fracionamento de

valores ou compra de bens, sendo essa a fase mais vulnerável à descoberta do crime. Em seguida, ocorre a etapa de ocultação, que é utilizada para dificultar o rastreamento da origem ilícita, na tentativa de "limpar" o dinheiro ou bem adquirido ilegalmente. Aqui são utilizadas empresas de fachada para conferir credibilidade a essa atividade e o resultado positivo dessa fase é a continuidade da conduta delitiva, pois ocorre a movimentação dos lucros e a possibilidade da sua utilização. Por fim, ocorre a integração, sendo essa etapa final onde o dinheiro já "lavado" é reintroduzido na economia legal, dispondo de uma aparência de origem lícita.

Com o tempo, essas etapas puderam ser aperfeiçoadas, especialmente porque a revolução tecnológica transformou diferentes atividades ao possibilitar inovações, mas também trouxe desafios significativos, principalmente no âmbito dos crimes financeiros, com o aperfeiçoamento da prática de lavagem de dinheiro diante das lacunas vulneráveis da era digital, possibilitando a execução de crimes econômicos (MPMT, 2024).

Isso porque, criminosos exploram o anonimato, a rapidez e a natureza transfronteiriça de transações digitais para lavar fundos ilícitos, valendo-se de técnicas e da tecnologia para obscurecer a origem, propriedade e destino dos fundos, tornando, dessa forma, a identificação e rastreamento desse dinheiro mais desafiador (MPMT, 2024). Nesse sentido, as desvantagens proporcionadas pelo sistema tecnológico são:

> [...] anonimato — transações digitais podem ser realizadas com pseudônimos ou por meio de plataformas que oferecem certo nível de anonimato, tornando difícil rastrear a origem dos fundos; abrangência global — transações digitais possibilitam a lavagem de dinheiro em fronteiras, explorando diferenças jurisdicionais e a complexidade dos sistemas financeiros internacionais; e velocidade e eficiência — transações digitais ocorrem em tempo real, permitindo que lavadores de dinheiro movimentem fundos rapidamente e explorem oportunidades sensíveis ao tempo (MPMT, 2024).

A criminalidade também se expandiu por intermédio dos sistemas financeiros, impulsionados pelo processo de integração de mercados (Rodrigues, 2014), que ampliou o espaço econômico, ao mesmo tempo em que trouxe desafios como os crimes financeiros e as organizações criminosas transnacionais.

Em 2025, descobriu-se, no Brasil, a utilização de *fintechs*[3] para a prática de lavagem de dinheiro e ocultação de grandes patrimônios. Essas *fintechs*, que prestam

[3]São empresas que utilizam inovação tecnológica para oferecer serviços financeiros. Nesse sentido, a digitalização de atividades propicia um ambiente favorável para o surgimento dessas empresas. De acordo com o Banco Interamericano de Desenvolvimento (BID), entre os anos de 2017 e 2023, houve um aumento

serviços financeiros de forma digital, eram utilizadas pelo crime organizado, para a realização de transações fraudulentas. Ressalta-se que isso foi possível em razão do nível de exigência regulatória para a prestação de contas sobre saldos e movimentações de *fintechs* ser distinto daquele aplicado às instituições bancárias tradicionais (O TEMPO, 2025).

O mesmo conjunto de normas que viabilizou as *fintechs* também permitiu a abertura de contas digitais, dispensando a presença em uma agência física, o que contribuiu para a realização de fraudes mediante a utilização de dados pessoais vazados (O TEMPO, 2025). Diante dessa possibilidade, observa-se que a monetização de dados pessoais pode ser utilizada como um meio para a prática de lavagem de dinheiro e fraudes financeiras, sendo mais um mecanismo de branqueamento de capitais para as organizações criminosas.

Diante do ocorrido, a Receita Federal do Brasil voltou a exigir das *fintechs* a apresentação da declaração e-financeira, equiparando-se assim aos bancos tradicionais, nos termos da instrução normativa RFB 2.278/2025, como medida de combate aos crimes contra a ordem tributária.

De acordo com o estudo realizado pelo Fórum Brasileiro de Segurança Pública e o Instituto Esfera, o Conselho de Controle de Atividades Financeiras (Coaf)[4] registrou um levantamento com dados entre 2015 a 2024 que apontou um aumento de 766% no número de operações suspeitas comunicadas ao órgão. Ainda, o estudo destacou o aperfeiçoamento de métodos na prática da lavagem de dinheiro, valendo-se justamente da digitalização financeira e brechas regulatórias, com o auxílio, em especial, das *fintechs*, plataformas de apostas onlines (BETs) e criptomoedas (Ribbeiro, 2025).

Nesse cenário, a utilização de dados pessoais na realização do crime de lavagem de dinheiro pode auxiliar na facilitação, ocultação ou conceder o aspecto legal a operações ilegais, valendo-se para a criação de contas, aberturas de linhas de crédito, solicitação de empréstimos, estruturação de instituições de fachada etc. Sendo assim, informações pessoais estão vulneráveis à comercialização ilícita para a exploração financeira indevida de seu caráter econômico.

---

de 340% do surgimento das *fintechs*. Saiba mais em: https://g1.globo.com/economia/noticia/2025/09/01/como-as-fintechs-mudaram-o-sistema-financeiro-no-brasil.ghtml.

[4]Unidade de Inteligência Financeira (UIF) do Brasil, associada ao Ministério da Fazenda, sendo responsável pelo combate a lavagem de dinheiro, entre outros crimes financeiros.

Não o suficiente, a existência de golpes que subtraem informações pessoais (também conhecido como roubo de identidade) envolvem o uso indevido de dados confidenciais, como CPF, senhas e números de cartão, para cometer fraudes financeiras e outros crimes. O principal método de obtenção desses dados é o *phishing*[5] que engana as vítimas para que forneçam suas informações.

Nessa circunstância, a digitalização de serviços também permitiu o aperfeiçoamento de técnicas para a prática de ilicitudes, sendo as habilidades mais comuns utilizadas para a lavagem de dinheiro, entre outros exemplos, o roubo de identidade digital e identidades sintéticas[6] (MPMT, 2024).

O MPMT (2024) observa que essas habilidades se caracterizam como uma "engenharia social", pois envolve a apropriação de dados pessoais para criar identidades fraudulentas. Ainda, as identidades sintéticas podem ser utilizadas para a abertura de contas bancárias, estabelecer empresas de fachada e realizar transações.

A realização dessas práticas para obter dados pessoais expõem que a existência de um mercado paralelo de comercialização de dados ocorre com frequência para alimentar atividades negociais e financeiras (Estrada, 2016), sendo os dados pessoais o próprio produto ou meio para a prática do crime de lavagem de dinheiro. Nessa perspectiva, Rodrigues e Rodrigues (2016) entendem que para a prevenção de atividades ilícitas, o crime deve ser combatido em sua verdadeira origem, utilizando-se da criação de mecanismos que impeçam a atividade delituosa.

Diante dos desafios proporcionados pela alta tecnologia em atividades financeiras, o desenvolvimento de sistemas de proteção se mostra como uma alternativa interessante. Nesse sentido, a existência da política *know your customer* (KYC)[7], sendo essa uma das principais obrigações estabelecidas pela Lei de Lavagem de Dinheiro, dispondo sobre em seu art. 10, inciso I (Fernandes; Zani, 2022), expõe a importância de compreender clientes

[5]É um tipo de golpe cibernético em que criminosos se disfarçam de entidades legítimas, como bancos, empresas etc., e se comunicam com usuários por meio de e-mail ou sites falsos para obter dados pessoais e sensíveis. Além disso, outro golpe cibernético muito conhecido é o *pharming*, que consiste em redirecionar usuários que acessam um site confiável para um site falso, operando como um sistema mais sofisticado que o *phising*.

[6]O roubo de identidade sintética é um tipo de fraude aprimorada, que combina informações reais e falsas para a partir disso criar uma nova identidade e utilizá-la, sendo mais difícil de detectar do que o tipo de roubo comum de identidade.

[7]É um sistema em que empresas financeiras aproveitam para identificar, verificar e compreender o perfil de risco de seus clientes, ampliando os padrões de segurança e prevenindo crimes como a lavagem de dinheiro. Dados pessoais são coletados, validados e monitorados, a fim de garantir a legitimidade nas transações realizadas.

e proteger seus dados, pois, embora o tratamento de informações pessoais possa oferecer riscos à privacidade dos indivíduos, a utilização lícita dessas informações é importante para o desenvolvimento de negócios.

Além disso, a criação do sistema *Open Banking*, que atualmente é conhecido por *Open Finance*, é um sistema de compartilhamento de dados bancários, concebido com o objetivo de organizar bancos e *fintechs* em relação de igualdade, caracterizando-se este como um processo de equalização das condições competitivas entre agentes do mercado financeiro (Fernandes; Zani, 2022).

Além disso, o *open banking* também é responsável por observar a portabilidade, interoperabilidade e proteção de dados pessoais, de modo a garantir e estimular a concorrência do mercado financeiro sem vulnerabilizar a privacidade dessas informações (Trindade, 2021). Dessa forma, esse sistema busca instaurar uma relação competitiva de mercado justa e, ao mesmo tempo, proteger informações pessoais de usuários bancários, para que o acesso a esses dados ocorra de forma legal e legítima.

Nesse contexto, Silva, Marques e Teixeira (2011) também apontam a importância do desenvolvimento de controle interno e a implementação de uma cultura de prevenção à lavagem de dinheiro. Além de sistemas próprios, a implementação de um controle por meio de *compliance*[8] pode auxiliar na identificação de problemas e dificuldades no funcionamento dessas empresas (Fernandes; Zani, 2022), pois é preciso considerar que empresas não dependem apenas do bom funcionamento de seus sistemas, mas também contam com a atuação ética de seus organizadores.

Desse modo, o compartilhamento de dados entre instituições financeiras e identificação de crimes como lavagem de dinheiro depende do comprometimento dos agentes que atuam nessas instituições, para que não tolerem ilícitos (Fernandes; Zani, 2022). Nesse sentido, o desenvolvimento legal de negócios financeiros não deve considerar apenas um sistema de compartilhamento e controle seguro de informações, mas também deve refletir a atuação direta de dirigentes, que não devem suportar relações ilícitas.

Portanto, imaginar a segurança e governança de dados em uma organização pressupõe identificar, de forma preliminar, os níveis de maturidade em que a empresa se

[8]Sistema que dispõe de um conjunto de práticas que asseguram a uma empresa estar em conformidade com as normas legais, regulamentos internos e a padrões éticos, promovendo uma cultura de integridade e transparência. Nesse contexto, o *compliance* é uma ferramenta importante na prevenção de fraudes e demais crimes.

encontra, o que implica também em conhecer os fluxos internos e externos durante cada ciclo de tratamento de informações pessoais (Silva; Silva; Rehbein, 2023), além de atuar no comprometimento dos agentes envolvidos, para que o fator humano esteja tão forte quanto os sistemas implementados na prevenção de ilícitos.

Em suma, a utilização de dados pessoais pode fomentar a execução do crime de lavagem de dinheiro, atuando tanto no momento prévio, podendo estar presente no crime auxiliar, como nas etapas próprias da lavagem de dinheiro, sendo também capaz de se tornar insumo para a realização de tal delito, o que pode incentivar ainda mais a prática desse crime com o auxílio da comercialização ilícita de dados pessoais.

5 CONSIDERAÇÕES FINAIS

Tendo em vista a discussão realizada no decorrer deste artigo, pode-se compreender que dados pessoais possuem uma nítida força econômica, ocupando uma posição importante nesta era digital. Além disso, informações pessoais transformam-se em ativos econômicos próprios, sendo uma fonte inesgotável, pois são recursos que surgem a todo momento, possibilitando de forma contínua a realização de novos negócios.

Nessa perspectiva, a monetização ilícita de dados pessoais pode auxiliar na prática da lavagem de dinheiro atuando como um facilitador nas etapas que constituem esse crime, especialmente no momento da ocultação, auxiliando na utilização de informações para a conversão de bens, valores e direitos adquiridos de forma ilegal. Ainda, a comercialização de informações pessoais pode impactar diretamente os sistemas de prevenção, como o KYC, fragilizando o sistema financeiro.

Uma possibilidade para harmonizar a relação entre dados pessoais e o desenvolvimento econômico é a observação quanto a necessária concordância do titular de dados pessoais no tratamento de suas informações. Além disso, também importa verificar a natureza das relações entre controlador, operador e titular de dados pessoais, para que atendam aos princípios, diretrizes e bases legais propostos pela LGPD, a fim de se possibilitar a criação de uma economia justa, competitiva e tecnológica, de modo a assegurar direitos fundamentais.

Além disso, é importante considerar que, apesar dos desafios e adaptações de práticas criminosas através do avanço tecnológico, a era digital apresenta vantagens que se sobressaem aos obstáculos apresentados, tendo em vista o desenvolvimento e inovação

dos setores público e privado, assim como as novas possibilidades de vida, negociação, transação, e experiências por intermédio da tecnologia.

Também se imagina uma modificação conjunta nas áreas de proteção a dados pessoais, privacidade e prevenção a crimes financeiros, para que suas respectivas normas estejam alinhadas, atuando assim de forma eficaz na precaução quanto à ocorrência de crimes que se utilizam de informações pessoais obtidas de forma ilícita ou não. Nesse sentido, as exigências igualitárias entre *fintechs* e demais bancos tradicionais se mostram como uma decisão positiva para atenuar a prática de crimes econômicos.

Por fim, o aprimoramento e fortalecimento de sistemas de controle e segurança são fundamentais para a conformidade entre empresas e a legislação, sendo importante também redirecionar a atenção acerca do funcionamento legal das relações financeiras para a atuação dos agentes de mercado, para que possam identificar transações ilícitas e operar de forma ética, a fim de coibir a realização de crimes financeiros e a utilização ilegal de informações pessoais.

REFERÊNCIAS

ADJEI, Joseph Kwame. **Monetization of Personal Identity Information**: technological and regulatory framework. IEEE Computer Society Washington, Washington, 2015. Disponível em: https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf. Acesso em: 1 dez. 2025.

ARAGÃO, Suéllyn Mattos; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Reciis – Rev Eletron Comun Inf Inov Saúde**, v. 14, n. 3, p. 692-708, 2020.

BARROS, Thaís Fagundes; SANTOS, Valdivino Passos. Monetização de dados pessoais: o direito a imagem e o direito a reparação em caso de violação. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 11, p. 261-279, nov. 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/16487. Acesso em: 10 dez. 2025.

CAVALLARO, Amanda. Big techs, data protection, and competition regulation in a data-driven economy: a multidisciplinary approach. **Revista de Defesa da Concorrência**, Brasília, v. 11, n. 2, p. 11-26, 2023.

COHEN, Max Fortunato. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação**, v. 31, n. 3, 2002. Disponível em:

http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 1 dez. 2025.

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. **Revista de Direito do Trabalho**, São Paulo, v. 42, n. 172, p. 35-54, nov. 2016. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/100576. Acesso em: 1 dez. 2025.

FERNANDES, Alessandro; ZANI, João. Análise e detecção dos indícios de lavagem de dinheiro por instituições financeiras: construção de uma ferramenta para identificação e mitigação dos riscos decorrentes da utilização de dados compartilhados. **Revista Científica do CPJM**, v. 1, n. 4, p. 152-179, jun. 2022. Disponível em: https://rcpjm.cpjm.uerj.br/revista/article/view/102. Acesso em: 12 dez. 2025.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, Florianópolis, v. 23, n. 9, p. 284-301. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 9 out. 2025.

FREUND, Gislaine Parra *et al.* Proteção e privacidade de dados: um modelo para o gerenciamento de evidências. **Em Questão**, Porto Alegre, v. 29, p. 1-28, 2023. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/128009. Acesso em: 9 out. 2025.

GOV. **PF investiga venda de dados obtidos com invasão a sistemas federais**. 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/01/pf-investiga-venda-de-dados-obtidos-com-invasao-a-sistemas-federais. Acesso em: 12 dez. 2025.

LAGE, Daniel Dore. Monetização de dados pessoais como alternativa regulatória no Brasil: explorando possibilidades e desafios. **Vertentes do Direito**, Tocantis, v. 11, n. 1, p. 84-108, maio 2024. Disponível em: https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/18704/22498. Acesso em: 1 dez. 2025.

LIMA, Vinícius Cozim; VAZ, Vitor Hugo Gutendorfer; LINI, Priscila. Lavagem de dinheiro e manipulação de informações contábeis: uma análise da legislação nacional e da atuação do conselho de controle de atividades financeiras - coaf. **Repositório UFMS**, Mato Grosso do Sul, p. 1-16, nov. 2022. Disponível em: https://cpna.ufms.br/files/2022/03/LAVAGEM-DE-DINHEIRO-E-MANIPULACAO-DE-INFORMACOES-CONTABEIS-UMA-ANALISE-DA-LEGISLACAO-NACIONAL-E-DA-ATUACAO-DO-CONSELHO-DE-CONTROLE-DE-ATIVIDADES-FINANCEIRAS-COAF.pdf. Acesso em: 12 dez. 2025.

MALGIERI, Gianclaudio; CUSTERS, Bart. Pricing Privacy – the right to know the value of your personal data. **Computer Law & Security Review**, 2017. Disponível em: https://ssrn.com/abstract=3047257. Acesso em: 1 dez. 2025.

MODESTO, Jéssica Andrade. Breves considerações acerca da monetização de dados pessoais na economia informacional à luz da lei geral de proteção de dados pessoais. **Revista de Direito, Governança e Novas Tecnologias**, Florianópolis, v. 6, n. 1, p. 37-58, ago. 2020. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/6558. Acesso em: 1 dez. 2025.

MPMT. **A lavagem de dinheiro em ambientes digitais**: análise técnica. 2024. Disponível em: https://mpmt.mp.br/portalcao/news/1217/133775/a-lavagem-de-dinheiro-em-ambientes-digitais-analise-tecnica/146. Acesso em: 12 dez. 2025.

NETO, Eugênio Facchini; DEMOLINER, Karine Silva. Direito à privacidade e novas tecnologias: breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, p. 19-40, 2018.

O TEMPO. **Cibercrime usa dados de cidadãos em fintechs para lavar dinheiro; saiba se você já foi vítima**. 2025. Disponível em: https://www.otempo.com.br/economia/2025/9/3/cibercrime-usa-dados-de-cidadaos-em-fintechs-para-lavar-dinheiro-saiba-se-voce-ja-foi-vitima#:~:text=Cibercrime%20usa%20dados%20de%20cidad%C3%A3os%20em%20fintechs%20para%20lavar%20dinheiro. Acesso em: 12 dez. 2025.

PEREIRA, Vinícius. **Como as fintechs mudaram o sistema financeiro no Brasil**. 2025. Disponível em: https://g1.globo.com/economia/noticia/2025/09/01/como-as-fintechs-mudaram-o-sistema-financeiro-no-brasil.ghtml. Acesso em: 01 dez. 2025.

RIBBEIRO, Leonardo. **Coaf registrou aumento de 766% na comunicação de operações suspeitas**. 2025. Disponível em: https://www.cnnbrasil.com.br/politica/coaf-registrou-aumento-de-766-nas-comunicacao-de-operacoes-suspeitas/. Acesso em: 12 dez. 2025.

RODRIGUES, Fillipe Azevedo; RODRIGUES, Liliana Bastos Pereira Santo de Azevedo. **Lavagem de dinheiro e crime organizado**: diálogos entre Brasil e Portugal. Belo Horizonte: Del Rey, 2016.

RODRIGUES, Fillipe Azevedo. **Crime organizado e a tutela penal do branqueamento de capitais**: um estudo crítico a partir do direito penal do bem jurídico. 2014. 30 f. TCC (Graduação) - Curso de Doutoramento em Direito, Universidade de Coimbra, Coimbra, 2014.

SALTER, Michael; MASON, Julie. **Writing law dissertations**: an introduction and guide to the conduct of legal research. 1. ed. Harlow: Pearson Longman, 2007.

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

SILVA, Jorge Luiz Rosa da; MARQUES, Luis Fernando Bicca; TEIXEIRA, Rosane. Prevenção à Lavagem de Dinheiro em Instituições financeiras: avaliação do grau de aderência aos controles internos. **Base - Revista de Administração e Contabilidade da Unisinos**, v. 8, n. 4, p. 300-310, out. 2011.

SILVA, Rosane Leal da; SILVA, Raonny Canabarro Costa da; REHBEIN, Katiele Daiana da Silva. A proteção de dados pessoais por agentes de pequeno porte: a governança e as boas práticas como estratégias de implementação da lgpd. **Meritum**, Minas Gerais, v. 18, n. 1, p. 35-54, abr. 2023. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/9249. Acesso em: 1 dez. 2025.

TOMELIN, Georghio Alessandro; AMAYA, Graciela. Tratamento de dados pessoais pelas farmácias brasileiras. **Revista de Direito da Saúde Comparado**, São Paulo, v. 3, n. 5, p. 72-94, dez. 2024. Disponível em: https://periodicos.unisa.br/index.php/direitosaude/article/view/706. Acesso em: 1 dez. 2025.

TRINDADE, Manoel Gustavo Neubarth. Open banking: trinômio portabilidade-interoperabilidade-proteção de dados pessoais no âmbito do sistema financeiro. **Revista Jurídica Luso-Brasileira**, n. 4, 2021.

VIANNA, João Lucas Paiva; COSTA, João Marcos Cerqueira Torres; LÉDA, Marina Rosas. A importância econômica e jurídica dos dados pessoais no século xxi: da sociedade da informação à proteção de dados pessoais. **Revista Foco**, v. 18, n. 12, p. 1-25, dez. 2025. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10947. Acesso em: 10 dez. 2025.

Contribuição dos autores

Todos os autores contribuíram igualmente para o desenvolvimento deste artigo.

Disponibilidade dos dados

Todos os conjuntos de dados relevantes para as conclusões deste estudo estão totalmente disponíveis no artigo.

Como citar este artigo (APA)

Rodrigues, F. A., Gomes, J. de L., & Guimarães, P. B. V. (2026). MONETIZAÇÃO ILÍCITA DE DADOS PESSOAIS E A ECONOMIA PARALELA. Veredas Do Direito, 23(6), e235877. https://doi.org/10.18623/rvd.v23.5877