Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

OPEN ACCESS

doi.org/10.51891/rease.v12i4.25791

# PRIVACIDADE E COMBATE AO CRIME NO JOGO ONLINE: RASTREABILIDADE, LGPD E O ENFRENTAMENTO DA LAVAGEM DE DINHEIRO

## PRIVACY AND COMBATING CRIME IN ONLINE GAMING: TRACEABILITY, LGPD AND COMBATING MONEY LAUNDERING

**Laura Eduarda Ribeiro de Araújo Silva**[1]
**Paulo Beli Moura Stakoviak Júnior**[2]

RESUMO: A evolução das tecnologias digitais e a expansão do mercado de jogos online geraram um ambiente dinâmico, complexo e suscetível à prática de crimes financeiros, principalmente a lavagem de dinheiro. Nesse contexto, a proteção de dados pessoais, fortalecida pela LGPD e intensificada pela crescente preocupação com a privacidade, começa a interagir diretamente com as demandas governamentais de rastreabilidade e combate à criminalidade econômica. Este artigo analisa essa tensão, explorando de que maneira as plataformas de jogos digitais, apesar de necessitarem do processamento de vastas quantidades de dados, se transformam em espaços susceptíveis a atos de fraude financeira. A partir de uma pesquisa qualitativa, fundamentada em revisão bibliográfica e análise normativa, busca-se entender como a LGPD, os mecanismos de compliance e as diretrizes nacionais e internacionais de PLD/FT podem interagir para equilibrar privacidade, segurança e integridade financeira. A conclusão é de que a eficácia no combate à lavagem de dinheiro em jogos online depende de um modelo regulatório que seja coerente, interoperável e tecnologicamente avançado, capaz de equilibrar direitos fundamentais com mecanismos de rastreamento robustos.



**Palavras-chave:** Privacidade. LGPD. Jogos online. Rastreabilidade. Lavagem de dinheiro.

ABSTRACT: The progress of digital technologies and the growth of the online gaming market have generated a dynamic, complex scenario that is susceptible to the occurrence of financial crimes, especially money laundering. In this context, the protection of personal data, strengthened by the LGPD and intensified by the growing concern about privacy, begins to interact directly with government demands for traceability and combating economic crime. This article analyzes this tension, investigating how digital gaming platforms, while depending on the processing of large volumes of data, become environments prone to financial fraud practices. Based on qualitative research, based on bibliographical review and normative analysis, we seek to understand how the LGPD, compliance mechanisms and national and international AML/FT guidelines can interact to balance privacy, security and financial integrity. The conclusion is that effectiveness in combating money laundering in online games depends on a regulatory model that is coherent, interoperable and technologically advanced, capable of balancing fundamental rights with robust tracking mechanisms.

**Keywords: Privacy.** LGPD. Online games. Traceability. Money laundering.

[1]Graduanda em Direito pela Universidade Estadual do Tocantins.
[2]Doutor em Direito pelo Instituto Brasiliense de Direito Público. Mestre em Direito pelo Instituto Brasiliense de Direito Público. Bacharel em Direito pelo Centro Universitário Luterano de Palmas. Professor e Coordenador do Curso de Direito da Universidade Estadual do Tocantins (UNITINS).

## 1 INTRODUÇÃO

A rápida digitalização das relações sociais e econômicas alterou significativamente a maneira como as pessoas interagem, consomem e se envolvem em ambientes virtuais. Nesse cenário, os jogos online surgem como ambientes com alta circulação de dados pessoais e movimentação financeira significativa, aumentando de forma exponencial os desafios regulatórios relacionados à privacidade, segurança e combate a atividades ilícitas. A proteção de dados, anteriormente vista como um aspecto da privacidade, tornou-se um componente fundamental para a prática da autonomia e para a confiabilidade dos ecossistemas digitais, de acordo com autores como Doneda (2014), Mendes (2019) e Bioni (2019).

Simultaneamente, o aumento de técnicas avançadas de lavagem de dinheiro no ambiente virtual demonstra que o modelo tradicional de fiscalização estatal já não é mais adequado para lidar com transações descentralizadas, micropagamentos automatizados, uso de criptoativos e operações transnacionais que excedem a capacidade regulatória das fronteiras nacionais. Dessa forma, o mercado de jogos online, devido à sua natureza descentralizada, global e extremamente lucrativa, começou a assumir um papel central na agenda regulatória atual.

No Brasil, diretrizes essenciais para o tratamento de dados e combate à lavagem de dinheiro são estabelecidas por instrumentos como o Marco Civil da Internet (Lei 12.965/2014), a Lei Geral de Proteção de Dados (LGPD) e a Lei 9.613/1998 (Lei de Lavagem de Dinheiro). No entanto, a falta de uma regulamentação específica para o setor de jogos eletrônicos - que foi parcialmente abordada por iniciativas recentes, como a Lei 14.790/2023 (Apostas de quota fixa) - evidencia que ainda existe uma discrepância entre a complexidade tecnológica do ambiente digital e a capacidade regulatória do país. A atuação de entidades como ANPD (Agência Nacional de Proteção de Dados), COAF (Conselho de Controle de Atividades Financeiras), Banco Central e Anatel (Agência Nacional de Telecomunicações) revela um panorama fragmentado, no qual diversas frentes buscam enfrentar riscos que estão interconectados.



Assim, o objetivo deste estudo, realizado por meio de uma abordagem qualitativa que inclui revisão bibliográfica, análise de marcos normativos e investigações sobre crimes financeiros, é analisar a conexão estrutural entre privacidade, rastreabilidade e prevenção à lavagem de dinheiro no âmbito dos jogos online. Busca-se entender como esses elementos, geralmente considerados opostos, podem interagir para criar um modelo regulatório equilibrado que assegure segurança sem comprometer direitos fundamentais.

Dessa forma, o artigo se desenvolve analisando a tensão entre proteção de dados e combate ao crime financeiro, os fundamentos da LGPD nas plataformas de jogos, os riscos inerentes do setor, o papel de tecnologias como IA (Inteligência Artificial), KYC ("Know Your Customer" - processo que verifica a identidade dos jogadores antes de permitir que apostem em plataformas digitais) e Blockchain (Tecnologia que permite registrar e rastrear transações em uma rede compartilhada e imutável), e a importância da cooperação internacional para o combate de práticas ilegais em ambientes digitais que operam além das fronteiras físicas.

## 2 A TENSÃO ENTRE PRIVACIDADE E COMBATE À LAVAGEM DE DINHEIRO

O debate sobre privacidade no ambiente digital passou a ser fundamental para a compreensão dos modelos regulatórios atuais. Além de ser um direito relacionado à intimidade, a privacidade tornou-se um requisito fundamental para o exercício da autonomia e para a participação segura em ambientes digitais complexos. Essa expansão conceitual - corroborada por autores como Barroso (2018), Sarlet (2015), Doneda (2014) e Mendes (2019) - vai além do campo teórico: impacta diretamente a dinâmica prática das plataformas digitais, que dependem da coleta constante de dados para sua atividade.



Apesar de o sistema jurídico brasileiro amparar esse direito por intermédio do Marco Civil da Internet (Lei 12.965/2014), da LGPD (Lei 13.709/2018) e de decisões do STF, como o RE 1010606 (Tema 987) e a ADPF 695, posteriormente reforçados pela EC 115/2022 (Proteção de Dados Pessoais), surgem tensões significativas entre privacidade, rastreabilidade e segurança. As plataformas digitais, principalmente aquelas que lidam com um alto volume de transações e interações transnacionais, aumentam significativamente a circulação de dados pessoais, gerando, assim, novas necessidades de governança, transparência e prevenção de abusos.

É nesse contexto que a discussão acerca da lavagem de dinheiro aparece. Tipicamente descrita em etapas de colocação (placement), ocultação (layering) e integração (integration), a lavagem de dinheiro tem se transformado devido à digitalização das relações econômicas. Essa mudança é abordada por Regis Prado (2017), André Callegari (2020) e por escritores internacionais como Michel Levi (2018) e Jack A. Blum (2016), que indicam o uso cada vez maior de tecnologia para dissimular valores e aumentar a opacidade nas transações.

O ponto central, entretanto, não reside na definição técnica do crime, mas na percepção de que os métodos tradicionais de prevenção se mostram menos eficientes frente a transações descentralizadas, micropagamentos automatizados, criptoativos e carteiras digitais. Essa

situação já foi demonstrada nas análises de Márcio Anselmo (2021) e nas Recomendações do GAFI/FATF (que são um padrão internacional para combater a lavagem de dinheiro, o financiamento do terrorismo e a proliferação de armas de destruição em massa), além das orientações da Lei 9.613/1998 e da Convenção de Palermo (Decreto 5.015/2004). Em outras palavras, a lavagem de dinheiro digital não é simplesmente uma versão digital do crime tradicional, mas um fenômeno que funciona de acordo com a mesma lógica estrutural dos sistemas digitais que tentamos regular.

O mercado de jogos online se tornou especialmente importante nessa interseção entre proteção de dados, rastreamento e fluxos econômicos digitais. Trata-se de um setor marcado pela ausência de fronteiras territoriais, pela aglomeração simultânea de milhões de usuários e por sistemas internos próprios de fluxo monetário - carteiras digitais, bônus, "moedas" virtuais, múltiplas contas e ativos que podem ser transformados em dinheiro real. Christopher Reale (2022), Marcelo Crespo (2021) e C. H. P. Marçal (2020), que descrevem os riscos operacionais comuns ao setor.

No cenário brasileiro atual, iniciativas de regulamentação, como a Lei 14.790/2023 e o PL 2.234/2022, evidenciam que o governo admite os perigos do setor. Ações como o bloqueio de plataformas ilegais pela Anatel (2024) fortalecem a ideia de que o mercado, apesar de promissor, necessita de mecanismos sólidos de compliance, identificação do usuário e monitoramento de transações.



Portanto, ao analisar em conjunto a evolução da proteção de dados, as mudanças na lavagem de dinheiro e a estrutura específica dos jogos online, fica claro que esses fatores não são autônomos. Ao contrário: as plataformas de jogos digitais estão exatamente no ponto de interseção entre eles. Dependem fortemente do processamento de dados pessoais, realizam transações de maneira rápida e descentralizada e estão expostas a técnicas de anonimização que facilitam atividades financeiras ilícitas.

Portanto, é claro que qualquer análise sobre rastreabilidade, segurança e LGPD no contexto dos jogos online deve considerar essa compreensão integrada: a proteção da privacidade e a prevenção da lavagem não são esferas que se excluem, mas dimensões que precisam dialogar para garantir um ambiente digital seguro, transparente e juridicamente equilibrado.

## 3 O FRAMEWORK REGULATÓRIO BRASILEIRO

Os jogos online se tornaram um dos ambientes mais dinâmicos para interação social contemporânea, mas também um dos mais desafiadores em termos de regulamentação. A variedade de perfis, operações financeiras internas, sistemas de comunicação e interoperabilidade entre plataformas coloca os operadores de e-games em um contexto em que a proteção de dados é tanto uma exigência legal quanto um requisito essencial para a legitimidade da atividade econômica. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018) estabelece o eixo normativo central para o tratamento de dados pessoais nessas plataformas, definindo princípios estruturantes (art. 6º), critérios de licitude (art. 7º) e salvaguardas específicas para dados sensíveis (art. 11).

A interpretação constitucional da LGPD, destacada por estudiosos como Danilo Doneda (2014) e Laura Schertel Mendes (2019), reforça a ideia de que a proteção dos dados está intimamente vinculada ao cerne essencial do direito à privacidade. Essa visão possibilita entender que, mesmo em contextos recreativos e privados como os jogos eletrônicos, o tratamento de dados deve respeitar os princípios de proporcionalidade, transparência e necessidade, especialmente quando se trata de metadados comportamentais, dados financeiros de microtransações ou estratégias de monitoramento antifraude.



Além disso, a literatura especializada - especialmente Rony Vainzof (2020), ao tratar da segurança da informação, e Bruno Bioni (2019), ao investigar os princípios básicos da LGPD - ajuda a demonstrar que a proteção de dados no setor de e-games vai além do consentimento ou da aceitação de termos de uso. Os responsáveis pelo serviço devem adotar práticas de governança, mecanismos técnicos robustos e políticas de retenção e descarte de dados compatíveis com o risco inerente ao seu modelo comercial.

Nesse contexto, surgem tensões características do setor: práticas de monitoramento para moderação de conteúdo, mecanismos de prevenção a fraudes e ferramentas de rastreamento de condutas suspeitas de lavagem de dinheiro operam, frequentemente, na linha tênue entre a proteção da privacidade e as demandas regulatórias do Estado. É exatamente nesse ponto de atrito que a atuação do controlador e do operador de dados requer maior sofisticação jurídica e técnica.

A Lei 9.613/1998, que define a regulamentação brasileira de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT), coloca as plataformas de jogos online em um marco normativo rigoroso, mesmo que muitas delas não tenham sido projetadas

inicialmente como instituições financeiras. As transações internas, a movimentação de ativos digitais, a comercialização de itens virtuais e a possibilidade de conversão econômica desses ativos geram fragilidades comuns em ambientes que favorecem o disfarce da origem ilegal de fundos.

Autores como Heleno Torres (2015), ao tratar do compliance financeiro, e penalistas como Pierpaolo Bottini (2013), Gustavo Badaró (2018) e Alexandre Wunderlich (2017) destacam que setores econômicos não convencionais - como os e-games - estão se integrando progressivamente às estruturas de controle financeiro do Estado. A lógica regulatória avança na direção de diminuir áreas de opacidade e ampliar os mecanismos de rastreabilidade.

Nesse cenário, as exigências impostas pelo COAF, evidenciadas em documentos como a Circular COAF n.º 01/2020, bem como os Guias de PLD/FT e as Resoluções do Banco Central, SUSEP e CVM, ganham destaque. Embora não sejam direcionadas especificamente ao setor de jogos, elas são utilizadas por analogia ou enquadramento quando as plataformas executam atividades semelhantes a serviços financeiros.

O COAF desempenha um papel crucial como unidade de inteligência financeira: ele recebe notificações de operações suspeitas e realiza o cruzamento de informações para detectar padrões anômalos. Isso destaca a importância de as plataformas possuírem sistemas internos de monitoramento capazes de registrar o comportamento do usuário, identificar transações atípicas e relatar ocorrências que possam indicar risco de lavagem.



Esse dever de comunicação, apesar de impactar diretamente a privacidade do usuário, possui fundamento na Constituição e na jurisprudência. No HC 598.051/SC (STJ, HC 598.051/SC, 2020), o STJ reafirmou a posição de que o rastreamento financeiro realizado pelo Estado não infringe o sigilo absoluto quando realizado dentro dos limites legais. Além disso, a Súmula Vinculante 24 do STF (STF, SV 24, 2009) destaca que a materialidade de crimes financeiros requer um lastro probatório mínimo, o que torna ainda mais importante a conformidade dos sistemas de registro e auditoria interna empregados pelos operadores de e-games.

Ainda não há um marco normativo único e unificado para regulamentar o mercado de e-games no que diz respeito à proteção de dados pessoais e prevenção à lavagem de dinheiro. O que se observa é uma interação entre instituições de diferentes órgãos. A ANPD supervisiona e orienta o manejo de dados (ANPD, 2021), ao passo que o COAF exige a vigilância e a notificação de operações suspeitas. Quando as plataformas conduzem transações financeiras

organizadas ou intermediadas, o Banco Central tem a capacidade de exercer autoridade regulatória adicional, implementando princípios de prevenção, identificação do cliente e rastreabilidade (BACEN, Resoluções PLD/FT).

Essa configuração híbrida enfatiza a necessidade de um marco regulatório sólido, capaz de conciliar o direito fundamental à privacidade - conforme argumentado por Doneda (2014), Mendes (2019), Bioni (2019) e Vainzof (2020) - com as exigências de conformidade previstas na legislação de PLD/FT.

Ao mesmo tempo, destaca que a privacidade no contexto dos jogos não pode ser entendida de forma isolada: ela está inserida em uma estrutura mais abrangente de segurança jurídica, integridade financeira e proteção dos usuários contra atividades ilegais.

## 4 DESAFIOS E SOLUÇÕES TECNOLÓGICAS

A introdução de tecnologias avançadas nos jogos online ampliou tanto as possibilidades de monitoramento quanto os riscos à privacidade e ao uso indevido de dados. As ferramentas como Inteligência Artificial (IA), sistemas de verificação de identidade (KYC) e análise de transações (KYT) tornaram-se centrais para a segurança dessas plataformas, sobretudo diante das exigências regulatórias de rastreabilidade e prevenção à lavagem de dinheiro. Ainda assim, seu uso exige análise crítica quanto a limites éticos, vieses e impactos sobre direitos fundamentais.



O debate sobre viés algorítmico ganha destaque nesse cenário. Cathy O'Neil adverte em Weapons of Math Destruction (2016) que sistemas automatizados podem reproduzir desigualdades e operar de forma opaca. Na mesma linha, Virginia Dignum (2019) defende que a aplicação da IA deve observar princípios como transparência, proporcionalidade e equidade, especialmente quando influencia decisões como bloqueios de contas ou identificação de operações suspeitas.

Conforme a perspectiva jurídica, estudiosos como Pedro Lenza, em Direito Constitucional Esquematizado (2024), e Ronaldo Lemos, especialmente em A Máquina do Caos (2020), sustentam que o uso da IA deve respeitar garantias constitucionais, como transparência e devido processo informacional. No contexto dos jogos online, isso implica assegurar que mecanismos de KYC e KYT atendam às exigências regulatórias sem promover coleta excessiva ou invasiva de dados. Normas como a Resolução da ANPD sobre segurança da informação, além de guias internacionais - como o Guia do Banco Central Europeu (BCE) sobre KYC

Digital (BCE, 2022), o Guia FinCEN de Verificação Eletrônica de Identidade (2020), e o AI Act europeu (EU AI Act, 2024) - oferecem parâmetros relevantes para estruturação dessas práticas.

O cenário se complexifica com o uso de criptoativos. A adoção de moedas digitais, tokens e itens tokenizados amplia o potencial econômico, mas também os riscos de anonimização e evasão regulatória. A descentralização das exchanges (operação de plataformas de negociação de criptoativos) e o uso de mixers, sidechains e carteiras de privacidade apresentam desafios significativos à rastreabilidade. Esse assunto já foi amplamente abordado por autores como Vitalik Buterin no Ethereum Whitepaper (2014), Don Tapscott em Blockchain Revolution (2016) e Fernando Ulrich em Bitcoin: A Revolução Digital do Dinheiro (2014). Esses autores ressaltam tanto o potencial transformador da blockchain quanto os desafios estruturais que ela enfrenta.

No Brasil, o Marco Legal das Criptomoedas (Lei 14.478/2022) e seus decretos regulamentadores do ano de 2023, definem diretrizes gerais para a operação de exchanges e provedores de serviços de ativos virtuais. No cenário internacional, o Guia de 2021 da FATF/GAFI para VASPs (2021) tem recomendado a várias jurisdições que implementem trilhas de auditoria e mecanismos de identificação do cliente, mesmo em contextos altamente descentralizados. Para plataformas de jogos online, isso implica equilibrar a dinâmica ágil dos ativos digitais com a exigência de sistemas eficientes de monitoramento, reporte e mitigação de riscos.



A combinação desses elementos demonstra que as soluções tecnológicas não devem ser implementadas de maneira irrefletida. Apesar de melhorarem a eficiência e a capacidade investigativa das plataformas, elas também elevam a responsabilidade jurídica dos operadores, demandando uma governança sólida, avaliações de impacto e conformidade com princípios éticos e regulatórios. Assim, o desafio consiste em desenvolver um ecossistema que empregue IA, KYC/KYT e blockchain como ferramentas de segurança e integridade, sem que isso converta o ambiente de jogo em um local de vigilância excessiva ou comprometimento da privacidade.

## 5 REGULAÇÃO INTERNACIONAL, COOPERAÇÃO E PADRÕES GLOBAIS

Ao mesmo tempo, a regulamentação global do mercado de jogos online apresenta um mosaico intrincado de modelos que tentam equilibrar, de várias formas, a proteção da privacidade dos usuários e as demandas de prevenção à lavagem de dinheiro. Na União

Europeia, a combinação do GDPR (Regulamento Geral de Proteção de Dados) com as diretivas de combate à lavagem de dinheiro - AMLD5 e AMLD6 - cria uma estrutura sólida que exerce uma influência significativa sobre o restante do mundo, conforme apontam estudiosos do direito digital europeu, como Chris Reed (2000) e Paul De Hert (2006). Já o Reino Unido, especialmente após o Brexit, reforçou a atuação conjunta entre o Gambling Act e as diretrizes da Financial Conduct Authority (FCA), criando um modelo de supervisão voltado tanto à integridade financeira quanto à proteção do consumidor.

Nos Estados Unidos, o FinCEN e o Bank Secrecy Act criam um esquema no qual operadores de jogos que trabalham com ativos conversíveis são tratados de maneira semelhante a instituições financeiras tradicionais, ampliando suas obrigações de monitoramento e comunicação de atividades suspeitas. Em contrapartida, regiões como Malta e Curaçao adotam abordagens mais flexíveis, tornando-se polos regulatórios que atraem plataformas globais, mas, simultaneamente, enfrentam críticas quanto a riscos de falta de clareza e desigualdade na supervisão.

Nesse cenário, o GAFI/FATF desempenha um papel central. Suas 40 Recomendações (particularmente as que dizem respeito ao setor privado e aos fornecedores de serviços digitais) servem como um padrão mínimo global de conformidade. Emile van der Does de Willebois (2011) e Tom Keatinge, do Royal United Services Institute (2014), ressaltam que a pressão do GAFI sobre os países para implementar mecanismos de prevenção mais rigorosos tem levado a mudanças nas leis em diversas jurisdições, incluindo nações com regulamentação historicamente mais flexível.



No entanto, a eficácia dessas regras se depara com desafios consideráveis devido ao caráter transnacional das plataformas, à descentralização das operações e à fragmentação das legislações. Para entender esse contexto, é fundamental adotar a perspectiva do direito transnacional, proposta por Philip Jessup (1956). Essa abordagem sugere que questões jurídicas que transcendem fronteiras nacionais exigem soluções que integrem normas internas, tratados internacionais e colaboração entre autoridades. De maneira semelhante, Anne-Marie Slaughter (2004) destaca que a cooperação entre agências reguladoras, unidades de inteligência financeira e autoridades de proteção de dados é um elemento essencial do enforcement global ao abordar as redes transgovernamentais.

Instrumentos internacionais multilaterais, como a Convenção de Palermo (2000), a Convenção de Mérida sobre corrupção e os acordos de assistência jurídica mútua (MLATs), são

essenciais para a troca de informações e viabilizam investigações que dependem da cooperação entre múltiplos países. Contudo, persistem desafios práticos: operadores em jurisdições permissivas, criptografia de ponta a ponta, utilização de mixers e plataformas descentralizadas dificultam a capacidade estatal de monitorar fluxos financeiros ilícitos.

Nesse contexto, estabelecer um ambiente regulatório global mais coeso exige não apenas a uniformização das regras, mas também a implementação de mecanismos mais eficientes para o compartilhamento de dados, padrões básicos de governança e o reforço das redes de colaboração internacional. Essa convergência se mostra especialmente urgente para o setor de jogos virtuais, pois somente um modelo sincronizado pode equilibrar de forma sustentável o direito à privacidade dos usuários e as exigências para minimizar riscos financeiros transfronteiriços.

## 6 ENTRE COERÊNCIA JURÍDICA E EFICIÊNCIA ECONÔMICA: PROPOSTAS PARA O BRASIL

Estabelecer um modelo regulatório eficiente para o setor de jogos online no Brasil requer não só uma interpretação conjunta da LGPD e da lei de prevenção à lavagem de dinheiro, mas também diretrizes normativas que demonstrem coerência, proporcionalidade e lógica econômica. Nesse processo, é fundamental entender que a proteção da privacidade e a rastreabilidade financeira não são valores opostos, mas aspectos que se complementam em um ecossistema digital seguro. A integração eficaz entre a LGPD e PLD/FT requer uma estrutura institucional que garanta tanto a proteção dos direitos fundamentais quanto a mitigação efetiva de riscos financeiros.



Do ponto de vista da teoria do direito, o conceito de integridade e coerência sistêmica proposto por Ronald Dworkin (1986) fornece um referencial significativo: regulações dispersas, sobrepostas ou contraditórias tendem a gerar assimetria de proteção, insegurança jurídica e baixa efetividade. No contexto brasileiro, isso significa que precisamos de uma regulamentação específica para e-games que esteja em consonância com os princípios da LGPD, além de atender às exigências da Lei 9.613/1998 e às diretrizes do COAF.

Por sua vez, a Análise Econômica do Direito pode ser usada para examinar a dimensão econômica da regulação, particularmente como Richard Posner (1998) a desenvolveu. A ausência de orientações precisas para identificação do usuário, auditoria das transações e mecanismos de due diligence ocasiona impactos negativos relevantes: aumenta o risco

sistêmico, reduz a confiança dos usuários e dificulta a entrada de operadores legítimos no mercado. Portanto, a definição de requisitos mínimos de compliance (como logs pseudonimizados, IA auditável, verificação de identidade proporcional ao risco e padrões mínimos de segurança), não é apenas uma formalidade, mas uma ferramenta para diminuir custos sociais e evitar que plataformas se transformem em áreas obscuras.

No âmbito regulatório, o conceito de "regulação adaptativa" proposto por Daniel Wang (2020) também fornece contribuições importantes para a criação de um modelo brasileiro mais eficaz. Em áreas de alta tecnologia, como jogos online, regras fixas rapidamente se tornam ultrapassadas. Assim, o ideal é implementar mecanismos de avaliação contínua, testes regulatórios (regulatory sandboxes) e atualizações normativas regulares, possibilitando que o sistema se mantenha atualizado em relação às novas práticas de mercado, modelos de monetização e tecnologias como IA generativa e blockchain.

Todavia, em relação à União Europeia e Reino Unido, o Brasil demonstra um atraso regulatório considerável. Ambos já dispõem de marcos regulatórios consolidados que englobam a proteção de dados, a regulação de jogos e o controle financeiro. Essa lacuna normativa gera impactos concretos: incidentes recentes vinculados a plataformas de apostas, fraudes e escândalos envolvendo criptomoedas evidenciam que a ausência de normas claras favorece abusos e causa prejuízos a consumidores e ao Estado, que enfrenta dificuldades de aplicação da lei e de acesso a informações.



Para avançar, o país deve estabelecer uma estratégia regulatória que inclua: (a) exigências específicas para operadores de jogos, levando em conta os riscos de microtransações, ativos digitais e interoperabilidade entre plataformas; (b) padrões mínimos obrigatórios de KYC/KYT; (c) auditorias regulares e certificação de sistemas; (d) mecanismos técnicos que garantam a privacidade desde a concepção (privacy by design) e priorizem a minimização de dados; e (e) colaboração efetiva entre ANPD, COAF e Banco Central para evitar falhas na supervisão.

Em resumo, a criação de um marco regulatório moderno e eficaz requer uma perspectiva que una a integridade jurídica (Dworkin, 1986), a racionalidade econômica (Posner, 1998) e a adaptabilidade institucional (Wang, 2020). Apenas com essa integração poderemos criar um modelo que equilibre de forma sustentável os direitos dos usuários, a integridade do sistema financeiro e o crescimento competitivo e seguro do mercado de jogos online no Brasil.

## 7 CONSIDERAÇÕES FINAIS

A análise realizada leva à conclusão de que o cenário dos jogos online é um dos ambientes mais complexos da agenda regulatória atual, pois envolve simultaneamente grandes volumes de dados pessoais, movimentação financeira intensa e mecanismos tecnológicos que facilitam a anonimização e descentralização. Nesse contexto, a privacidade e a prevenção à lavagem de dinheiro não são vistas como áreas opostas, mas como aspectos que se complementam de um único desafio: a construção de um ecossistema digital seguro, transparente e juridicamente consistente.

O estudo mostra que a LGPD fornece fundamentos robustos para a proteção do usuário e para a estruturação do tratamento de dados nessas plataformas. No entanto, sua efetividade depende da integração com a legislação de PLD/FT e com mecanismos de rastreabilidade adequados ao risco financeiro implicado. De maneira semelhante, a atuação de entidades como ANPD, COAF e Banco Central demonstra uma estrutura regulatória ainda desarticulada, que necessita de harmonização para lidar de forma eficaz com as práticas sofisticadas de lavagem de dinheiro que ocorrem no ambiente virtual.

Outro ponto essencial diz respeito às soluções tecnológicas. Ferramentas como Inteligência Artificial, KYC, KYT, análise comportamental e blockchain podem fortalecer significativamente o combate ao crime, contudo envolvem riscos ligados à vigilância exagerada, coleta excessiva de dados e atitudes discriminatórias. Por isso, devem ser implementadas fundamentadas nos princípios de proporcionalidade, necessidade e transparência, com avaliações periódicas de impacto e governança responsável.



Em conclusão, o caráter transnacional dos jogos online demanda uma abordagem igualmente transnacional para combatê-los. Nenhum país consegue, por conta própria, monitorar fluxos financeiros que cruzam fronteiras em milissegundos. A cooperação internacional, em conformidade com as orientações do GAFI, convenções multilaterais e redes transgovernamentais, é essencial para que os países não se tornem ineficazes frente à complexidade tecnológica atual.

Assim, é evidente que um modelo regulatório integrado, atualizado e tecnicamente avançado é a única maneira de equilibrar privacidade, rastreabilidade e combate à lavagem de dinheiro no setor de jogos online. Esse modelo deve integrar a proteção dos direitos fundamentais, eficiência econômica, mecanismos de compliance e cooperação internacional, estabelecendo um ambiente seguro e confiável para usuários, plataformas e Estado.

## REFERÊNCIAS

ANPD (Autoridade Nacional de Proteção de Dados). **Guia de segurança da informação.** Brasília, 2021. Disponível em: https://www.gov.br/anpd/. Acesso em: 9 jan. 2026.

ANSELMO, Márcio Adriano. **Lavagem de dinheiro e cooperação jurídica internacional.** São Paulo: Editora Saraiva, 2021.

BANCO CENTRAL DO BRASIL (BACEN). **Resoluções sobre prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD/FT).** Brasília, [s.d.]. Disponível em: https://www.bcb.gov.br/. Acesso em: 9 jan. 2026.

BADARÓ, Gustavo. **Curso de Processo Penal**. São Paulo: Revista dos Tribunais, 2018.

BARROSO, Luís Roberto. **A nova interpretação constitucional**. São Paulo: Saraiva, 2018.

BANCO CENTRAL EUROPEU (BCE). **Digital KYC guidelines.** Frankfurt, 2022. Disponível em: https://www.ecb.europa.eu/. Acesso em: 10 jan. 2026.

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

BLUM, Jack A. **Financial crime and money laundering.** Nova York: Routledge, 2016.

BOTTINI, Pierpaolo. **Lavagem de dinheiro.** São Paulo: Revista dos Tribunais, 2013.

BRASIL. Lei nº 14.790, de 29 de dezembro de 2023. **Dispõe sobre a regulamentação das apostas esportivas.** Disponível em: https://www.planalto.gov.br/. Acesso em: 15 jan. 2026.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. **Dispõe sobre diretrizes para a prestação de serviços de ativos virtuais.** Disponível em: https://www.planalto.gov.br/. Acesso em: 15 jan. 2026.

BUTERIN, Vitalik. **Ethereum Whitepaper**. 2014. Disponível em: https://ethereum.org/. Acesso em: 9 jan. 2026.

CALLEGARI, André. **Lavagem de dinheiro**. São Paulo: Atlas, 2020.

CONVENÇÃO DAS NAÇÕES UNIDAS CONTRA O CRIME ORGANIZADO TRANSNACIONAL (**Convenção de Palermo**). Decreto nº 5.015, de 12 de março de 2004. Disponível em: https://www.planalto.gov.br/. Acesso em: 10 jan. 2026.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (**COAF**). Circular nº 1, de 2020. Brasília, 2020. Disponível em: https://www.gov.br/coaf/. Acesso em: 9 jan. 2026.

CRESPO, Marcelo. **Direito digital**. São Paulo: Saraiva, 2021.

DE HERT, Paul. **European Data Protection Law Review**. 2006. Disponível em: https://www.lexxion.eu/. Acesso em: 11 jan. 2026.

DIGNUM, Virginia. **Responsible Artificial Intelligence.** London: Springer, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2014.

DWORKIN, Ronald. **Law's Empire**. Cambridge: Harvard University Press, 1986. Disponível em: https://www.hup.harvard.edu/. Acesso em: 9 jan. 2026.

EUROPEAN UNION. **AI Act – Artificial Intelligence Regulation**. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/. Acesso em: 17 jan. 2026.

FATF/GAFI. **Guidance for a Risk-Based Approach to Virtual Assets and VASPs**. Paris: FATF, 2021. Disponível em: https://www.fatf-gafi.org/. Acesso em: 9 jan. 2026.

FINCEN. **Electronic Identity Verification Guidelines**. Washington: FinCEN, 2020. Disponível em: https://www.fincen.gov/. Acesso em: 13 jan. 2026.

HERT, Paul de. **European Data Protection Law Review**. 2006. Disponível em: https://www.lexxion.eu/. Acesso em: 17 jan. 2026.

JESSUP, Philip. **Transnational Law.** New Haven: Yale University Press, 1956.

KEATINGE, Tom. **Reports on AML and Illicit Finance**. Londres: RUSI, 2014. Disponível em: https://rusi.org/. Acesso em: 13 jan. 2026.

LENZA, Pedro. **Direito Constitucional Esquematizado**. São Paulo: Saraiva, 2024.



LEMOS, Ronaldo. **A Máquina do Caos**. São Paulo: Companhia das Letras, 2020.

LEVI, Michael. **Money Laundering and Financial Crime**. Londres: Bloomsbury, 2018.

MARÇAL, C. H. P. **Temas de Direito Digital**. São Paulo, 2020.

MARCO CIVIL DA INTERNET. **Lei nº 12.965/2014**. Disponível em: https://www.planalto.gov.br/. Acesso em: 9 jan. 2026.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Revista dos Tribunais, 2019.

O'NEIL, Cathy. **Weapons of Math Destruction**. New York: Crown, 2016.

PLD/FT – **LEI DE LAVAGEM DE DINHEIRO**. Lei nº 9.613/1998. Disponível em: https://www.planalto.gov.br/. Acesso em: 10 jan. 2026.

POSNER, Richard A. **Economic analysis of law.** 5. ed. New York: Aspen Publishers, 1998.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**. 15. ed. São Paulo: Editora Revista dos Tribunais, 2017.

REALE, Christopher. **Temas de Direito e Tecnologia**. Lisboa, 2022.

REED, Chris. **Internet Law: Text and Materials**. Cambridge: Cambridge University Press, 2000.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 2015.

SLAUGHTER, Anne-Marie. **A new world order. Princeton: Princeton University Press**, 2004.

SLOAN, Anne-Marie. **A New World Order**. Princeton: Princeton University Press, 2004.

STF. **ADPF 695**. Brasília: STF, 2022. Disponível em: https://www.stf.jus.br/. Acesso em: 17 jan. 2026.

STF. **Súmula Vinculante 24**. Brasília, 2009. Disponível em: https://www.stf.jus.br/. Acesso em: 13 jan. 2026.

STF. **Tema 987 – RE 1010606**. Disponível em: https://www.stf.jus.br/. Acesso em: 10 jan. 2026.

STJ. **HC 598.051/SC**. Brasília, 2020. Disponível em: https://www.stj.jus.br/. Acesso em: 13 jan. 2026.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**. New York: Penguin, 2016.

TORRES, Heleno Taveira. **Tributação e Direito Financeiro**. São Paulo, 2015.

ULRICH, Fernando. **Bitcoin: A Revolução Digital do Dinheiro**. São Paulo: Instituto Mises, 2014.



UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (**General Data Protection Regulation – GDPR**). 2016. Disponível em: https://gdpr.eu/. Acesso em: 25 jan. 2026.

UNIÃO EUROPEIA. **Diretivas AMLD5 e AMLD6 – combate à lavagem de dinheiro**. Bruxelas, [s.d.]. Disponível em: https://eur-lex.europa.eu/. Acesso em: 25 jan. 2026.

VAINZOF, Rony. **Segurança da informação e proteção de dados**. São Paulo: Saraiva, 2020.

WANG, Daniel Wei Liang. **Regulação e uso de evidências: desafios para a adaptação institucional**. São Paulo: Fundação Getulio Vargas, 2020.

WILLEBOIS, Emile van der Does de. **The Puppet Masters**. Washington: World Bank, 2011.

WUNDERLICH, Alexandre. **Lavagem de Dinheiro e Compliance Penal**. Porto Alegre, 2017.