AMANDA MARIA MOTA TAVARES
HIGOR VINICIUS NOGUEIRA JORGE

BLOCKCHAIN NO DIREITO E NA SEGURANÇA PÚBLICA

Prova Digital, Registros, Identidade e Governança Tecnológica

2026

EDITORA JusPODIVM
www.editorajuspodivm.com.br

CAPÍTULO 14

PIRATARIA DIGITAL E MEDIDAS DE REPRESSÃO

Investigação, prova digital, cooperação com plataformas e resposta institucional

Higor Vinicius Nogueira Jorge

14.1. A MUTAÇÃO DA PIRATARIA NO ECOSSISTEMA DIGITAL

A pirataria digital já não pode ser compreendida apenas como reprodução clandestina de arquivos isolados. O fenômeno contemporâneo se aproxima muito mais de uma economia ilícita de acesso, estruturada por serviços, fluxos recorrentes de monetização e arquitetura tecnológica adaptável. A antiga centralidade do download individual perdeu terreno para ecossistemas mais dinâmicos, baseados em streaming irregular, IPTV ilícita, reencaminhamento de transmissões ao vivo, aplicativos não autorizados, serviços de hospedagem opacos, redirecionamentos em cadeia e espelhamento veloz de domínios. Em vez de uma infração episódica, vê-se hoje uma engrenagem contínua, orientada por escala, resiliência e capacidade de recomposição após ações de contenção (EUIPO, 2024; EUIPO; Europol, 2022).

Essa transformação altera também a forma de ler juridicamente o problema. A pirataria contemporânea não opera apenas na margem do sistema legítimo; ela imita sua lógica operacional. Há

interface amigável, curadoria de catálogo, ofertas por assinatura, publicidade segmentada, canais de suporte, reconfiguração de acesso e estratégias de fidelização. O ilícito, portanto, não se apresenta mais apenas como cópia grosseira, mas como serviço parasitário que explora a familiaridade do usuário com a economia do acesso instantâneo. É justamente essa semelhança funcional com o mercado regular que torna a repressão mais desafiadora e, ao mesmo tempo, mais dependente de inteligência tecnológica e resposta coordenada (Interpol, 2026a; EUIPO, 2025).

Em tal cenário, a repressão puramente reativa revela-se insuficiente. O bloqueio tardio de um endereço, a remoção pontual de um arquivo ou a identificação isolada de um usuário final podem produzir impacto modesto quando confrontados com estruturas que trocam rapidamente de domínio, replicam espelhos, terceirizam partes da operação e se apoiam em múltiplos intermediários técnicos. A resposta institucional efetiva exige compreender a pirataria como ecossistema, e não como ato singular. Isso significa olhar simultaneamente para conteúdo, infraestrutura, monetização, rastros técnicos, fluxos transnacionais e capacidade de reiteração (WIPO, 2025a; EUIPO, 2023).

14.2. MODALIDADES CONTEMPORÂNEAS E RACIONALIDADE ECONÔMICA DO ILÍCITO

As modalidades atuais de pirataria variam, mas guardam um traço comum: procuram reduzir atrito para o consumidor e aumentar a durabilidade do negócio ilícito. O streaming irregular de obras audiovisuais continua relevante, mas passou a conviver com modelos mais agressivos de retransmissão em tempo real, especialmente em eventos esportivos e outras transmissões de valor concentrado no instante. Ao lado disso, subsistem serviços de download indireto, plataformas de compartilhamento, aplicações não oficiais, listas IPTV clandestinas, softwares de ripping e circuitos híbridos que combinam repositórios, canais de distribuição em redes sociais e mecanismos automáticos de redirecionamento. O mercado ilícito, em suma, diversificou-se tecnicamente para reduzir dependência de um único canal e preservar a continuidade do acesso mesmo sob pressão repressiva (EUIPO, 2024; EUIPO, 2023).

Essa diversificação é acompanhada por uma racionalidade econômica bastante sofisticada. A pirataria digital não se sustenta apenas por gratuidade aparente ao usuário. Ela pode ser monetizada por publicidade, assinaturas informais, doações, marketing de afiliação, exploração abusiva de dados e outros mecanismos de captura de valor. A Interpol observa que serviços piratas geram receita por anúncios, contribuições financeiras, planos pagos, revenda de dados e direcionamento do usuário a outros serviços, enquanto a EUIPO tem demonstrado que websites infratores e de alto risco continuam inseridos em cadeias relevantes de publicidade digital e intermediação comercial (Interpol, 2026a; EUIPO, 2025). O ponto central é simples: quem investiga pirataria digital sem seguir o dinheiro vê apenas a superfície do problema.

Há ainda um aspecto estrutural importante. O ambiente ilícito tornou-se altamente adaptativo. A EUIPO registra que websites piratas vêm apresentando maior nível de churn, com redirecionamentos automáticos, domínios substitutos e espelhos que surgem como resposta a medidas de bloqueio e contenção (EUIPO, 2025). Isso significa que a persistência do ilícito já não depende da permanência de uma página específica, mas da manutenção de uma malha de acesso. Em consequência, a repressão eficiente não pode mirar apenas o endereço visível no momento da constatação. É preciso enxergar a infraestrutura de continuidade: mirrors, domínios correlatos, aplicações associadas, serviços de hospedagem, redes de distribuição de conteúdo, intermediários de pagamento e circuitos de aquisição de audiência.

14.3. PIRATARIA DIGITAL, CIBER-RISCO E CRIMINALIDADE ORGANIZADA

Um dos erros mais recorrentes na análise pública da pirataria digital é tratá-la como ilícito de baixa densidade ofensiva, quase como simples "atalho" de consumo. Essa imagem é tecnicamente pobre e empiricamente enganosa. A documentação recente da Europol e da Interpol mostra que a pirataria digital pode estar associada a malware, cryptojacking, fraude, lavagem de dinheiro, publicidade abusiva e outras cadeias criminosas mais amplas. Em outras palavras, o ambiente pirata não representa apenas perda econômica para o titular; ele pode funcionar como ponto de entrada para outros mercados

ilícitos, multiplicando riscos para usuários, empresas e autoridades (EUIPO; Europol, 2022; Interpol, 2026b).

A Interpol adverte, por exemplo, que sites e serviços piratas podem expor consumidores a roubo de identidade, fraude financeira, coleta indevida de dados e conteúdo malicioso, além de servirem como fonte de receitas para grupos criminosos que operam em múltiplos segmentos ilícitos (Interpol, 2026a). A Europol, por sua vez, destaca que a pirataria de conteúdo digital se liga, em alguns casos, à distribuição de malware e ao uso de contramedidas técnicas avançadas para ocultar rastros e manter redes de hospedagem resilientes (EUIPO; EUROPOL, 2022). A soma desses fatores muda a chave de leitura do problema: a pirataria digital não é apenas ofensa patrimonial difusa, mas também vetor de insegurança cibernética e de financiamento criminal.

Isso tem duas consequências práticas. A primeira é que a repressão não deve se limitar ao conteúdo ilícito circulante, mas precisa atingir a organização econômica que o sustenta. A segunda é que a resposta investigativa exige integração entre direito autoral, inteligência financeira, análise de infraestrutura digital e cooperação internacional. O operador que observa apenas a obra pirateada tende a perder de vista o modelo de negócio clandestino. E, muitas vezes, é justamente esse modelo – mais do que o arquivo ou o stream individual – que sustenta a permanência do dano em escala.

14.4. PROVA DIGITAL E RECONSTRUÇÃO DO ECOSSISTEMA INFRATOR

A investigação da pirataria digital depende de uma premissa metodológica elementar: conteúdo ilícito online é evidência instável. Ele pode ser apagado, deslocado, comprimido, reapresentado em outro domínio, encapsulado em aplicativo diferente ou reaparecer sob nova identidade visual em intervalo muito curto. Por isso, o êxito repressivo está menos na intuição sobre a ilicitude e mais na qualidade da preservação probatória. O NIST observa que a preservação de evidência digital apresenta problemas próprios, porque o valor jurídico frequentemente reside no conteúdo e nas informações relacionadas a ele, e não apenas no suporte físico, sendo essencial registrar adequadamente arquivos, objetos digitais e contextos remotos ou em nuvem (NIST, 2022).

Aplicada à pirataria digital, essa premissa significa que a prova útil raramente se resume à captura de tela. O material probatório relevante costuma incluir o arquivo disponibilizado ou transmitido, a URL ou sequência de URLs envolvidas, data e hora da coleta, metadados remanescentes, respostas de servidor, eventuais registros de cabeçalho, identificadores de conta, anúncios veiculados, meios de pagamento associados, vínculos entre domínios, arquivos de playlist, rastros de distribuição e documentação da cadeia de preservação. A evidência não deve provar apenas que o conteúdo apareceu; deve permitir reconstruir como ele apareceu, por quem foi oferecido, por quais meios foi monetizado e que conexões técnicas mantinha com outros pontos da estrutura ilícita.

Esse cuidado é ainda mais relevante quando a operação se vale de serviços voláteis, hospedagem distribuída ou aplicações de acesso indireto. Nesses casos, a distinção entre conteúdo, infraestrutura e intermediação torna-se central. Em uma página pirata, por exemplo, a transmissão visível ao usuário pode depender de múltiplos agentes: operador do site, provedor de hospedagem, rede de distribuição, plataforma de anúncios, serviço de redirecionamento, processador de pagamento e, em alguns casos, aplicativo de terceiros. A prova robusta precisa mapear esse arranjo. A investigação fraca se satisfaz com a aparência frontal do site; a investigação tecnicamente madura reconstitui a cadeia de suporte do ilícito.

Ferramentas tecnológicas podem ampliar enormemente essa capacidade de reconstrução. A WIPO descreve soluções que combinam inteligência artificial, aprendizado de máquina, automação, reconhecimento de imagem e vídeo, e coleta automatizada de inteligência em fontes abertas para detectar, confirmar e responder a incidentes de pirataria em tempo real. Entre os elementos reconhecíveis por essas soluções estão logotipos, marcas d'água, placares, publicidade veiculada e outros sinais de vinculação com a transmissão ilícita (WIPO, 2025b). Isso mostra que a investigação contemporânea da pirataria não se limita à busca manual de conteúdos; ela demanda correlação automatizada, validação humana e documentação rigorosa do método empregado.

Há, contudo, uma cautela importante. O uso de tecnologia de detecção não substitui a necessidade de explicação clara do caminho probatório. Ferramentas automáticas podem localizar padrões,

mas a persuasão jurídica do resultado continua a depender de demonstração compreensível: qual conteúdo foi identificado, por que se entendeu que era ilícito, que elementos objetivos confirmaram a correspondência com a obra ou transmissão protegida, como os dados foram preservados e quais limitações técnicas o método apresenta. Em matéria de prova digital, o poder da ferramenta não dispensa o dever de fundamentação.

14.5. COOPERAÇÃO COM INTERMEDIÁRIOS E MEDIDAS DE CONTENÇÃO

A repressão à pirataria digital tornou-se inseparável da cooperação com intermediários. Isso não decorre de uma simples transferência de deveres ao setor privado, mas de uma constatação técnica: boa parte das medidas aptas a interromper ou reduzir o dano depende de agentes situados entre o operador ilícito e o usuário final. Provedores de acesso, serviços de hospedagem, redes de distribuição, mecanismos de busca, lojas de aplicativos, plataformas de anúncios e processadores de pagamento ocupam posições estratégicas na cadeia de circulação. Ignorar essa arquitetura significa insistir em uma repressão que alcança menos do que poderia.

Nesse contexto, o bloqueio de acesso passou a ocupar papel relevante. Os documentos recentes da WIPO indicam que o bloqueio de sites piratas por intermediários tornou-se um dos remédios mais difundidos no enfrentamento da pirataria online e que, quando estruturado com salvaguardas adequadas, pode reduzir tráfego para websites infratores e aumentar o uso de serviços legítimos (WIPO, 2025a; WIPO, 2025c). A discussão tecnicamente séria, porém, não está em saber se o bloqueio existe, mas em que condições se justifica. A experiência comparada aponta para alguns parâmetros recorrentes: efetividade real, proporcionalidade, proteção de conteúdos legítimos, inexistência de monitoramento geral indiscriminado e possibilidade de resposta suficientemente rápida diante da mutação do ecossistema pirata (EUIPO, 2021; EUIPO, 2023).

Essa última dimensão – a rapidez – é particularmente crítica em transmissões ao vivo. Quando o valor econômico do conteúdo se concentra no momento da exibição, a remoção tardia já não preserva adequadamente o bem jurídico atingido. É por isso que a literatura recente sobre live event piracy insiste na necessidade de

respostas ágeis, combinando ordens dinâmicas, atualização de listas de bloqueio, atuação de autoridades especializadas e cooperação operacional entre titulares e intermediários (EUIPO, 2023; WIPO, 2025c). Em tais hipóteses, o tempo deixa de ser detalhe procedimental e passa a ser parte do próprio mérito da tutela.

Ao lado do bloqueio, a contenção econômica ganhou protagonismo. Se a pirataria digital funciona como negócio, a repressão eficiente precisa afetar seu fluxo de receita. A cooperação com intermediários de publicidade e pagamento cumpre exatamente esse papel. A Interpol registra que associações antipirataria e titulares trabalham com provedores de pagamento para interromper o fluxo financeiro dos serviços piratas, enquanto a EUIPO demonstra que websites infratores continuam captando receitas publicitárias significativas por meio de complexas cadeias de intermediação (Interpol, 2026a; EUIPO, 2025). A desmonetização, portanto, não é medida acessória; é técnica de sufocamento estrutural do ilícito.

Há ainda a frente dos aplicativos e serviços correlatos. Documentos recentes discutidos na WIPO mostram que lojas de aplicativos e ambientes digitais já vêm exigindo mecanismos de denúncia, filtragem, bloqueio e resposta a usos indevidos em determinados contextos, especialmente quando o serviço favorece ou estimula infrações (WIPO, 2025d). Isso reforça um dado essencial: a repressão à pirataria digital não se resolve apenas na página final onde o conteúdo aparece, mas em toda a cadeia que permite a descoberta, o acesso, a cobrança e a persistência do serviço ilícito.

14.6. REPRESSÃO INTELIGENTE: ENTRE O BLOQUEIO VISÍVEL E A INVESTIGAÇÃO PATRIMONIAL

A medida repressiva mais visível costuma ser a remoção ou o bloqueio. Mas as estratégias mais eficazes são, em regra, mais amplas. O enfrentamento da pirataria digital em escala demanda atuação simultânea em pelo menos três planos: contenção do acesso, disrupção da infraestrutura e rastreamento patrimonial. O primeiro reduz a fruição imediata do conteúdo ilícito. O segundo dificulta a resiliência técnica do esquema. O terceiro procura atingir o incentivo econômico que torna o negócio repetível. Reprimir apenas o acesso é como fechar a vitrine e preservar intacto o caixa.

A cooperação internacional é componente inevitável dessa equação. A INTERPOL, por meio do projeto I-SOP, enfatiza exatamente a necessidade de fortalecer troca de informações, análise de inteligência, derrubada de websites e servidores, desarticulação de redes criminosas e focalização de ativos vinculados à pirataria digital (INTERPOL, 2026b). A razão é evidente. Operadores, domínios, hospedagem, anunciantes, meios de pagamento e serviços técnicos podem estar dispersos em várias jurisdições, o que reduz a efetividade de respostas exclusivamente locais. Em ilícitos digitais, o território do dano raramente coincide com o território da operação.

Também se tornou claro que repressão inteligente exige priorização. Nem toda infração online representa o mesmo grau de complexidade, dano ou organização. Há casos de disponibilização episódica e de baixa escala; há, em sentido diverso, estruturas profissionais que comercializam acesso, terceirizam infraestrutura, operam com múltiplos espelhos e mantêm mecanismos de financiamento estáveis. A alocação racional de recursos investigativos pede diferenciação entre essas hipóteses. Investigar com profundidade organizadores, financiadores, operadores técnicos e reincidentes qualificados tende a produzir efeito sistêmico superior ao obtido com ações pulverizadas e de baixo impacto estratégico.

Nesse ponto, convém registrar uma hipótese alternativa relevante, para evitar viés de confirmação. Nem todo fluxo suspeito de transmissão irregular decorre imediatamente de uma organização pirata estruturada. Pode haver, por exemplo, redistribuição oportunista feita por usuário individual, conflito contratual sobre escopo territorial de licença, uso indevido de credenciais de assinante legítimo ou reencaminhamento automatizado por serviço intermediário sem plena consciência do conteúdo circulante. O indício que pode sustentar essas hipóteses alternativas está, muitas vezes, na precariedade técnica da operação, na ausência de monetização organizada, na curta duração do evento ou na inexistência de vínculos entre múltiplos domínios e contas. A diligência apta a confirmá-las ou afastá-las passa pela correlação entre infraestrutura, recorrência, monetização, volume de tráfego, logs disponíveis e histórico de reincidência. Em investigação tecnológica, pressupor organização criminosa antes de mapear o ecossistema é trocar método por ansiedade.

A repressão proporcional, portanto, não é leniência. É técnica. Significa escolher medidas compatíveis com o grau de organização do ilícito, preservar evidência antes de interromper canais críticos quando isso for viável, evitar dano colateral indevido a conteúdos legítimos e concentrar o esforço estatal nos pontos de maior alavancagem: repetidores profissionais, provedores conscientemente integrados ao esquema, fluxos de monetização e operadores que convertem pirataria em serviço continuado.

14.7. CONSIDERAÇÕES FINAIS

A pirataria digital contemporânea deixou de ser simples problema de cópia não autorizada para se tornar um problema de infraestrutura ilícita de acesso. Seu núcleo já não está apenas na obra reproduzida, mas na combinação entre tecnologia de distribuição, monetização opaca, resiliência arquitetônica e exploração parasitária da lógica de consumo sob demanda. Quem analisa apenas o arquivo pirateado vê pouco. Quem examina a rede de suporte do ilícito compreende melhor o fenômeno e decide com mais precisão.

Daí a insuficiência de respostas unidimensionais. Nem a remoção isolada resolve o problema, nem a repressão penal simbólica, desacompanhada de prova técnica e investigação patrimonial, produz efeito consistente. A experiência recente aponta para um modelo mais sofisticado: preservação rigorosa da evidência digital, uso criterioso de ferramentas tecnológicas de detecção, cooperação com intermediários, bloqueio proporcional e adaptativo, desmonetização do serviço ilícito, compartilhamento internacional de inteligência e foco nos operadores que transformam a infração em negócio recorrente (NIST, 2022; WIPO, 2025a; Interpol, 2026b).

A conclusão prática é direta. Em matéria de pirataria digital, reprimir bem significa enxergar o ilícito como ecossistema. Isso implica sair da superfície do conteúdo disponível e penetrar em sua cadeia de sustentação: domínios, espelhos, anúncios, pagamentos, hospedagem, aplicações, redes de distribuição e agentes de reincidência. A boa repressão não é a que apenas reage ao sintoma mais visível, mas a que desorganiza a estrutura que o reproduz.

REFERÊNCIAS DO CAPÍTULO

EUIPO. *Live Event Piracy*: Discussion Paper. Alicante: European Union Intellectual Property Office, 2023. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Live_Event_Piracy/2023_Live_Event_Piracy_Discussion_Paper_FullR_en.pdf. Acesso em: 9 mar. 2026.

EUIPO. *Online advertising on IPR infringing websites and apps 2024*. Alicante: European Union Intellectual Property Office, 2025. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2025_Online_Advertising_on_IRP_Infringing_websites/Online_advertising_on_IPR_Infringing_Websites_and_Apps_FullR_en.pdf. Acesso em: 9 mar. 2026.

EUIPO. *Online copyright infringement in the European Union* – films, music, publications, software and TV (2017-2023). Alicante: European Union Intellectual Property Office, 2024. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_online_copyright_infringement/2024_online_copyright_infringement_in_the_EU_FullR_en.pdf. Acesso em: 9 mar. 2026.

EUIPO. *Study on Dynamic Blocking Injunctions in the European* Union. Alicante: European Union Intellectual Property Office, 2021. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Dynamic_Blocking_Injuctions/2021_Study_on_Dynamic_Blocking_Injuctions_in_the_European_Union_FullR_en.pdf. Acesso em: 9 mar. 2026.

EUIPO; EUROPOL. *Intellectual Property Crime Threat Assessment 2022*. Alicante: European Union Intellectual Property Office; The Hague: Europol, 2022. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf. Acesso em: 9 mar. 2026.

INTERPOL. *Digital piracy*. Lyon: INTERPOL, 2026a. Disponível em: https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Digital-piracy. Acesso em: 9 mar. 2026.

INTERPOL. *Project I-SOP*. Lyon: INTERPOL, 2026b. Disponível em: https://www.interpol.int/Crimes/Illicit-goods/Projects/Project-I-SOP. Acesso em: 9 mar. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Digital Evidence Preservation*: Considerations for Evidence Handlers. Gaithersburg: NIST, 2022. Disponível em: https://doi.org/10.6028/NIST.IR.8387. Acesso em: 9 mar. 2026.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Sharing experiences and best practices on site blocking and no-fault injunctions*. Geneva: WIPO, 2025a. Disponível em: https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_14_prov.pdf. Acesso em: 9 mar. 2026.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Technological tools in combatting digital piracy and counterfeiting*. Geneva: WIPO, 2025b. Disponível

em: https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_17_prov.pdf. Acesso em: 9 mar. 2026.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Study on the effectiveness and the legal and technical methods used to support the implementation of site blocking orders.* Geneva: WIPO, 2025c. Disponível em: https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_13.pdf. Acesso em: 9 mar. 2026.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Advisory Committee on Enforcement.* Geneva: WIPO, 2025d. Disponível em: https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_12.pdf. Acesso em: 9 mar. 2026.

CAPÍTULO 15

RESPONSABILIDADE DE PROVEDORES DE INTERNET E PLATAFORMAS

Governança da circulação, preservação de registros e valor probatório dos ambientes digitais

Higor Vinicius Nogueira Jorge

15.1. O PROBLEMA CORRETO: PLATAFORMAS NÃO SÃO APENAS CANAIS, MAS INFRAESTRUTURAS DE CIRCULAÇÃO E PROVA

A responsabilidade de provedores de internet e plataformas digitais já não pode ser pensada apenas a partir da velha pergunta sobre quem publicou o conteúdo originário. Essa formulação, embora ainda relevante, tornou-se insuficiente para explicar o papel que os intermediários desempenham no ecossistema informacional contemporâneo. As plataformas não apenas armazenam, transportam ou exibem conteúdos. Elas organizam visibilidade, modulam alcance, administram denúncias, automatizam recomendações, preservam ou apagam rastros, definem padrões de acesso, monetizam fluxos e, em muitos casos, condicionam a própria possibilidade de reconstrução probatória do que ocorreu no ambiente digital.

Esse deslocamento é especialmente importante para uma obra voltada a blockchain, provas, registros e smart contracts. No plano prático, a responsabilidade das plataformas interessa menos como debate abstrato sobre culpa e mais como tema ligado à governança de registros. Quem controla a infraestrutura de publicação, indexação, ranqueamento, remoção, desindexação, monetização e guarda de eventos digitais controla, em boa medida, a qualidade da memória técnica do conflito. Em ambiente de rede, a responsabilidade do intermediário não se mede apenas pela permanência do conteúdo ilícito, mas também por sua atuação na formação, manutenção ou perda da trilha informacional que permitirá posterior auditoria.

É por isso que uma análise madura do tema deve abandonar a imagem simplificadora da plataforma como "espaço neutro". Em muitos casos, o intermediário atua como verdadeiro gestor da circulação. Ele seleciona, hierarquiza, recomenda, oculta, impulsiona, desacelera, remunera e registra. Sua relevância jurídica decorre, precisamente, dessa posição arquitetônica. O problema contemporâneo não está apenas em saber se o intermediário respondeu ou não por conteúdo de terceiro, mas em identificar quais deveres de diligência, transparência, documentação e cooperação recaem sobre quem ocupa posição estrutural na cadeia digital.

Essa chave de leitura é ainda mais útil quando se examinam infrações complexas, como circulação de material pirateado, fraude por perfis falsos, comércio digital ilícito, deepfakes, apps maliciosos, desinformação operacionalizada por automação e violações de propriedade intelectual em múltiplas camadas. Nesses cenários, o conteúdo visível ao usuário costuma ser apenas a face mais aparente de um arranjo técnico maior. A resposta jurídica eficiente depende, portanto, menos de slogans sobre neutralidade e mais de análise funcional sobre poderes, deveres e rastros.

15.2. TIPOLOGIA FUNCIONAL DOS INTERMEDIÁRIOS E GRADAÇÃO DE RESPONSABILIDADE

Um dos primeiros erros metodológicos em matéria de responsabilidade de provedores é tratar todos os intermediários como se desempenhassem o mesmo papel. O ambiente digital contemporâneo é formado por agentes funcionalmente distintos: provedores de acesso, serviços de hospedagem, computação em nuvem,

mecanismos de busca, marketplaces, redes sociais, serviços de mensageria, plataformas de vídeo, lojas de aplicativos, redes de distribuição de conteúdo, gateways de pagamento e outros atores que operam em posições específicas dentro da cadeia técnica. A responsabilidade juridicamente bem construída precisa levar em conta essa diferença de função.

Essa premissa é importante porque o poder de interferência varia enormemente entre os intermediários. Há agentes cuja atuação é predominantemente instrumental, voltada ao transporte ou ao suporte técnico. Há outros que organizam o encontro entre oferta e demanda, exploram economicamente a visibilidade do conteúdo, definem termos de uso, promovem publicidade e executam políticas internas de moderação. Há, ainda, ambientes híbridos, em que uma mesma empresa acumula hospedagem, recomendação, processamento de pagamentos, publicidade e retenção de dados. Em tais hipóteses, a análise funcional é superior a qualquer classificação nominal rígida.

A consequência prática é direta. Quanto maior o poder de organização do ambiente, de intervenção sobre fluxos de circulação e de preservação de registros, maior tende a ser a densidade dos deveres de diligência esperados do intermediário. Isso não significa impor obrigação impossível de controle absoluto, nem converter plataformas em órgãos estatais paralelos. Significa reconhecer que a responsabilidade não pode ser desligada da arquitetura de poder exercida sobre o ecossistema. Quem apenas transmite não se confunde com quem recomenda; quem apenas aloja não se confunde com quem monetiza; quem apenas fornece armazenamento bruto não se confunde com quem audita e modera o conteúdo.

Essa diferenciação também é útil para o campo probatório. Uma rede social, por exemplo, não interessa apenas pelo conteúdo postado. Interessa pelo histórico de criação da conta, pelos metadados de upload, pelos registros de denúncia, pela cronologia de impulsionamento, pelos eventos de moderação, pelos vínculos com meios de pagamento e por eventuais integrações com serviços externos. Uma loja de aplicativos, por sua vez, interessa não só porque distribui software, mas porque pode reter documentação sobre submissão, revisões, permissões solicitadas, atualizações, remoções e

justificativas técnicas. A plataforma, portanto, não é apenas veículo; é fonte de contexto.

15.3. MODERAÇÃO, RECOMENDAÇÃO ALGORÍTMICA E DEVERES DE TRANSPARÊNCIA

A responsabilidade das plataformas tornou-se inseparável da discussão sobre moderação e recomendação algorítmica. O debate público frequentemente se concentra na remoção de conteúdos, mas a questão é mais ampla. Em ambientes digitais de grande escala, a plataforma não participa do resultado social apenas quando retira ou mantém uma publicação. Ela também participa quando decide o que amplificar, o que recomendar, a quem mostrar, com que prioridade, por quanto tempo e sob quais critérios. O problema jurídico contemporâneo, assim, já não se limita à permanência do conteúdo; alcança sua circulação qualificada.

Essa constatação impõe uma mudança de enfoque. Plataformas não podem ser analisadas apenas como repositórios, mas como sistemas de decisão. Mesmo quando a decisão é parcialmente automatizada, ela continua a produzir efeitos humanos, econômicos e jurídicos relevantes. Daí a centralidade crescente das exigências de transparência, accountability e explicabilidade mínima dos processos de moderação e recomendação. O ponto não é exigir exposição completa de segredos empresariais ou engenharia integral do sistema, mas assegurar inteligibilidade institucional suficiente para permitir controle, contestação e auditoria.

A opacidade algorítmica produz efeitos jurídicos concretos. Se o usuário desconhece por que seu conteúdo foi suprimido, rebaixado, desmonetizado ou impulsionado; se a vítima não consegue compreender por que uma denúncia foi ignorada; se a autoridade não consegue identificar a trilha decisória que levou à recomendação massiva de conteúdo nocivo; então a própria ideia de responsabilidade se torna precária. Responsabilizar exige compreender. E compreender, no ambiente digital, exige algum grau de abertura sobre regras de funcionamento, categorias de classificação, parâmetros de intervenção e mecanismos de revisão.

Essa exigência se torna ainda mais relevante em contextos de conteúdo ilícito massivamente escalável, como pirataria digital,