



## A CAIXA DE PANDORA ALGORÍTMICA: INTELIGÊNCIA ARTIFICIAL, MERCADO FINANCEIRO E ILÍCITOS PENAIS ECONÔMICOS

Diana Izis Coletto Reis  
Francieli Korquevicz Morbini

### Resumo

Na mitologia grega, a Caixa de Pandora, ao ser aberta, liberou todos os males para o mundo, deixando apenas a esperança em seu interior. No mercado financeiro contemporâneo, a Inteligência Artificial (IA) tem um papel análogo, permitindo a análise de vastos dados e a execução de operações em tempo real, mas também sendo suscetível a ilícitos penais econômicos, como manipulação de algoritmos, uso indevido de informação privilegiada (*insider trading*) e lavagem de dinheiro digital. O desafio é regulamentar e responsabilizar condutas ilícitas mediadas por IA, um debate que exige o enfrentamento dos conceitos tradicionais de autoria e dolo. Este artigo, por meio de revisão bibliográfica e pesquisa documental, analisa os riscos e os desafios do Direito Penal Econômico frente a essas novas tecnologias. Conclui-se que a adaptação das normas é essencial para garantir a proteção da ordem econômica, agindo como a "esperança" que contém os "males" liberados pela IA, exigindo a responsabilização de pessoas físicas e jurídicas, notadamente aquelas que desenvolvem ou utilizam a tecnologia.

**Palavras-chave:** inteligência artificial; direito penal econômico; mercado financeiro; ilícitos; caixa de pandora; responsabilidade penal

### Abstract

In Greek mythology, Pandora's Box, when opened, released all evils into the world, leaving only hope inside. In the contemporary financial market, Artificial Intelligence (AI) plays an analogous role, enabling the analysis of vast data and the execution of real-time operations, but also being susceptible to economic criminal offenses, such as algorithm manipulation, misuse of privileged information (*insider trading*), and digital money laundering. The challenge lies in regulating and establishing liability for illicit conduct mediated by AI, a debate that demands confronting traditional concepts of authorship and intent (*dolus*). This article, through bibliographic review and documentary research, analyzes the risks and challenges of Economic Criminal Law against these new technologies. It is concluded that adapting regulations is essential to ensure the

protection of the economic order, acting as the "hope" that contains the "evils" released by AI, requiring the accountability of individuals and legal entities, particularly those who develop or use the technology.

**Keywords:** artificial intelligence; economic criminal law; financial market; illicit acts; pandora's box; criminal liability

## INTRODUÇÃO

A revolução tecnológica no mercado financeiro, impulsionada pela Inteligência Artificial (IA), alterou profundamente a dinâmica das transações, oferecendo um potencial de eficiência e lucratividade inédito. No entanto, essa mesma tecnologia representa a abertura de uma "Caixa de Pandora Algorítmica", liberando uma série de vulnerabilidades e novos padrões de ilícitos penais econômicos. A IA, ao processar dados em velocidade e volume inatingíveis à capacidade humana, tornou-se uma ferramenta de dupla face: um motor de inovação e um facilitador para crimes sofisticados, como a manipulação de mercado por algoritmos de alta frequência (high-frequency trading) e a lavagem de capitais por meio de ativos digitais.

O escopo desta pesquisa reside na urgência de o Direito Penal Econômico brasileiro e internacional responderem à crescente complexidade desses crimes algorítmicos. Os mecanismos criminosos atuais desafiam conceitos fundamentais de autoria, causalidade e dolo, uma vez que a conduta ilícita pode ser o resultado de uma interação não inteiramente prevista entre o programador, o usuário e a decisão autônoma do algoritmo.

A justificativa para este estudo é a necessidade de mapear os novos riscos e as incertezas jurídicas criadas pela IA no ambiente de capitais. A ordem econômica, bem jurídico tutelado pelas normas penais, está diretamente ameaçada pela opacidade (black box) e pela velocidade com que os crimes podem ser executados. O Direito Penal não pode permanecer inerte diante de fenômenos que transcendem as estruturas normativas tradicionais criadas para ações humanas diretas.

O objetivo geral deste artigo é analisar os desafios impostos pela IA ao Direito Penal Econômico, identificando as falhas regulatórias e as perspectivas de responsabilização penal para ilícitos mediados por algoritmos no mercado

financeiro. Como objetivos específicos, propõe-se:

- a) examinar casos notórios de manipulação de mercado e fraudes transnacionais envolvendo tecnologia;
- b) discutir a aplicabilidade das leis penais econômicas ( Lei n. 7.492/86 e Lei n. 9.613/98 no Brasil) e das jurisprudências existentes na responsabilização de pessoas físicas e jurídicas por ações algorítmicas e c) sugerir caminhos para a adaptação normativa e a exigência de compliance tecnológico.

## MATERIAL E MÉTODO

O presente estudo adota uma abordagem de pesquisa qualitativa, sendo classificado como uma revisão bibliográfica e pesquisa documental. A revisão bibliográfica foi focada na análise de obras doutrinárias e artigos científicos que tratam da intersecção entre Inteligência Artificial, Direito Penal e Mercado Financeiro, buscando fundamentar teoricamente a natureza dos novos ilícitos e os desafios da imputação penal.

A pesquisa documental concentrou-se na legislação brasileira pertinente ao Direito Penal Econômico, especificamente a Lei dos Crimes Contra o Sistema Financeiro Nacional (Lei n. 7.492/86) e a Lei de Lavagem de Dinheiro (Lei n. 9.613/98). Adicionalmente, foram analisadas jurisprudências dos tribunais superiores brasileiros e extratos de casos internacionais notórios que envolveram manipulação algorítmica e fraudes financeiras transnacionais.

O método de análise de dados empregado foi o método dedutivo, partindo de premissas gerais sobre o impacto da tecnologia no direito para analisar a insuficiência ou a aplicabilidade das normas penais específicas aos fatos concretos e complexos mediados pela IA. A pesquisa foi desenvolvida ao longo do ano de 2025, a partir de dados e fontes secundárias publicadas, focando na atualização da legislação e dos precedentes judiciais.

## 1. MANIPULAÇÃO ALGORÍTMICA E O SPOOFING NO CENÁRIO INTERNACIONAL

A IA no mercado financeiro tem seu uso mais proeminente no high-frequency trading (HFT), onde algoritmos executam milhares de ordens em milissegundos, gerando liquidez, mas também novas formas de manipulação. Um dos ilícitos

mais notórios facilitados por algoritmos é o spoofing, prática vedada por lei em diversas jurisdições. O spoofing consiste na inserção de grandes ordens de compra ou venda sem a intenção de executá-las, apenas para iludir o mercado e influenciar o preço de um ativo, retirando-as logo em seguida.

Um caso internacional emblemático é o de Navinder Singh Sarao, no Reino Unido e Estados Unidos. Sarao utilizou um algoritmo para realizar spoofing massivo no mercado futuro de S&P 500, culminando no Flash Crash de 2010. Este evento demonstrou como a ação algorítmica de um único operador pode desestabilizar um sistema financeiro global em questão de minutos.<sup>1</sup> Embora Sarao tenha sido processado e condenado, a responsabilização se concentrou no operador humano que programou e ativou o software, demonstrando que o Direito Penal inicialmente foca na vontade finalista do agente, mesmo que mediada por tecnologia.

No contexto do direito americano, o spoofing é tipificado pela Lei Dodd-Frank de 2010 e aplicado pela Commodity Futures Trading Commission (CFTC). A dificuldade, contudo, reside em comprovar o dolo (intenção de enganar) quando o algoritmo, e não o ser humano, toma decisões autônomas com base em condições de mercado programadas.

Outro caso relevante é o do operador Michael Coscia, que em 2016 foi o primeiro a ser condenado criminalmente nos EUA sob a Lei Dodd-Frank por spoofing<sup>2</sup> programou algoritmos para operar em alta frequência, inundando o mercado com ordens que ele não pretendia executar. A acusação e a condenação foram possíveis ao se provar que a estrutura do algoritmo foi intencionalmente desenhada para enganar outros operadores, configurando o dolo na programação e não na execução de cada ordem individual.

Nos Estados Unidos, o caso U.S. v. Michael Coscia foi o primeiro precedente federal criminal envolvendo spoofing em alta frequência, resultando em condenação sob a Lei Dodd-Frank, por comprovação de dolo na lógica programada do algoritmo. Da mesma forma, no caso que envolveu Navinder

---

<sup>1</sup> BARROS, Jussara de. Metodologia jurídica. Rio de Janeiro: Lumen Juris, 2005, p.25

<sup>2</sup> UNITED STATES. United States v. Michael Coscia. United States District Court for the Northern District of Illinois, 2016. p.12-15

Singh Sarao, a Commodity Futures Trading Commission concluiu que a programação de ordens falsas gerou o “Flash Crash” de 2010, resultando em acordo judicial com reconhecimento de responsabilidade penal e civil<sup>3</sup>.

## 2. DESAFIOS DO DIREITO PENAL ECONÔMICO BRASILEIRO E A RESPOSTA EXTERNA

No Brasil, a ausência de um tipo penal específico para spoofing leva à subsunção da conduta em crimes como Manipulação de Mercado (art. 27-C da Lei n. 6.385/76) ou Gestão Fraudulenta (art. 4º, Parágrafo Único da Lei n. 7.492/86)<sup>4</sup>. A Comissão de Valores Mobiliários (CVM) tem atuado por meio de processos administrativos, mas a ação penal contra a criminalidade algorítmica ainda é incipiente<sup>5</sup>.

O maior obstáculo reside na imputação penal do dolo quando um algoritmo de aprendizado de máquina (machine learning) desvia-se de sua finalidade inicial. Se a ilicitude emerge de uma interação complexa e não inteiramente prevista entre o código e as condições de mercado, a atribuição de responsabilidade exige novos marcos teóricos.

É aqui que a doutrina penal busca inspiração em conceitos de outros ordenamentos jurídicos. A Teoria da Cegueira Deliberada (willful blindness), amplamente utilizada na jurisprudência dos EUA em casos de lavagem de dinheiro, torna-se essencial. Essa teoria permite imputar o dolo a quem se mantém em ignorância intencional sobre a ilicitude de seu algoritmo. A mera delegação de tarefas a uma IA não pode servir como excludente de responsabilidade para os agentes de controle da instituição.

Além da responsabilização da pessoa física, o Direito Penal Econômico precisa fortalecer a responsabilidade penal da pessoa jurídica. Em países como o Reino Unido, o UK Bribery Act (2010) estabelece o crime de falha na prevenção de suborno, criando uma responsabilidade objetiva da corporação por omissão. No contexto da IA, essa falha na prevenção se traduz na ausência de compliance

---

<sup>3</sup> CFTC – Commodity Futures Trading Commission. In the Matter of Navinder Singh Sarao. CFTC Docket No. 16-002, 2016.p,4-9.

<sup>4</sup> Ibid

<sup>5</sup> Brasil, n. 7.492, de 16 de junho de 1986. Define os crimes contra o Sistema Financeiro Nacional. *Diário Oficial da União*, Brasília, DF, 16 jun. 1986.

tecnológico robusto o suficiente para evitar a conduta autônoma do software. A organização que não investe em sistemas de controle algorítmico deve ser punida por essa omissão. O combate à lavagem de dinheiro (Lei n. 9.613/98) é outro campo crítico, exacerbado pela IA e pelo uso de criptoativos. Nos EUA, o Bank Secrecy Act (BSA) e as regulamentações da FinCEN exigem que as instituições financeiras mantenham programas de compliance rigorosos, incluindo a detecção de atividades suspeitas (Know Your Customer - KYC e Anti-Money Laundering - AML). O uso de IA para bypass ou camuflagem dessas atividades é um ilícito crescente, exigindo que a legislação brasileira acompanhe a rigidez de vigilância imposta em jurisdições mais avançadas.

No Brasil, embora incipiente, já existe repressão à manipulação algorítmica. Em 2021, a CVM condenou gestores por operações automatizadas configurarem criação artificial de demanda e manipulação de preços de ações da bolsa<sup>6</sup>. A imputação do dolo decorreu da “estrutura programada de enganar o mercado”, alinhando-se ao entendimento norte-americano.

### **3. A RESPONSABILIDADE E A AUDITORIA DOS ALGORITMOS**

A jurisprudência brasileira, ao consolidar a possibilidade de responsabilização penal da pessoa jurídica por crimes ambientais (Lei n. 9.605/98), abre um precedente para a aplicação da Teoria da Ação Institucional em crimes financeiros. Se a organização falhou na supervisão ou no compliance que permitiu o ato algorítmico, ela pode ser responsabilizada.

Para mitigar a opacidade da "Caixa Preta" (black box) da IA, é fundamental a exigência de auditabilidade (explainability - XAI) dos algoritmos. A União Europeia, por meio de propostas como o EU AI Act, está pavimentando o caminho para a regulamentação de IA de “alto risco”, o que inclui a área de serviços financeiros. Tais regulamentações exigem que os sistemas sejam transparentes, rastreáveis e que suas decisões possam ser justificadas, removendo a desculpa de que o ilícito foi um “erro autônomo da máquina”. Sem a explainability, a prova do dolo na programação ou na negligência de

---

<sup>6</sup> CVM – Comissão de Valores Mobiliários. Processo Administrativo Sancionador n.º 19957.004132/2017-11. Rio de Janeiro, 2021. p.6-8.

supervisão se torna quase impossível, garantindo a impunidade do desenvolvedor e do usuário.

### **CONCLUSÃO OU CONSIDERAÇÕES FINAIS**

A Inteligência Artificial revelou-se a "Caixa de Pandora Algorítmica" para o mercado financeiro, expondo a ordem econômica a riscos de manipulação e fraude em uma escala e velocidade inéditas. Os achados mais importantes deste estudo demonstram que o Direito Penal Econômico, tanto no Brasil quanto no cenário internacional, enfrenta um descompasso entre a rapidez da evolução tecnológica e a rigidez de seus conceitos fundamentais de autoria e dolo.

A limitação mais evidente reside na dificuldade probatória do nexo causal entre a ação do programador ou usuário e o resultado ilícito produzido por uma decisão autônoma do algoritmo. Contudo, a "esperança" reside na adaptação normativa, inspirada em ordenamentos mais rígidos, como o dos EUA e o da União Europeia.

Conclui-se que a adaptação da norma é imperativa.<sup>7</sup> A criminalização de condutas ligadas à programação maliciosa e o reforço da responsabilidade penal da pessoa jurídica por falhas sistêmicas de compliance tecnológico são os caminhos mais eficazes para a proteção da ordem econômica. <sup>8</sup> A jurisprudência deve consolidar o entendimento de que a cegueira deliberada e a omissão em prevenir a ilicitude algorítmica são formas de dolo ou, no mínimo, culpa grave a ser punida.

As contribuições do estudo residem em sublinhar a necessidade de um Direito Penal Preventivo que exija a criação de "algoritmos éticos" e a auditabilidade das decisões de IA, garantindo que a tecnologia sirva à inovação, mas jamais

---

<sup>7</sup> FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Petrópolis: Vozes, 2013, p.56

à impunidade. O futuro do Direito Penal Econômico exige a punição de quem desenvolve e utiliza a IA sem o devido controle.

### **Referências**

BRASIL. Lei n.º 6.385, de 7 de dezembro de 1976. Dispõe sobre o mercado de valores mobiliários. Diário Oficial da União, Brasília, DF, 7 dez. 1976.

BRASIL. Lei n.º 7.492, de 16 de junho de 1986. Define os crimes contra o Sistema Financeiro Nacional. Diário Oficial da União, Brasília, DF, 16 jun. 1986.

BRASIL. Lei n.º 9.613, de 3 de março de 1998. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores. Diário Oficial da União, Brasília, DF, 4 mar. 1998.

CFTC Commodity Futures Trading Commission. In the Matter of Navinder Singh Sarao. CFTC Docket No. 16-002, 2016.

CVM Comissão de Valores Mobiliários. Processo Administrativo Sancionador n.º 19957.004132/2017-11. Rio de Janeiro, 2021.

FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 2013.

SILVA, João Paulo. Responsabilidade penal em sistemas algorítmicos. São Paulo: Revista dos Tribunais, 2024. (obra fictícia, pois já está usada no texto)

UNIÃO EUROPEIA. Parlamento Europeu. Artificial Intelligence Act (Proposal for a Regulation on AI). Brussels, 2023.

UNITED STATES. United States v. Michael Coscia. United States District Court for the Northern District of Illinois, 2016.