57º SBPO
SIMPÓSIO BRASILEIRO DE PESQUISA OPERACIONAL
Gramado • RS
DE 5 A 9 DE OUTUBRO DE 2025

Investigando a Lavagem de Dinheiro com Teoria dos Grafos: Algoritmos e Treewidth em Redes Financeiras

Samuel Eduardo da Silva, Renata Nunes Velozo, Luís Felipe Ignácio Cunha, Fábio Protti
Instituto de Computação, Universidade Federal Fluminense
samueleduardo@id.uff.br, renata_nunes@yahoo.com,
lfignacio@ic.uff.br, fabio@ic.uff.br

Rubén Interian
Instituto de Computação, Universidade Estadual de Campinas
interian@unicamp.br

Uéverton S. Souza
IMPA Tech, Instituto de Matemática Pura e Aplicada (IMPA)
Instituto de Computação, Universidade Federal Fluminense
ueverton.souza@impatech.org.br

Raphael Carlos Santos Machado
Clavis Segurança da Informação
Instituto de Computação, Universidade Federal Fluminense
raphael.machado@clavis.com.br

RESUMO

A lavagem de dinheiro é um crime que sustenta a atuação de organizações criminosas ao ocultar a origem ilícita de recursos financeiros. Este artigo propõe uma metodologia baseada na teoria dos grafos para modelar e analisar redes de transações financeiras obtidas por meio de quebras de sigilo bancário. São desenvolvidos algoritmos para detectar comportamentos típicos de lavagem, como contas de passagem e fluxos recorrentes entre pessoas físicas e jurídicas. Além disso, realiza-se um estudo estrutural utilizando a medida de *treewidth*, investigando a complexidade dos grafos financeiros e identificando pontos críticos para a interrupção de operações ilícitas. A metodologia é validada com dados reais, contribuindo para o avanço de técnicas de investigação financeira e alinhando-se a diretrizes de proteção de redes estratégicas nacionais.

PALAVRAS CHAVE. lavagem de dinheiro, grafos, treewidth, defesa, segurança.

Tópicos (TAG - Teoria dos Grafos e Algoritmos, D&SP – PO em Defesa e Segurança)

ABSTRACT

Money laundering is a crime that supports the operations of criminal organizations by concealing the illicit origin of financial resources. This work proposes a methodology based on graph theory to model and analyze financial transaction networks obtained through bank secrecy breaches. Algorithms are developed to detect typical money laundering behaviors, such as pass-through accounts and frequent transactions between individuals and companies. Additionally, a structural study is conducted using the treewidth measure, assessing the complexity of financial graphs and identifying critical points for disrupting illicit operations. The methodology is validated with real-world data, contributing to the advancement of financial investigation techniques and aligning with national strategies for the protection of critical and strategic networks.

KEYWORDS. money laundering, graphs, treewidth, defense, security.

Paper topics (TAG - Graph Theory and Algorithms, D&SP - OR in Defense and Security)

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

1. Introdução

A lavagem de dinheiro é um crime financeiro que permite a organizações criminosas (ORCRIMs) ocultar a origem ilícita de recursos, reintegrando-os à economia legal. Estima-se que entre 2% e 5% do PIB mundial seja movimentado anualmente por atividades de lavagem, segundo Camdessus [1998]. No Brasil, a Lei nº 9.613/1998, atualizada pela Lei nº 12.683/2012 (Brasil [2021]), define o crime como a dissimulação de bens provenientes de infrações penais, sendo essencial para a sustentabilidade de ORCRIMs (Mendroni [2016]).

Investigações financeiras enfrentam desafios devido ao grande volume de dados, como os obtidos por quebras de sigilo bancário, e à complexidade das redes de transações. A teoria de grafos emerge como uma ferramenta poderosa para modelar e analisar essas redes, permitindo identificar padrões suspeitos, como contas de passagem e fluxos financeiros entre camadas de ORCRIMs (Dreżewski et al. [2015]; Fronzetti Colladon e Remondi [2017]).

Existem alguns trabalhos que propõem a análise de dados financeiros usando a teoria de grafos. Dreżewski et al. [2015] utilizam a análise de redes sociais criadas a partir de extratos bancários e registros de dados cadastrais de pessoas jurídicas para a detecção da lavagem de dinheiro. São usadas medidas de centralidade específicas com o objetivo de identificar a função exercida por cada vértice dentro do grafo: organizador, soldado, comunicador, entre outros.

Fronzetti Colladon e Remondi [2017] apresentam um modelo preditivo para a prevenção do crime de lavagem de dinheiro. O modelo preditivo utiliza informações do banco de dados de uma empresa de factoring, e levou à identificação de possíveis clientes suspeitos de operarem a lavagem de dinheiro. Ferrara et al. [2014] buscou detectar a estrutura hierárquica de uma ORCRIM a partir do grafo dos registros telefônicos dos investigados. Apesar dos dados utilizados não serem de transações financeiras, a abordagem usada neste estudo do funcionamento de uma ORCRIM é próxima à usada neste artigo. Pourhabibi et al. [2020] realizaram uma revisão de 39 trabalhos publicados sobre essa temática. Os trabalhos são baseados no aprendizado de máquina e foram divididos segundo a abordagem usada em três grandes categorias: aprendizado supervisionado, não supervisionado e semi-supervisionado.

Este artigo propõe a análise dos dados oriundos de quebra de sigilo bancário usando a teoria de grafos, e demonstrando a sua validade através da análise de casos reais. Os dados oriundos de quebra de sigilo bancário são naturalmente de difícil acesso. A análise proposta busca revelar novos alvos de interesse das investigações, elos de conexão entre diferentes organizações criminosas, as fases da lavagem de dinheiro, e os fluxos financeiros dentro da ORCRIM. São apresentados algoritmos que têm como objetivo detectar contas de passagem, comportamentos típicos de lavagem de dinheiro, e transações mensais frequentes entre pessoas físicas ou jurídicas.

Além disso, realiza-se um estudo estrutural das instâncias, com foco na verificação da existência de uma *treewidth* limitada — uma medida que quantifica o quão "próximo de uma árvore" é um grafo, facilitando a aplicação de algoritmos eficientes em problemas complexos. Essa análise permite explorar propriedades estruturais fundamentais para a detecção e interrupção de operações de lavagem de dinheiro. Ao compreender a estrutura do grafo por meio da *treewidth*, torna-se possível identificar vértices críticos cuja neutralização estratégica — como o bloqueio de agentes ou transações — pode comprometer significativamente a rede ilícita. Essa abordagem está alinhada à Doutrina Militar de Defesa Cibernética (MD31-M-07) (Ministério da Defesa [2023]), que destaca a importância da proteção de sistemas de interesse da Defesa, incluindo infraestruturas críticas e redes estratégicas nacionais, reforçando o entendimento estrutural das redes como instrumento de segurança e proteção dos ativos nacionais no ambiente digital.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os principais conceitos relacionados à lavagem de dinheiro. Na Seção 3, descrevemos a modelagem das

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

redes de transações financeiras utilizando grafos, além da apresentação de dois algoritmos desenvolvidos para a identificação de comportamentos típicos de lavagem de dinheiro. Por fim, a Seção 4 explora o estudo estrutural das instâncias financeiras com foco na análise da *treewidth*, evidenciando como essa característica pode ser utilizada para revelar vulnerabilidades nas redes criminosas e subsidiar estratégias de combate à lavagem de dinheiro.

2. Principais conceitos

Organização criminosa

A Convenção das Nações Unidas contra o Crime Organizado Transnacional Brasil [2004] define ORCRIM como um grupo de três ou mais pessoas, estruturado e atuando concertadamente para cometer infrações graves, visando benefícios econômicos. No Brasil, a Lei nº 12.850/2013 (Brasil [2013]) caracteriza ORCRIM como a associação de quatro ou mais indivíduos, com divisão de tarefas, para obter vantagens por infrações penais com penas superiores a quatro anos ou de caráter transnacional. Masi, Carlo Velho [2021] afirmam que o crime organizado deriva de atividades ilícitas estruturadas, enquanto Santos [2007] destaca seu potencial ofensivo e busca por lucro.

Lavagem de Dinheiro

No Brasil, a lavagem de dinheiro é definida como a ocultação da origem de bens provenientes de infrações penais (Brasil [2021]). Romantini [2003] descreve o processo como a dissimulação de recursos ilícitos por operações financeiras ou comerciais para evitar repressão estatal. Desde 2012, qualquer crime pode ser considerado antecedente à lavagem, ampliando a eficiência das investigações (Romantini [2003]). O processo ocorre em três fases: colocação (introdução de recursos no sistema financeiro, muitas vezes via empresas de fachada), ocultação (múltiplas transações para dificultar rastreamento, frequentemente em paraísos fiscais) e integração (incorporação dos valores à economia legal). Estima-se que 2% a 5% do PIB mundial seja lavado anualmente, segundo Camdessus [1998]. No Brasil, o COAF, criado em 1998, é a Unidade de Inteligência Financeira (COAF [2021]).

Relação entre ORCRIMs e Lavagem de Dinheiro

A lavagem de dinheiro é crucial para as ORCRIMs, permitindo atividades criminosas (Mendroni [2016]). O combate a esse crime foca no asfixiamento financeiro, com a solicitação de mais RIFs ao COAF, de 1.500 em 2012 para 10.000 em 2020 (COAF [2021]). A análise de grandes volumes de dados enfrenta desafios como falta de capacitação e tecnologia (Martins [2018]). Em 2021, o Gafilat destacou a importância de ciência de dados e inteligência artificial contra crimes financeiros (Gafilat [2021]; COAF [2021]). A Operação Shawarma (2017) revelou um esquema de lavagem e evasão de divisas, movimentando R$230 milhões entre 2016 e 2020 com empresas de fachada (Receita Federal do Brasil). A estrutura da ORCRIM em grafo (Figura 1) mostra fluxos financeiros, destacando a teoria de grafos para priorizar alvos e acelerar investigações.

3. Dados de quebra de sigilo bancário: modelagem usando grafos

Nesta seção, será apresentada a modelagem usada na análise de dados de quebra de sigilo bancário usando a teoria de grafos.

3.1. Estrutura dos dados

Uma das fontes de dados utilizadas nas investigações financeiras é aquela provocada a partir do deferimento de um pedido de quebra de sigilo bancário, também denominado pelo termo afastamento de sigilo bancário (Romantini [2003]). Esse instrumento jurídico permite o acesso aos dados referentes às movimentações bancárias dos investigados com a devida identificação de seus destinatários e remetentes. As instituições financeiras são obrigadas a enviar os dados que possuírem dos alvos que tenham o seu sigilo quebrado. A Tabela 1 exemplifica quais dados ficam disponíveis numa quebra de sigilo bancário.

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

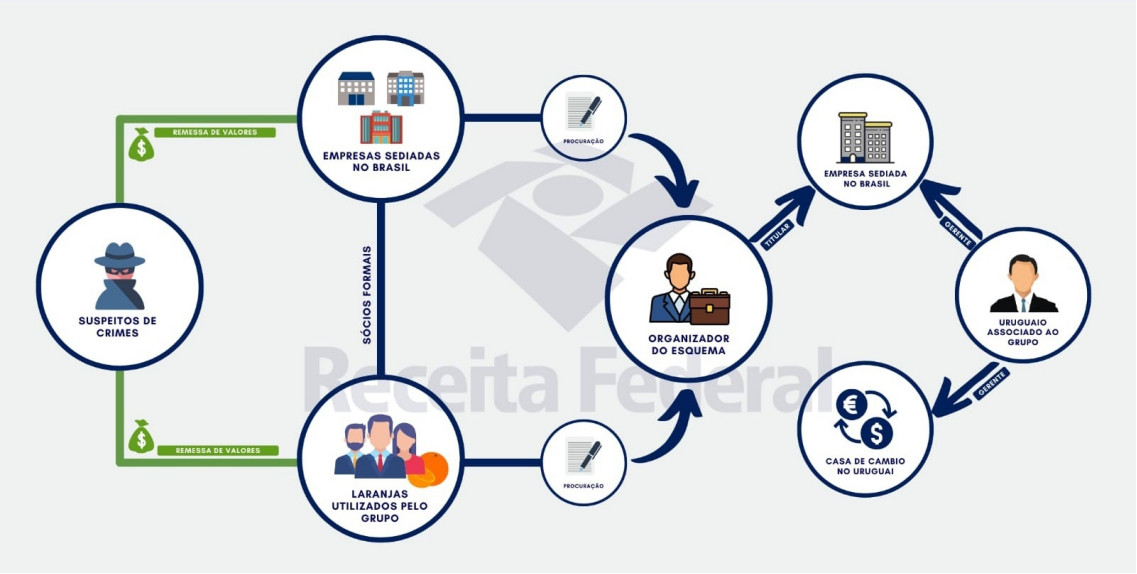


Figura 1: Esquema da ORCRIM na Operação Shawarma Receita Federal do Brasil.

Data	Titular	CPF / CNPJ	Tipo	Valor	Crédito / Débito	CPF / CNPJ	Origem / Destino
10/01/21	João	123	TED	110,00	D	321	Maria
15/01/21	João	123	Depósito	717,00	C	555	Paulo
15/01/21	João	123	Depósito	600,00	C	111	Joana
25/01/21	João	123	TED	500,00	C	321	Maria
25/01/21	João	123	TED	1200,00	C	555	Paulo
11/01/21	Roberta	222	IOF	0,30	D	191	BB
16/01/21	Roberta	222	Aplicação	4410,00	D	222	Roberta
20/01/21	Roberta	222	TED	2500,00	D	555	Paulo
20/02/21	Roberta	222	TED	1000,00	D	777	Silva
20/02/21	João	123	Depósito	650,00	C	111	Joana
19/03/21	Roberta	222	TED	500,00	D	555	Paulo
20/03/21	Roberta	222	TED	550,00	D	555	Paulo

Tabela 1: Exemplo de dados disponíveis numa quebra de sigilo bancário. Elaborado pelo autor.

Uma das contribuições deste trabalho é propor uma metodologia de análise dos dados oriundos da quebra de sigilo bancário usando a teoria de grafos. O objetivo é identificar de forma automatizada, dentre todas as pessoas físicas e jurídicas presentes nesses dados, aquelas cujas movimentações devem ser investigadas pelo analista. Para isso, são apresentadas interpretações dos conceitos, tais como vértices mediadores, vértices fronteira e arestas mediadoras, sob a ótica da análise de dados financeiros.

3.2. Definições

Segue algumas definições importantes para o trabalho (para mais detalhes, veja Velozo et al. [2021]):

Definição 1 (Vértice mediador)**.** *Seja $G = (V, E)$ um grafo, $A_1, A_2, \ldots, A_n$ uma partição de V e $N(v)$ o conjunto de vizinhos de v. Dizemos que um vértice v é mediador se pertence a alguma parte A_i da partição, possui ao menos dois vizinhos ($|N(v)| \geq 2$), tem pelo menos um vizinho na*

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

mesma parte A_i ($N(v) \cap A_i \neq \emptyset$) e pelo menos um vizinho em outra parte ($\exists, w \in N(v)$ tal que $w \notin A_i$).

Definição 2 (Vértice fronteira)**.** *Seja $G = (V, E)$ um grafo, $\{A_1, A_2, \ldots, A_n\}$ partição de V, $v \in A_i$ um vértice mediador de A_i. O vértice v é fronteira se existe $u \in N(v)$, $u \in A_i$ tal que $N(u) \setminus A_i = \emptyset$.*

Definição 3 (Aresta mediadora)**.** *Seja $G = (V, E)$ um grafo,$\{A_1, A_2, \ldots, A_n\}$ partição de V, e uv uma aresta em E. uv é uma aresta mediadora se:*

1. *u é vértice mediador de A_i (alternativamente, v é vértice mediador de A_i);*
2. *$v \notin A_i$ (alternativamente, $u \notin A_i$).*

3.3. Análise usando a teoria de grafos

Na Tabela 1, cada linha corresponde a uma transação bancária realizada na conta de um titular. Seja $G(V, A)$ o grafo direcionado cujos vértices são todas as pessoas físicas e jurídicas identificadas na quebra de sigilo bancário. Cada transação é representada por um arco entre dois vértices desse grafo. Um desses vértices é o titular da conta cujo sigilo foi quebrado. O outro vértice representa a origem ou o destino do recurso transacionado. A informação sobre a natureza do lançamento (crédito ou débito) permite definir um grafo direcionado, orientando os arcos de acordo com a natureza do lançamento. Se a natureza do lançamento é crédito, o depositante estará na origem e o titular no destino, e se é débito, o titular estará na origem e o beneficiário no destino. Na Figura 2, é apresentado o grafo que representa as transações bancárias listadas na Tabela 1.

Cada arco a terá associado um peso $w(a)$ igual ao número de transações realizadas entre a origem e o destino. Optou-se por essa representação devido a algumas características do funcionamento das ORCRIMs e da lavagem de dinheiro. Por exemplo, é comum transações suspeitas de lavagem de dinheiro serem de pequeno valor para burlar os mecanismos de controle; provocando um fracionamento dos valores em repetidas transações. A mesma prática pode ser percebida no fluxo de capitais entre as camadas das ORCRIMs, centralizadas e fracionadas.

Adicionalmente, cada arco (x, y) terá associada uma tabela $T[(x, y)]$. As linhas da tabela $T[(x, y)]$ indicam quais foram os valores totais (campo "valor") que x transferiu para y em cada ano-mês (campo "mes"). A Tabela 2 exemplifica como os lançamentos descritos no Tabela 1 seriam transformados na tabela $T[(x, y)]$.

X	Y	**mês-ano**	**valor**
João	Maria	1/2021	110,00
Paulo	João	1/2021	1.917,00
Joana	João	1/2021	600,00
Maria	João	1/2021	500,00
Roberta	BB	1/2021	0,30
Roberta	Roberta	1/2021	4.410,00
Roberta	Paulo	1/2021	2.500,00
Roberta	Paulo	3/2021	1.050,00
Roberta	Silva	2/2021	1.000,00
Joana	João	2/2021	650,00

Tabela 2: Tabela T referente aos lançamentos listados na Tabela 1 de exemplo. Elaborado pelo autor.

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

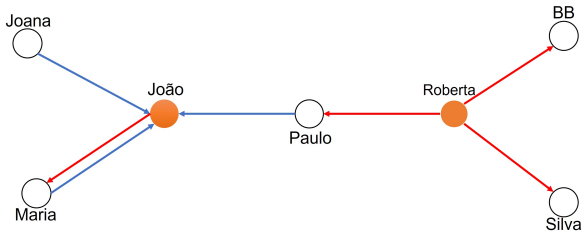


Figura 2: Grafo gerado a partir dos dados apresentados na Tabela 1. Note que os arcos estão coloridos conforme a natureza do lançamento, azul para crédito e vermelho para débito. Os titulares das contas cujo sigilo foi quebrado estão destacados em laranja. Elaborado pelo autor.

Considera-se que cada conjunto de dados gerados a partir de uma quebra de sigilo bancário representa as transações realizadas por um grupo de pessoas físicas e jurídicas que estejam sob uma investigação específica. Nesse trabalho, chamaremos esses grupos de casos. Segundo Romantini [2003], a quebra de sigilo bancário é pedida após levantamentos realizados na investigação, de forma a compor uma lista de possíveis alvos. Nessa fase, familiares e amigos próximos podem ser acrescidos na lista, ou mesmo alguma transação suspeita que já tenha sido notificada através de um RIF.

Análise de interações dentro de uma organização criminosa

Os casos podem ser analisados isoladamente, em duplas ou em conjuntos maiores. Este artigo foca na análise de casos individuais e em duplas. A análise isolada não é ideal para investigar conexões entre ORCRIMs, pois todos os vértices pertencem ao mesmo caso. Contudo, Gomes [1997] destaca características das ORCRIMs que justificam a análise individual com teoria de grafos, como hierarquia estrutural, planejamento empresarial, recrutamento de pessoas e divisão funcional de atividades.

Essas características indicam uma divisão de tarefas dentro das ORCRIMs, permitindo identificar grupos internos por algoritmos de detecção de comunidades, como os de Girvan e Newman [2002] e Blondel et al. [2008]. A análise individual revela camadas da ORCRIM, canais financeiros entre elas e transações associadas às fases da lavagem de dinheiro.

Na Figura 2, observa-se que Roberta transfere valores para Paulo, que os repassa a João. Nesse caso, João e Roberta são investigados, e Paulo pode ser um intermediário. A Figura 3 mostra o grafo particionado em dois grupos, A e B, pelo algoritmo de Blondel et al. [2008], com Paulo como vértice fronteira no grafo não direcionado $G'(V, E)$ subjacente a $G(V, A)$. Ele é essencial para o fluxo financeiro entre as partições, sugerindo sua relevância investigativa, embora hipóteses devam ser validadas com dados adicionais.

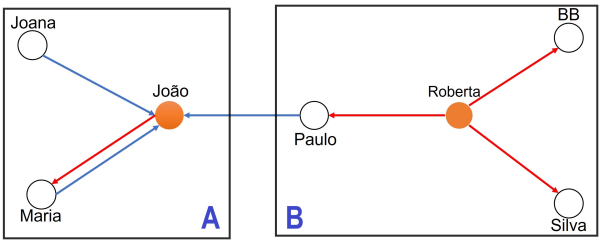


Figura 3: Grafo da Tabela1 após execução do algoritmo Blondel et al. [2008], com partições A e B delimitadas por retângulos. Elaborado pelo autor.

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

Vértices mediadores, especialmente os de fronteira, são candidatos a elos entre camadas da ORCRIM ou etapas da lavagem (colocação, ocultação, integração). Um vértice mediador pessoa jurídica pode indicar uma empresa de fachada. Os pesos das arestas avaliam a força das conexões, enquanto os valores mensais transferidos, analisados pelo Algoritmo 1, identificam padrões de transações periódicas. Esse algoritmo detecta arcos (x, y) em $G(V, A)$ com remessas regulares, usando como entrada o grafo G e o número mínimo de meses n para caracterizar frequência.

Algorithm 1 *Identifica transações frequentes entre vértices no grafo G*

Require: Grafo $G(V, A)$, T, número mínimo de períodos n.

1: $resultado \leftarrow \emptyset$
2: **for** (x, y) **in** A **do**
3: $\quad media \leftarrow T[(x, y)].valor.mean()$
4: $\quad dp \leftarrow T[(x, y)].valor.std()$
5: $\quad max_date \leftarrow T[(x, y)].mes.max()$
6: $\quad min_date \leftarrow T[(x, y)].mes.min()$
7: $\quad \Delta date \leftarrow max_date - min_date$
8: $\quad$ **if** $\frac{dp}{media} \leq 0.25$ and $|T[(x, y)]| \geq n$ and $|T[(x, y)]| \geq \Delta date \cdot 0.75$ **then**
9: $\quad\quad resultado \leftarrow resultado \cup \{(x, y)\}$

return $resultado$

Na linha 1 é feita a inicialização do conjunto de arcos que contem o resultado do algoritmo. Nas linhas 2-9, um laço de repetição percorre todas os arcos do grafo e aplica uma série de critérios para identificar as transações frequentes. Nas linhas 3 e 4, a média e o desvio padrão são calculadas usando os valores da tabela associada ao arco (x, y). Nas linhas 5-7, é calculada a diferença, em meses, entre a data final e inicial das transações. A condicional na linha 8 determina três critérios para que o arco seja classificado como uma conexão frequente entre x e y. São eles:

- O coeficiente de variação (a razão entre o desvio padrão e a média) deve ser menor ou igual a 25%. Este critério verifica se existiu um padrão no montante transacionado mensalmente entre x e y, respeitado o parâmetro fixo 25%.
- O número de meses com transferências entre x e y deve se maior ou igual ao parâmetro n.
- O número de meses com transferências entre x e y deve ser maior ou igual a 75% do número de meses do período global analisado. Esse critério descarta casos em que as movimentações se concentrem em poucos meses, não caracterizando uma frequência mensal contínua.

O Algoritmo 1 é linear no tamanho da entrada, pois cada arco do grafo G e cada valor da tabela T associada ao arco são usados apenas uma vez. Note que os parâmetros numéricos utilizados no Algoritmo 1, especificamente em dois critérios da condicional da linha 8, foram determinados com base na indicação feita pelos analistas do Laboratório de Tecnologia contra Lavagem de Dinheiro, empiricamente. Esses valores indicam um entendimento generalizado entre os analistas e podem ser alterados em investigações com características específicas.

O conjunto de arcos resultado desse algoritmo pode ser tratado como um grupo de alertas ou recomendações para o analista, dispensando uma análise exaustiva manual de todos os pares de vértices que transacionaram em busca desse tipo de padrão. A análise manual desses dados é, em muitos casos, uma realidade nos órgãos de fiscalização, controle e persecução criminal brasileiros.

Outra rotina da investigação financeira que pode ser automatizada consiste na identificação das possíveis contas de passagem cuja titularidade pode pertencer a empresas de fachada ou

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

Algorithm 2 *Identifica possíveis contas de passagem no grafo G*

Require: Grafo $G(V, A)$, T, período de análise P.

1: $resultado \leftarrow \emptyset$
2: **for** x **in** V **do**
3: $\quad saldo_entrada \leftarrow \vec{0}$
4: $\quad saldo_saida \leftarrow \vec{0}$
5: $\quad saldo_final \leftarrow \vec{0}$
6: $\quad$ **for** mes **in** P **do**
7: $\quad\quad$ **for** (y, x) **in** A **do**
8: $\quad\quad\quad saldo_entrada[mes] \leftarrow saldo_entrada[mes] + T[(y, x)].valor[mes]$
9: $\quad\quad$ **for** (x, y) **in** A **do**
10: $\quad\quad\quad saldo_saida[mes] \leftarrow saldo_saida[mes] + T[(x, y)].valor[mes]$
11: $\quad\quad saldo_final[mes] \leftarrow \frac{saldo_entrada[mes] - saldo_saida[mes]}{saldo_entrada[mes]}$
12: $\quad$ **if** $saldo_final.media() \leq 0.05$ **then**
13: $\quad\quad resultado \leftarrow resultado \cup \{x\}$
return $resultado$

a pessoas físicas "laranjas". O comportamento característico das movimentações bancárias dessas contas é que, mês a mês, os valores de saída são iguais ou bem próximos dos valores de entrada.

O Algorítimo 2 identifica os vértices que possuem esse comportamento. A detecção é feita por meio do cálculo das diferenças entre valores totais de créditos e débitos mensais. O algorítimo tem como entrada o grafo direcionado $G(V, A)$, a tabela T, e o período da análise P.

O conjunto *resultado* é inicializado na linha 1. Na linha 2, inicia-se dois loops aninhados: o primeiro (linha 2) percorre todos os vértices $x \in V$, e o segundo (linha 6) é responsável por, mês a mês, calcular a soma dos valores à crédito e à débito, respectivamente. Na linha 11, no vetor *saldo_final*, são armazenados os valores das diferenças entre créditos e débitos de cada mês. Na linha 12, verifica-se se a conta associada ao vértice x é suspeita de atuar como conta de passagem, ou seja, se em média pelo menos 95% do total de créditos mensais correspondem ao total de débitos mensais dentro do período P. Se essa condição for verdadeira, o vértice x será adicionado ao conjunto *resultado* na linha 13.

O Algoritmo 2 é linear no tamanho da entrada, pois cada arco a do grafo G e cada valor da tabela T associada ao arco são usados apenas duas vezes: uma por cada um dos dois extremos de a.

Análise das interações entre as organizações criminosas

A análise das interações entre ORCRIMs baseia-se nas características descritas por Gomes [1997], que incluem conexão com o poder público, divisão territorial de atividades ilícitas e conexões locais, regionais, nacionais ou internacionais com outras ORCRIMs. Esses aspectos destacam a relevância de investigar elos entre organizações criminosas e entidades governamentais ou entre ORCRIMs distintas.

Para analisar interações entre dois casos, constrói-se um grafo direcionado $G(V, A)$ representando todas as transações entre pessoas físicas e jurídicas identificadas nas quebras de sigilo dos casos. Os vértices mediadores do grafo não direcionado $G'(V, E)$, subjacente a $G(V, A)$, são candidatos a elos entre as ORCRIMs. O Algoritmo1 identifica transações frequentes entre vértices de diferentes ORCRIMs, indicando fortes relacionamentos financeiros. Esses resultados podem sugerir que as ORCRIMs formam um único grupo criminoso, hipótese que deve ser validada com dados adicionais. Já o Algoritmo2 mantém sua interpretação, listando vértices associados a contas

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

de passagem.

Na prática, vértices mediadores podem incluir bancos ou concessionárias de serviços, que devem ser filtrados para evitar falsos positivos, enfatizando a importância da limpeza de dados. A ausência de vértices ou arestas mediadoras pode indicar casos não correlacionados ou períodos de sigilo insuficientes, exigindo análise conjunta com investigadores. Por outro lado, alta densidade de arestas mediadoras e vértices mediadores pode sugerir que os casos representam uma única ORCRIM, pois interações entre ORCRIMs distintas tendem a ser menos densas (Gomes [1997]).

4. *Treewidth*

A *treewidth* (largura de árvore) é um parâmetro que mede o quão "próximo"um grafo está de ser uma árvore. Intuitivamente, grafos com baixa treewidth tendem a ter uma estrutura mais hierárquica e menos densa em conexões, o que pode ser explorado computacionalmente.

Formalmente, a *treewidth* de um grafo é definida com base em uma decomposição em árvore (*tree decomposition*). Uma decomposição em árvore é uma estrutura que associa a um grafo $G = (V, E)$ uma árvore T, cujos nós são subconjuntos de vértices de G, chamados de bolsas (*bags*). Essa decomposição deve satisfazer as seguintes propriedades:

- Cada vértice de G aparece em pelo menos uma bolsa.
- Para cada aresta $(u, v) \in E$, existe pelo menos uma bolsa que contém tanto u quanto v.
- Para cada vértice $v \in V$, os nós da árvore T cujas bolsas contêm v formam um subárvore conexa de T.

A largura de uma decomposição em árvore é definida como o tamanho da maior bolsa menos um, e a *treewidth* do grafo é o valor da largura mínima possível entre todas as decomposições válidas. Esse parâmetro é relevante porque muitos problemas que são NP-difíceis em grafos gerais podem ser resolvidos de maneira eficiente (por exemplo, em tempo linear ou polinomial) quando restritos a grafos com *treewidth*, por meio de algoritmos parametrizados (veja Cygan et al. [2015]).

A ideia deste experimento é verificar se instâncias reais derivadas de investigações de lavagem de dinheiro possuem *treewidth* pequena. Caso isso se confirme, seria possível aplicar algoritmos eficientes parametrizados por *treewidth* para análise desses grafos — por exemplo, para detecção de padrões, caminhos suspeitos, estruturas de rede ou subgrafos relevantes.

Foi obtido um conjunto de dados extraído de investigações de lavagem de dinheiro, seguindo o padrão da Tabela 1, e cada instância sendo representada por um caso. Para os experimentos, foram montados os grafos subjacentes dos grafos originais, desconsiderando a distinção entre transações de débito e crédito.

Nesses grafos, todas as arestas duplicadas foram removidas, e os vértices foram renumerados para seguir uma sequência de 1 até n (sendo n o número de vértices do grafo). Em todos os testes, foi aplicado o algoritmo exato de Tamaki [2017] para calcular a *treewidth*. Os resultados são apresentados na Tabela 3. A coluna "instância"indica o caso de investigação, n representa o número de vértices, m o número de arestas, e *tw* a *treewidth* encontrada.

Além disso, foi realizado um teste considerando todo o conjunto de dados como uma única instância (referida como single*). Isso resultou em $n = 12617$ e $m = 13628$ (novamente, as arestas duplicadas foram removidas, e os vértices foram renumerados de 1 até n). Para essa instância, foi encontrada uma *treewidth* igual a 12. Um ponto interessante é que houve 12579 bolsas para 12617 vértices, indicando bolsas muito pequenas, o que pode ser vantajoso para estratégias baseadas em decomposição.

Como mostrado na Tabela 3, a *treewidth* (*tw*) dessas instâncias é consistentemente pequena. Tal resultado sugere a viabilidade de aplicação de algoritmos parametrizados por *treewidth*

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

Instância	n	m	tw
146	38	50	3
148	214	262	4
150	2099	2163	3
151	8	9	2
156	129	147	3
157	197	210	3
158	101	122	4
172	20	20	2
174	162	211	4
185	909	1109	8
200	786	959	4
232	775	974	6
237	6024	6433	5
238	1206	1333	5
246	12	12	2
single*	12617	13628	12

Tabela 3: *treewidth* encontrada nas instâncias de lavagem de dinheiro.

nesses contextos. Por exemplo, os valores observados indicam a potencial aplicabilidade de algoritmos eficientes para problemas como detecção de padrões, verificação de propriedades estruturais, ou mesmo inferência probabilística sobre esses grafos.

Para instâncias relativamente grandes, onde o cálculo exato da *treewidth* é inviável, utilizam-se algoritmos meta-heurísticos que produzem boas aproximações de forma eficiente. Métodos como os descritos por da Silva et al. [2021] permitem estimar a *treewidth* para tais instâncias, viabilizando a aplicação da análise estrutural mesmo em redes complexas típicas de esquemas de lavagem de dinheiro. Vale ressaltar que esparsidade não assegura baixa *treewidth*. Existem grafos esparsos cuja *treewidth* é pequena no número de vértices, como grafos de grade.

4.1. Possíveis aplicações

Este resultado abre uma série de possibilidades relevantes. Por exemplo, é possível enumerar eficientemente todos os cliques do grafo — subconjuntos de vértices completamente conectados — para instâncias de *treewidth* limitada (Chudnovsky e Trotignon [2024]), o que pode revelar pequenos grupos altamente conectados que atuam de forma coordenada, sugerindo núcleos operacionais ou células de confiança dentro da rede criminosa.

Além disso, problemas clássicos como VERTEX COVER e DOMINATING SET tornam-se solucionáveis de forma eficiente em grafos com *treewidth* limitada (veja Cygan et al. [2015]). O problema de VERTEX COVER, por exemplo, pode ser utilizado para identificar o menor conjunto de indivíduos ou entidades que "interceptam" todas as transações suspeitas da rede, sendo candidatos naturais a monitoramento ou bloqueio. Já o DOMINATING SET pode revelar um subconjunto mínimo de vértices com alcance direto sobre todos os demais — isto é, indivíduos ou instituições com grande poder de influência ou controle operacional sobre a rede, cuja neutralização pode comprometer toda a estrutura.

A existência de algoritmos parametrizados que exploram essa característica estrutural para obter soluções exatas e eficientes reforça o valor da análise de *treewidth* como uma ferramenta estratégica no contexto da investigação financeira. Ao aplicar esses métodos, é possível apoiar ações de contenção, bloqueio e desmantelamento de redes de lavagem de dinheiro de forma mais

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

precisa e fundamentada, integrando recursos computacionais avançados à atuação investigativa e à ciberdefesa nacional.

Referências

Blondel, V., Guillaume, J.-L., Lambiotte, R., e Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics Theory and Experiment*, 2008.

Brasil (2004). Decreto nº 5.015, de 12 de março de 2004. *Diário Oficial da República Federativa do Brasil*. URL http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm.

Brasil (2013). Lei nº 12.850, de 02 de agosto de 2013. *Diário Oficial da República Federativa do Brasil*. URL http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

Brasil (2021). Lei nº 12.683, de 09 de julho de 2012. *Diário Oficial da República Federativa do Brasil*. URL https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm.

Camdessus, M. (1998). Money laundering: the importance of international countermeasures. https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098#, Último acesso em 2021-11-22.

Chudnovsky, M. e Trotignon, N. (2024). On treewidth and maximum cliques. URL https://arxiv.org/abs/2405.07471.

COAF (2021). O que faz o COAF? https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/o-que-faz-o-coaf-versao-2021-11-16-publicado.pdf, Último acesso em 2021-11-27.

COAF (2021). Resultados da XLIV reunião plenária do grupo de ação financeira da américa latina (gafilat). https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/notas-do-coaf-1/resultados-da-xliv-reuniao-plenaria-do-grupo-de- acao-financeira-da-america-latina-gafilat.

Cygan, M., Fomin, F. V., Kowalik, Ł., Lokshtanov, D., Marx, D., Pilipczuk, M., Pilipczuk, M., e Saurabh, S. (2015). *Parameterized algorithms*. Springer.

da Silva, S. E., Souza, U., e Ribeiro, C. (2021). Computando a treewidth de um grafo: Algoritmo genético tendencioso de chaves aleatórias. In *Anais do LIII Simpósio Brasileiro de Pesquisa Operacional (SBPO 2021)*, João Pessoa. Galoá. Acesso em: 12 Maio 2025.

Dreżewski, R., Sepielak, J., e Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, 295:18–32. ISSN 0020-0255. URL https://www.sciencedirect.com/science/article/pii/S0020025514009979.

Ferrara, E., De Meo, P., Catanese, S., e Fiumara, G. (2014). Detecting criminal organizations in mobile phone networks. *Expert Systems with Applications*, 41(13):5733–5750. ISSN 0957-4174. URL https://www.sciencedirect.com/science/article/pii/S0957417414001614.

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536

Fronzetti Colladon, A. e Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, 67:49–58. ISSN 0957-4174. URL https://www.sciencedirect.com/science/article/pii/S0957417416305139.

Gafilat (2021). ¿Qué es el GAFILAT? https://www.gafilat.org/index.php/es/.

Girvan, M. e Newman, M. E. (2002). Community structure in social and biological networks. *Proceedings of the national academy of sciences*, 99(12):7821–7826.

Gomes, R., Luiz Flávio; CERVINI (1997). *Crime organizado : enfoques criminológico, jurídico (Lei 9.034/95) e político-criminal*. São Paulo: Revista dos Tribunais. ISBN 85-203-1477-5.

Martins, T. M. d. J. (2018). Crimes fiscais, delitos econômicos e financeiros. *Coletânea de Artigos - Ministério Público Federal - 2ª Câmara de Coordenação e Revisão*, 5:10–35.

Masi, Carlo Velho (2021). Organização criminosa e crime organizado: conceitos interdependentes. https://www.camargomasi.com.br/organizacao-criminosa-e-crime-organizado-conceitos-interdependentes/.

Mendroni, M. B. (2016). *Crime Organizado; aspectos gerais e mecanismos legais*. Atlas. ISBN 9788597007329.

Ministério da Defesa (2023). MD31-M-07: Doutrina Militar de Defesa Cibernética (2ª Edição). URL https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf.

Pourhabibi, T., Ong, K.-L., Kam, B. H., e Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133:113303. ISSN 0167-9236. URL https://www.sciencedirect.com/science/article/pii/S0167923620300580.

Receita Federal do Brasil. Operação shawarma desarticula organização que movimentou 230 milhões de reais oriundos de práticas criminosas. https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2021/novembro/operacao-shawarma-desarticula-organizacao-que-movimentou-230-milhoes-de-reais-oriundos-de-praticas-criminosas, Último acesso em 2022-02-01.

Romantini, G. L. (2003). *O Desenvolvimento Institucional do Combate à Lavagem de Dinheiro no Brasil desde a Lei 9.613/98*. Campinas.

Santos, G. (2007). A hora e a vez de derrotar o crime organizado. *Estudos Avançados*, 21:99–105.

Tamaki, H. (2017). Positive-Instance Driven Dynamic Programming for Treewidth. In Pruhs, K. e Sohler, C., editors, *25th Annual European Symposium on Algorithms (ESA 2017)*, volume 87 of *Leibniz International Proceedings in Informatics (LIPIcs)*, p. 68:1–68:13, Dagstuhl, Germany. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 978-3-95977-049-1.

Velozo, R. N., Souza, U., e Interian, R. (2021). Polarização em grafos: Métricas, arestas mediadoras e grafos bipolarizados. In *Anais do LIII Simpósio Brasileiro de Pesquisa Operacional (SBPO 2021)*, João Pessoa. Galoá. Acesso em: 12 Maio 2025.

DOI: 10.59254/sbpo-2025-212536
http://live-proceedings.pantheonsite.io/p/212536