



CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM MATEMÁTICA E COMPUTACIONAL

ESTUDO DA COMPLEXIDADE DE REDES DE CRIMINALIDADE

ALEX SANDER DE OLIVEIRA TOLEDO

Orientador: Allbens Atman Picardi Faria
CEFET/MG

Coorientadora: Laura C. Carpi
CEFET/MG

BELO HORIZONTE
OUTUBRO DE 2018

ALEX SANDER DE OLIVEIRA TOLEDO

ESTUDO DA COMPLEXIDADE DE REDES DE CRIMINALIDADE

Dissertação apresentada ao Programa de Pós-graduação em Modelagem Matemática e Computacional do Centro Federal de Educação Tecnológica de Minas Gerais, como requisito parcial para a obtenção do título de Mestre em Modelagem Matemática e Computacional.

Área de concentração: Modelagem Matemática e Computacional

Linha de pesquisa: Métodos Matemáticos Aplicados

Orientador: Allbens Atman Picardi Faria
CEFET/MG

Coorientadora: Laura C. Carpi
CEFET/MG

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM MATEMÁTICA E COMPUTACIONAL
BELO HORIZONTE
OUTUBRO DE 2018

T649e Toledo, Alex Sander de Oliveira
Estudo da complexidade de redes de criminalidade / Alex Sander de Oliveira Toledo. – 2018.
112 f.

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Modelagem Matemática e Computacional.
Orientador: Allbens Atman Picardi Faria.
Coorientadora: Laura C. Carpi.
Dissertação (mestrado) – Centro Federal de Educação Tecnológica de Minas Gerais.

1. Crime – Pesquisas – Minas Gerais – Teses. 2. Análise de sistemas – Modelos matemáticos – Teses. 3. Autômato celular – Teses. 4. Multiplexação – Redes de computadores – Teses. 5. Simulação por computador – Teses.
I. Faria, Allbens Atman Picardi. II. Carpi, Laura C. III. Centro Federal de Educação Tecnológica de Minas Gerais. IV. Título.

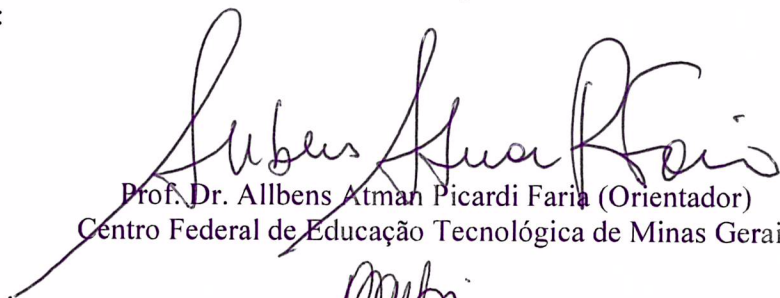
CDD 511.8

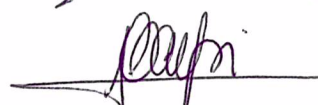


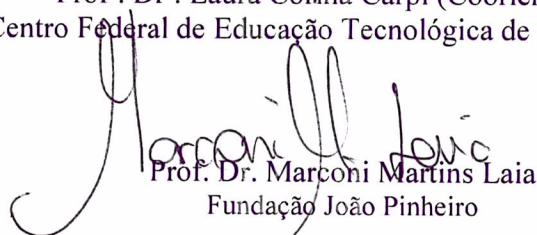
SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
COORDENAÇÃO DO CURSO DE MESTRADO EM MODELAGEM MATEMÁTICA E COMPUTACIONAL

“ESTUDO DA COMPLEXIDADE DE REDES DE CRIMINALIDADE”

Dissertação de Mestrado apresentada por **Alex Sander de Oliveira Toledo**, em 13 de novembro de 2018, ao Programa de Pós-Graduação em Modelagem Matemática e Computacional do CEFET-MG, e aprovada pela banca examinadora constituída pelos professores:

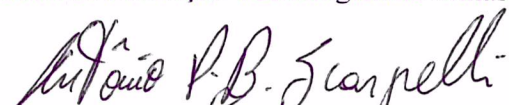

Prof. Dr. Allbens Atman Picardi Faria (Orientador)
Centro Federal de Educação Tecnológica de Minas Gerais


Prof.ª Dr.ª Laura Corina Carpi (Coorientadora)
Centro Federal de Educação Tecnológica de Minas Gerais

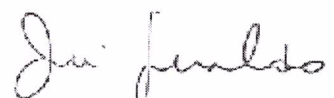

Prof. Dr. Marconi Martins Laia
Fundação João Pinheiro


Prof. Dr. Martín Gómez Ravetti
Universidade Federal de Minas Gerais


Prof. Dr. Arthur Rodrigo Bosco de Magalhães
Centro Federal de Educação Tecnológica de Minas Gerais


Prof. Dr. Antônio Paulo Baêta Scarpelli
Centro Federal de Educação Tecnológica de Minas Gerais

Visto e permitida a impressão,


Prof. Dr. José Geraldo Peixoto de Faria
Coordenador do Programa de Pós-Graduação em
Modelagem Matemática e Computacional

À minha amada Patrícia, por compreender e aceitar minhas ausências dedicadas aos estudos e pesquisas. Aos meus filhos, Larissa, Maria Eduarda e João Augusto, meus maiores legados.

Agradecimentos

Cultive o hábito de pensar em Deus durante as suas atividades. É extremamente importante tornar este hábito parte de sua vida diária. Não siga a regra apenas por alguns dias, esquecendo-a logo depois. Siga-a todos os dias, da melhor maneira possível. Mesmo que escorregue e volte a seus antigos hábitos, continue tentando. No devido tempo, você se tornará uma pessoa saudável e espiritualmente forte. Paramahansa Yogananda

Agradeço a Deus por sua divina misericórdia ao me conduzir sempre pelos caminhos de luz, paz e felicidade.

“A árvore não prova a doçura dos próprios frutos; o rio não bebe suas ondas; as nuvens não despejam água sobre si mesmas, A força dos bons deve ser usada para benefício de todos”. Provérbio hindu

A meu orientador, Professor Allbens Atman, pelo seu esforço em me conduzir pelo caminho desafiador do aprendizado, muitas vezes difícil de entender, mas deslumbrante ao descortinar-se. *Amicus certus in re incerta cernitur.*

“Quem executa, diligente, contente, o trabalho que lhe foi atribuído, qualquer que seja, encaminha-se para a perfeição.” Provérbio hindu

Meu agradecimento àqueles que por seus esforços e exemplos procurei seguir. Em especial a minha coorientadora Laura Carpi pela disponibilidade, acompanhamento e esclarecimentos necessários a este trabalho.

Se o sábio lhes der ouvidos, aumentará seu conhecimento, e quem tem discernimento obterá orientação. (Provérbios 1:5)

Resumo

Este trabalho evidenciou as redes de criminalidade de Minas Gerais. O estudo de redes de criminalidade permitiu novas abordagens e respostas para fazer frente à demanda crescente de Segurança Pública. A pesquisa concentrou-se na hierarquia, personagens e violência nas organizações criminosas. A partir da modelagem de relacionamentos oriundos de um banco de dados de Inteligência de Segurança Pública e utilizando elementos de redes complexas, foi possível identificar redes de criminalidade, relacionamentos entre criminosos e líderes. O uso de autômatos celulares permitiu modelar e analisar a evolução de rede de criminalidade e testar a robustez à ruptura e resiliência. A utilização pioneira de redes *multiplex* para identificação e análise de redes de criminalidade possibilitou a visualização da estrutura criminosa em camadas hierárquicas, sendo explorada a medida de diversidade de nós para identificação de líderes.

Palavras-chave: Modelagem. Simulação. Redes de Criminalidade. Elementos de Rede Complexa. Autômato Celular. Redes Multiplex.

Abstract

This work evidenced the crime networks of Minas Gerais. The study of crime networks has allowed new approaches and responses to meet the growing demand for Public Security. The research focused on hierarchy, characters, and violence in criminal organizations. From the modeling of relationships from a Public Security Intelligence database and using elements of complex networks, it was possible to identify criminal networks, relationships between criminals and leaders. The use of cellular automata allowed to model and analyze the evolution of the crime network and to test robustness to rupture and resilience. The pioneering use of multiplex networks to identify and analyze criminal networks made it possible to visualize the criminal structure in hierarchical layers, exploiting the measure of node diversity to identify leaders.

Keywords: Modeling. Simulation. Crime Networks. Complex Network Elements. Cellular Automata. Multiplex Networks.

Lista de Figuras

Figura 1 – Evolução do Cadastro de Vínculos de Ocorrências da PMMG	4
Figura 2 – Representação de grafos	15
Figura 3 – Representação por matriz de adjacência	16
Figura 4 – Redes sociais	17
Figura 5 – Representações de matriz e grafo	18
Figura 6 – Ilustração de camadas de Redes <i>multiplex</i>	20
Figura 7 – Ilustração da matriz de adjacência	36
Figura 8 – Ilustração dos vínculos de indivíduos	36
Figura 9 – Ilustração gráfica da rede de criminalidade, utilizando gráfico tipo circular	38
Figura 10 – Ilustração gráfica da rede de criminalidade, utilizando gráfico tipo randômico	38
Figura 11 – Rede de Inteligência	39
Figura 12 – Rede de Autores	40
Figura 13 – Rede de Condenados	40
Figura 14 – Rede de Gangues	41
Figura 15 – Ilustração da conversão de dados em inteligência	45
Figura 16 – <i>Degree centrality</i> da Rede de Inteligência	46
Figura 17 – <i>Betweenness centrality</i> da Rede de Inteligência	47
Figura 18 – <i>PageRank</i> da Rede de Inteligência	48
Figura 19 – <i>Média Degree centrality + Betweenness centrality + PageRank</i> da Rede de Inteligência	49
Figura 20 – Medidas de Centralidade da sub-Rede de Autores	50
Figura 21 – Medidas de Centralidade da sub-Rede de Condenados	51
Figura 22 – Medidas de Centralidade da Rede de Gangue	52
Figura 23 – Subgrupos da Rede de Inteligência	54
Figura 24 – Subgrupos da Rede de Inteligência evidenciando os líderes	55
Figura 25 – Subgrupos da Rede de Gangue	56
Figura 26 – Evolução temporal da Rede de Inteligência	57
Figura 27 – <i>Power Law</i>	60
Figura 28 – Eficiência da cadeia de valor	62
Figura 29 – Segurança da cadeia de valor	63
Figura 30 – Representação dos passos da simulação (a)	64
Figura 31 – Representação dos passos da simulação (b)	65
Figura 32 – Eficiência da ruptura da rede	66
Figura 33 – Representação das redes após rupturas parciais (a)	67
Figura 34 – Representação das redes após rupturas parciais (b)	68
Figura 35 – Identificação das nove modalidades de crime	69

Figura 36 – Rede <i>multiplex</i> de Gangue e Inteligência	70
Figura 37 – Rede <i>multiplex</i> de criminalidade	71
Figura 38 – Número de criminosos	72
Figura 39 – Rede <i>multiplex</i> de criminalidade em sete camadas	73
Figura 40 – Rede <i>multiplex</i> de criminalidade em sete camadas, evidenciando os 10 maiores valores de <i>Multiplexity</i>	74
Figura 41 – Cálculo da diversidade de uma estrutura de 4 camadas	78
Figura 42 – Resultados da Dissimilaridade das Camadas da rede <i>multiplex</i> de crimi- nalidade	78
Figura 43 – Diversidade de Nó	79
Figura 44 – Rede de maior quantidade de laços <i>multiplex</i>	80

Lista de Tabelas

Tabela 1 – Principais Estatísticas das Redes	41
--	----

Sumário

1 – Introdução	1
1.1 Justificativa	3
1.2 Motivação	4
1.3 Objetivo Geral	5
1.4 Objetivos Específicos	5
1.5 Organização do trabalho	6
2 – Fundamentação Teórica	7
2.1 A Polícia, o Crime e a Inteligência	7
2.2 A Natureza das Redes de Criminalidade	10
2.3 Elementos de Redes Complexas	14
2.4 Redes <i>Multiplex</i>	19
2.5 Autômatos Celulares	21
3 – Metodologia	24
3.1 Delineamento da pesquisa	24
3.2 Coleta e tratamento de dados	27
4 – Trabalhos Relacionados	29
4.1 A complexidade de rede de dados criminosos: um estudo de caso de suas consequências para o crime, controle e estudo de redes	29
4.2 A ineficiência relativa da interrupção da rede criminosos	30
4.3 Confie em teu vizinho desonesto: multiplexidade nas redes de crime organizado de Chicago	32
5 – Resultados	35
5.1 Desenvolvimento de Protocolo para Identificação de Rede de Criminalidade	35
5.2 Estatísticas de Rede de Criminalidade	38
5.3 Análise de Redes de Criminalidade	44
5.4 Simulação de Ruptura e Resiliência de Rede de Criminalidade	58
5.5 Multiplexidade de Redes de Criminalidade	68
6 – Conclusão	81
6.1 Trabalhos Futuros	81
6.2 Considerações Finais	82
Referências	83

Apêndices	91
APÊNDICE A – Medidas de Centralidade para Análise de Redes Sociais	92
APÊNDICE B – Medidas de Centralidade da Rede de Inteligência	94
APÊNDICE C – Medidas de Centralidade da sub-Rede de Autores	96
APÊNDICE D – Medidas de Centralidade da sub-Rede de Condenados	98
APÊNDICE E – Medidas de Centralidade da Rede de Gangues	100
APÊNDICE F – Identificação de Comunidades da Rede de Inteligência	101
APÊNDICE G – Medidas de Eficiência de Resiliência	102
APÊNDICE H – Medidas de Segurança de Resiliência	103
APÊNDICE I – Medidas de Eficiência de Ruptura	104
APÊNDICE J – Identificação de Crimes praticados pelos Infratores	105
APÊNDICE K – Medidas <i>Multiplex</i>	106
APÊNDICE L – Medidas de Diversidade de Nó	107
APÊNDICE M – Quantidade de Laços <i>Multiplex</i>	108
Anexos	111
ANEXO A – Memorando PMMG	112

1 Introdução

O crime organizado constitui um dos maiores temores da sociedade no mundo todo. Ameaças como o cyber-crime, a pornografia infantil, tráfico de drogas, roubo de identidade, entre muitos outros crimes, exigem intervenções proativas que sejam capazes de controlar as organizações criminosas por trás delas (DUIJN; KASHIRIN; SLOOT, 2014). No mundo todo, agências governamentais, estudiosos do tema e policiais procuram constantemente formas eficientes de romper ou controlar estas estruturas criminosas.

O grande foco da atuação policial no mundo se dá por zonas quentes de criminalidade. Através de métodos estatísticos são identificados os locais geográficos onde os crimes acontecem e intervenções pontuais são realizadas nestes locais (MORSELLI, 2009). Porém o que se verifica com esta atuação é a migração geográfica do crime, pois não se levou em consideração os aspectos intrínsecos das redes de criminalidade, onde seus atores interagem e conseguem mudar a forma e local de atuação, rearticulando toda sua forma de agir.

Desde a década de 1990, a perspectiva de rede para explorar os fenômenos criminais vem aumentando rapidamente e, desta forma, um número crescente de definições de crime organizado começou a incluir o termo "rede" (VARESE, 2012). Ao mesmo tempo, técnicas de análise de redes vem sendo utilizadas cada vez mais com o objetivo de estudar as interações entre os criminosos (PAPACHRISTOS, 2011; BOUCHARD; AMIRAULT, 2013; BRUINSMA; BERNASCO, 2004).

Em muitos destes trabalhos, que utilizam Análise de Redes Sociais para obter uma melhor compreensão destas organizações, surgem controvérsias na forma em que o crime organizado vinha sendo pensado (DUIJN; KASHIRIN; SLOOT, 2014). Segundo eles, as organizações criminosas, precisam ser consideradas, contrariamente ao que se pensava até o momento, como redes sociais com relações internas flexíveis e não hierárquicas.

Desta forma, o ataque do líder no topo de uma organização criminosa não necessariamente resultaria no seu colapso, já que a fluidez e a flexibilidade destas estruturas as tornam altamente resilientes a estratégias tradicionais de aplicação da lei (SPARROW, 1991; DUIJN; KLERKS, 2014; KREBS, 2002; NATARAJAN, 2006; MORSELLI, 2009; SPAPENS, 2010; RAAB; MILWARD, 2003; SPAPENS, 2011). Estas características demonstram a grande complexidade da estrutura e dinâmica das redes de criminalidade, onde mudanças podem ocorrer como resultado de novas oportunidades de negócios, como consequência de uma competição, ou como um resultado direto dos controles de aplicação da lei que podem levar à queda ou adaptação da rede (SLOOT; KAMPIS; GULYÁS, 2013).

A perspectiva de rede tem sido cada vez mais usada para explicar os fenômenos

criminais, com a Análise de Redes Sociais se fixando no campo da criminologia, porém o estudo nesta área permanece na análise descritiva.

Estudos dividem as redes em duas perspectivas: a substantiva, que determina uma rede como uma forma específica de organização; a instrumental, baseada na presença de indivíduos (nós) e ligações (laços). Isto causa dualidade entre as duas perspectivas no contexto de redes criminosas, no que diz respeito a forma de estudar e analisar as redes (CAMPANA, 2016).

Podolny e Page (1998) definem uma rede como uma forma distinta de organização:

Definimos uma forma de organização em rede como qualquer coleção de atores ($N \geq 2$) que buscam relações de troca repetidas e duradouras entre si e, ao mesmo tempo, carece de autoridade organizacional legítima para arbitrar e resolver disputas que possam surgir durante o intercâmbio.
[Tradução do autor]

As redes são muito atraentes para criminosos, pois são flexíveis e dinâmicas, capazes de limitar a exposição a riscos, permitindo formação de alianças entre criminosos. A confiança entre os criminosos é uma das principais características da rede de criminalidade, como uma forma ideal de organizar atividades criminosas, sendo um elemento constitutivo do modo de organização da rede. (CAMPANA, 2016)

As redes estabelecem um conjunto finito de nós e laços, onde os indivíduos têm uma intencionalidade em sua participação, pois tem uma maneira própria de pensar sobre suas relações sociais. A perspectiva de verificar estes nós e laços é referida como Análise de Redes Sociais.

O uso de Análise de Redes Sociais para explicar os fenômenos criminais vem crescendo muito nos últimos anos. No estudo de redes, a Análise de Redes Sociais caracteriza-se como uma abordagem instrumental, sendo altamente sensível à qualidade de dados coletados, como atribuição incorreta de características de nós e laços na mineração das diversas fontes de dados. Outro problema nesta abordagem pode ser visto pela falta de dados, ou seja, ausência de nós e laços. Por isto, procedimentos de validação devem ser adotados como forma de checar os dados extraídos de determinada fonte. Outro problema diz respeito aos limites de uma rede. A falta de uma lista de associações acessíveis é um dos fatores de problemas em redes criminosas. Enfim, medidas estruturais podem estar sujeitas a problemas devido a erros, procedimentos de amostragem, problemas de especificação e limites e dados ausentes.

Apesar de medidas estruturais serem ferramentas muito úteis para análise de redes de criminalidade, uma confiança excessiva pode levar a compreensão inadequada ao contexto em estudo. As medidas de centralidade são muito utilizadas para análise em redes de criminalidade, particularmente a centralidade de grau. O alto nível de centralidade

de grau é atribuído ao indivíduo mais proeminente da rede. Já os menores graus são atribuídos aos indivíduos mais periféricos. Isto é verdadeiro para grande maioria das redes, mas deve ser bem avaliado, pois há casos em que isto não é verdadeiro. Isto poderá ser visto pela assortatividade negativa das redes de criminalidade, ao contrário das redes sociais. Há casos de análise de redes de criminalidade que informações qualitativas, como interceptação de conversas telefônicas, podem evidenciar a centralidade ou a periferia de determinados indivíduos. Isto se deve a natureza relacional, onde os dados da rede podem violar a suposição de independência das observações sobre quais modelos estatísticos padrões são construídos. Neste aspecto, o uso de redes *multiplex* mostra ser uma viável.

Assim, a pesquisa de redes criminosas tende a ser exploratória e descritiva, procurando explicações na estrutura gráfica das redes, onde desenvolvimentos recentes buscam a detecção de determinados indivíduos e fatores que podem levar ao rompimento de redes criminosas.

1.1 Justificativa

Modelagem e simulação se apresentam como alternativas interessantes para compreensão de comportamentos de redes de criminalidade, ajudando na execução de experimentos para validar teorias.

Por vários anos, a Física Estatística desenvolveu métodos teóricos e numéricos para o estudo e compreensão de diversos campos da ciência, onde processos complexos poderiam ser explorados por modelos e simulações por computador, projetados como ferramentas para explorar, testar e comprovar diversas hipóteses de representações mais genéricas.

A modelagem e a simulação são amplamente utilizadas na especificação de comportamentos de sistemas. Um modelo pode ser definido como a simplificação do mundo, em uma escala menor, em diversos níveis de complexidade. Simulação é uma forma de modelagem, que busca imitar o mundo real, inclusive social, alcançada pelos avanços na área de informática, modernos equipamentos e novas linguagens de programação (BOCCARA, 2010). As simulações auxiliam em diversas percepções de atividades numa sociedade, permitindo obter uma melhor compreensão para algumas características da sociedade, entre elas o comportamento de grupos criminosos, que se unem para prática de ações ilícitas.

A modelagem e simulação das sociedades humanas são uma difícil questão, visto que mesmo utilizando estudos e tecnologias recentes, os agentes (indivíduos), podem se comportar de formas diversas e variadas quando atuam em conjunto, fugindo de diversos comportamentos esperados. O comportamento em virtude dos relacionamentos propiciados pelo fenômeno das redes sociais também contribui para a relevância do tema. (MORSELLI, 2009)

Modelagem e simulação de comportamentos de redes de criminalidade são necessidades emergentes nas Organizações de Segurança Pública, podendo substituir o modelo estatístico georeferenciado, hoje amplamente utilizado, por modelos que permitam a identificação de seus líderes, seus subgrupos e comportamentos, bem como também simulações de resiliência e ruptura das redes criminosas.

1.2 Motivação

Informações sobre grupos criminosos são muito difíceis de serem obtidas, pelas próprias características destes grupos, que dependem do anonimato para manterem suas atividades e obterem lograr êxito em suas ações criminosas. Porém, diversas ações de organizações policiais pelo mundo têm promovido esforços para catalogar pessoas e grupos em banco de dados, onde são inseridas as pessoas presas por práticas de diversos e específicos tipos de crimes.

O sistema denominado Cadastro de Vínculos de Ocorrências (CVO), vinculado a Inteligência da Polícia Militar de Minas Gerais (PMMG), caracteriza um destes sistemas. Possui grande quantidade de informações sobre redes de criminalidade armazenadas em um único repositório, um Banco de Dados Eletrônico vinculado a Rede Estratégica de Inteligência (REINT), que é utilizado por policiais para armazenar informações sobre criminosos e seus relacionamentos, com alto nível de detalhamento. A Figura 1 mostra o crescimento do CVO desde sua criação e implantação em 2006, até dezembro de 2014, totalizando 152.973 (cento e cinquenta e dois mil, novecentos e setenta e três) cadastros criminais.

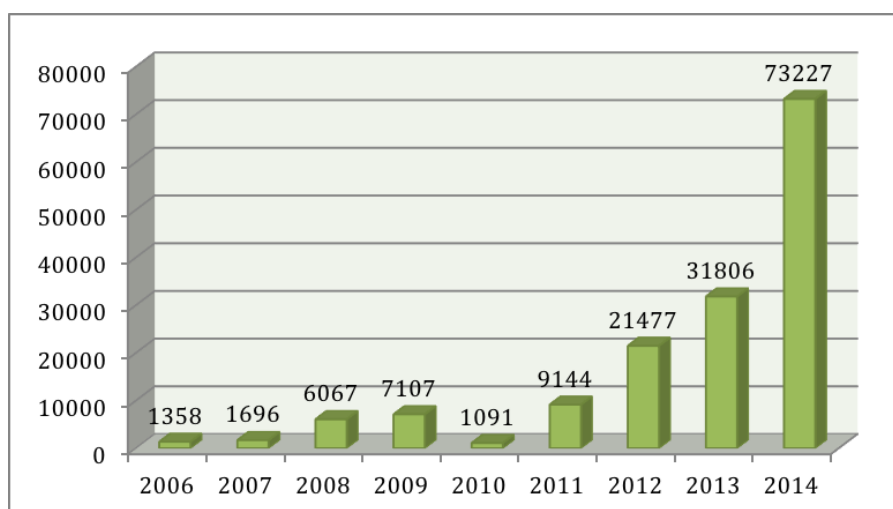


Figura 1 – Evolução do Cadastro de Vínculos de Ocorrências da PMMG.

Fonte: REINT

Visto que o Banco de Dados do CVO atingiu imenso tamanho, o problema agora é conseguir identificar e visualizar, de forma computacionalmente viável, as redes de criminalidade. Problemas como descobrir o tamanho, os líderes e os relacionamentos

das redes de criminalidade se tornam essenciais, visto que oferecem a possibilidade de promover ações para o desmantelamento de tais redes.

1.3 Objetivo Geral

Tem-se como objetivo geral desta pesquisa: construir, testar e validar um modelo baseado em redes complexas para transformar um banco de dados em grafos dinâmicos, que permitam estudar interações na rede, identificando as redes de criminalidade e caracterizando sua atuação.

1.4 Objetivos Específicos

Como objetivos específicos temos:

1. Identificar redes de criminalidade;
2. Identificar os líderes das redes de criminalidade;
3. Identificar os relacionamentos existentes nas redes de criminalidade
4. Decompor as redes de criminalidade em camadas para identificação de relacionamentos baseados em tipos de crimes;
5. Simular a evolução das redes de criminalidade;
6. Desenvolver ferramentas computacionais para análise e estudo de redes de criminalidade.

Através de elementos de redes complexas identificou-se as redes, os líderes e os relacionamentos existentes nas redes de criminalidade. Com a utilização de redes *multiplex*, foi decomposto um banco de dados, que permitiu a exploração de camadas de redes, abstraindo como os crimes evoluíram em uma rede de criminalidade, como os criminosos coexistem dentro da mesma população, como interação entre si e a gangue ou organização criminosa que participam. A aplicação de autômatos celulares permitiu modelar redes de criminalidade e analisar sua evolução e interligações, simulando comportamentos diversos das redes de criminalidade, para atuação policial.

Assim, através da análise dos dados, o **problema foi: como modelar os relacionamentos criminosos, de modo a evidenciar suas interligações e colaborações?**

Para o estudo foi fundamental a modelagem e simulação, que possibilitaram o entendimento comportamental e as implicações dos comportamentos de um sistema social.

Como **hipótese, a partir de um banco de dados real, objetivou-se criar algoritmos capazes de identificar redes de criminalidade e as conexões entre os criminosos.**

1.5 Organização do trabalho

Este trabalho está estruturado da seguinte forma: Capítulo 1 introdução, apresentou a necessidade de utilizar modelagem e simulação para o entendimento das redes de criminalidade; Capítulo 2 revisão bibliográfica, na qual são detalhados conceitos de polícia, crime e inteligência, das perspectivas das redes de criminalidade na sociedade, elementos de redes complexas, redes *multiplex* e autômatos celulares; no Capítulo 3 são destacados os objetivos, o problema e a hipótese do estudo; o Capítulo 4 descreve a metodologia de pesquisa utilizada neste estudo; no Capítulo 5 são apresentados os trabalhos relacionados que serviram de guia para o estudo; no Capítulo 5 são apresentados os resultados da identificação de redes de criminalidade, suas estatísticas gerais, a análise das redes de criminalidade, as simulações de ruptura e resiliência da rede de criminalidade e a multiplexidade destas redes criminosas, no ponto de vista dos crimes praticados por seus indivíduos; por fim, o Capítulo 6 apresenta as conclusões e perspectivas oriundas do trabalho.

2 Fundamentação Teórica

As instituições policiais não dispõem de capacidades necessárias para controlar as atividades criminosas, especificamente as mais modernas, que estão sempre evoluindo em sua forma de atuar. Esta falta de capacidade não é atribuída aos policiais, mas a uma deficiência institucional, social e governamental, que se alimenta de múltiplas fontes para prática do ato criminoso. Assim, a luta contra a criminalidade deixa de ser uma ação somente policial, mas uma questão político-governamental, que ultrapassa as fronteiras territoriais dos países (MONET, 2001).

Das ocorrências urbanas à criminalidade transfronteiriça, não há apenas modificação de graus, mas também na natureza dos crimes. O universo policial se rompe em todo mundo entrando na era das “Polícias de duas velocidades”, na qual se mantém os policiais de patrulha, mas se induz o policial com a preocupação de ser mais eficaz na repressão às formas complexas de criminalidade, pois são incapazes de lutar apenas com suas forças e métodos clássicos contra atividades criminais que os superam.

As novas formas de criminalidade precisam de uma Polícia atualizada para fazer frente. A centralização das informações criminais se acelera, com as Polícias buscando contar com equipamentos, computadores e processos informacionais capazes de contribuir com a modernização de sistemas e capazes de identificar o crime e o criminoso, de forma a induzir a atuação preventiva e repressiva das Polícias.

Apresentaremos a seguir considerações formais face ao enfrentamento ao crime e casos relacionados que norteiam a pesquisa, com revisão dos modelos que permitam direcionar esforços para identificação de redes de criminalidade.

2.1 A Polícia, o Crime e a Inteligência

É comum associar inovação na Polícia ao nome de Robert Peel (BAYLEY; SKOLNICK, 2006), que em 1829 trouxe em evidência a Polícia Metropolitana de Londres. Seu estudo mostrou ao mundo o medo dos cidadãos frente aos altos índices de criminalidade, caracterizado por um temor generalizado diante da inércia da Polícia, ao mesmo tempo que introduziu inovações simples e brilhantes, como criação de novos uniformes, introdução dos policiais em locais de trabalho onde tinham vínculos, patrulhas a pé *etc.*

Atualmente as Polícias enfrentam os mesmos problemas do século XIX, mas em maior escala. Tais desafios são inerentes ao trabalho policial numa sociedade livre e democrática, onde se luta para manter um equilíbrio entre a efetiva aplicação da lei e a imparcialidade no tratamento dos indivíduos.

Pesquisas mostram que as estratégias tradicionais da Polícia não estão funcionando com eficiência. Segundo Bayley e Skolnick (2006) *"aumentar o número de policiais não reduz necessariamente o índice de criminalidade¹, nem eleva a proporção de crimes solucionados"*. Podemos afirmar que se não houver mais policiais haverá mais crimes, todavia, o número de policiais atinge um limiar de cobertura a partir do qual não se torna eficiente o aumento para redução da criminalidade. Ainda segundo Bayley e Skolnick (2006), *"o serviço de patrulha motorizada aleatória não reduz o crime nem melhora a possibilidade de prender suspeitos"*. Assim, o uso de patrulhamento ostensivo² como forma de redução do crime é limitado, tendo pouco impacto junto a população, bem como junto aos criminosos.

Segundo Filho et al. (2001), *"as ferramentas de tratamento de dados geográficos atualmente disponíveis permitem que áreas de concentração aparentemente alta de eventos tais como homicídios sejam facilmente visualizadas"*. Isto permite que se direcione policiais para atuação em áreas com maior concentração de crimes. Porém, o número de policiais empregados no policiamento também não reduz o crime ou aumenta a prisão de criminosos. Segundo Bayley e Skolnick (2006), o patrulhamento ostensivo de uma determinada área reduz o crime apenas temporariamente, porque há o deslocamento do crime para outras áreas.

Os crimes que mais aterrorizam os cidadãos são: assalto à mão armada, roubo, furto de domicílio, estupro e homicídio. Estes crimes raramente são enfrentados pelo policiamento de patrulha padrão. As prisões eficientes são casos raros, pois os policiais gastam a maior parte do tempo com o patrulhamento passivo e prestando serviços de emergência. O tempo de atendimento das chamadas de emergência não tem qualquer efeito sobre a possibilidade de prender os criminosos ou a satisfação dos cidadãos envolvidos, porque a sensação é de que o criminoso estará longe quando o policial chegar, isto porque o tempo médio de acionamento aos serviços de emergência policial é de quatro a cinco minutos, o que só surtiria efeito se tivesse um policial em cada esquina, com a reação instantânea e eficaz na prisão do criminoso. Os crimes não são solucionados pelas investigações policiais. Geralmente os crimes são solucionados pela prisão em flagrante (quando o crime ocorre) ou pela identificação por parte de testemunhas. Sem isto, as chances de solucionar um crime caem para menos de uma em dez (BAYLEY; SKOLNICK, 2006).

Estes resultados são alarmantes, pois mostram que as estratégias primárias de policiamento não reduzem o crime nem tranquilizam a população.

De maneira geral a Polícia até os dias de hoje não é submetida a uma análise comparativa. Cientistas até bem pouco tempo não reconheciam o importante papel desempenhado

¹ Índice estatístico para computar crimes tendo como base a população por 100.000 habitantes. (MEIRELLES, 2007)

² Ato de policiais realizarem patrulhas em determinada área, atuando com a população no processo de identificação e resolução de problemas, incluindo crimes, medo do crime, drogas, desordens físicas e sociais etc (SANTO; MEIRELLES, 2003).

pelas Polícias no mundo. O que havia escrito sobre a Polícia foi feito pelos próprios policiais, através de suas observações em seu cotidiano (BAYLEY; SKOLNICK, 2006).

Estudar a Polícia, seu papel e soluções possíveis para a atividade policial desperta pouco interesse nos meios acadêmicos (BAYLEY; SKOLNICK, 2006). Apesar disso, a manutenção da ordem é papel fundamental de qualquer governo constituído. São identificados quatro fatores para a falta de interesse do meio acadêmico em lidar com a Polícia:

Primeiro, a Polícia raramente desempenha um papel importante nos grandes eventos históricos. Não estão envolvidas com batalhas épicas, marchas heróicas ou retiradas espetaculares. Suas atividades são rotineiras demais, sua presença é disseminada demais e sua clientela é comum demais para compor o assunto de um grande drama. Ela não elabora regras sociais gerais, mas se dedica a problemas humanos de um modo em particular [...] Segundo, policiamento não é uma atividade glamorosa, de alto prestígio. Suas tarefas, mesmo aquelas ligadas à investigação criminal, são maçantes e repetitivas [...] Terceiro, o policiamento também pode ter sido negligenciado porque é mal visto. Coerção, controle e opressão são sem dúvida necessários à sociedade, mas não são agradáveis. [...] Quarto, aqueles interessados em conduzir estudos sobre Polícia enfrentam enormes problemas práticos [...] o material de documentação normalmente não é coletado, catalogado e disponibilizado em bibliotecas. (BAYLEY; SKOLNICK, 2006)

Para conhecer a Polícia, é necessário estudar sua diversidade regional e ao redor do mundo. Uma característica comum às Polícias do mundo todo é que *“estão autorizadas a usar a força física para regular as relações interpessoais nas comunidades”* (BAYLEY, 2001).

O trabalho policial pode ser definido considerando diferentes abordagens, que são: pelo que é designada a fazer; pelas situações que tem que lidar, desde simples ocorrências familiares até múltiplos homicídios praticados por gangues; pelas ações que têm que empreender em um tipo de crime. Suas atribuições organizacionais descrevem o que estão fazendo – patrulhamento, controle, acompanhamento, dentre outros. Brigas domésticas, perturbação do sossego, pessoas suspeitas, arrombamentos, distúrbios, mortes, criminosos e organizações criminosas são situações de ocorrência rotineira. Relatar, prender, advertir, prestar primeiros socorros, acompanhar e anteceder aos fatos criminosos são ações que a Polícia tem que empreender numa comunidade.

O trabalho de patrulhamento é significativamente o mais importante feito pelas organizações policiais. Nos últimos tempos, têm surgido novas atribuições que apontam à prevenção do delito e do crime através da Inteligência³ que se destacam por prevenir o delito, o crime.

As informações sobre a natureza das situações que a Polícia enfrenta exercem papel fundamental no combate ao crime e provêm, segundo Bayley (2001) de quatro situações:

³ Entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre os fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. (MOURA, 2017)

observações detalhadas, relatórios de atividades, arquivos de atividades coletivos e o registro de chamadas públicas de assistência policial, este último, a fonte final de informações para o trabalho policial. Estas situações refletem nas informações sobre situações trazidas à atenção da Polícia, mas, sobretudo, devem ser uma resposta aos anseios da sociedade. As informações⁴ devem ser recolhidas como parte do trabalho de campo e armazenadas em registros oficiais, que por vezes criam volumes enormes para serem analisados que levam ao emprego de esquemas de amostragem, o que é desaconselhável, pois não representam a realidade do crime.

A produção de tabulações sobre a natureza das chamadas de serviço é fundamental para a atividade policial, o que demanda tempo, pessoas e muito trabalho, já que significa folhear volumosos arquivos e registros. Para isto, a obtenção de informação completa e confiável sobre situações de crime e delitos termina sendo extremamente difícil.

Uma vez que a variedade de situações com as quais a Polícia tem que lidar é tão vasta, comparações só podem ser feitas se forem descritas em tipos gerais. O número e natureza de categorias necessárias é questão de julgamento. Quanto mais categorias, menor a distorção da realidade; quanto menos categorias, mais difícil se torna tipificar cada situação de modo confiável. (BAYLEY, 2001)

As fontes de informação discordantes e a falta de confiabilidade leva a uma dificuldade de comparação dos resultados.

O que realmente se deseja é o desenvolvimento de novas estratégias, mais específicas e articuladas, que ofereçam uma estrutura básica para facilitar o estudo e comparação de dados sobre o crime.

2.2 A Natureza das Redes de Criminalidade

O escopo, as formas e o conteúdo das redes de criminalidade variam através do tempo. Podem ir desde ofensas e ameaças até o monopólio de um mercado ou território. Podem se basear em incentivos mútuos, reforçando sua produtividade e interação co-participativa. Podem se basear em laços de amizade de família ou afinidades diversas. As redes de criminalidade levam ao compartilhamento de recursos, à lealdade entre o grupo, à melhora da expertise individual e a uma liderança dominante (MORSELLI, 2009). Estas redes podem ter diversas proporções, desde pequenos grupos, compostos de duas pessoas, até organizações espalhadas por vários países. À medida que estas redes crescem, tendem a obstruir o sistema de valores que mantém a ordem coletiva, impondo ações e regras

⁴ A informação, segundo Feitoza (2010), considerada *stricto sensu*, refere-se a dados já examinados, submetidos a algum trabalho de análise e interpretação. Em síntese, significa dizer que a informação traduz o dado com algum sentido e já exprime certo valor de relevância. A informação ainda está susceptível à verificação.

criminosas (MORSELLI, 2009). Ainda, segundo Morselli (2009), o que se verifica na maioria dos crimes é o envolvimento de mais de uma pessoa.

O estudo de redes de criminalidade não conta ainda com um conceito que abranja todas as suas perspectivas, podendo assim oferecer flexibilidade suficiente para incorporar uma ampla variedade de formas. Os sociólogos que estudam o crime passaram conceitos que denotam a aglomeração social dos infratores sob diferentes ângulos. Muitas vezes, os recursos de unificação de um conceito foram consideravelmente influenciados pelas doutrinas vigentes à época (MORSELLI, 2009).

Segundo Felson (2003) *apud* Morselli (2009), hoje predomina um cenário de convergência, um lugar onde os potenciais infratores podem atender, solicitar ou recrutar outros criminosos em potencial para agregar suas redes de criminalidade. Assim, o criminoso transita de uma rede para outra, mantendo ou não a lealdade a seu grupo original.

Easley e Kleinberg (2010), num sentido básico, definem que “uma rede é qualquer coleção de objetos em que alguns pares desses objetos são conectados por laços”. Esta definição é bem flexível e depende de múltiplas formas como as diferentes relações e/ou conexões podem ser usadas e apresentadas através de seus laços. Assim, fica evidente que podemos encontrar redes em diferentes domínios.

Redes de criminalidade são um subconjunto marginalizado de uma vizinhança problemática, uma subcultura desviante, no espaço geográfico ou no mercado criminoso, onde existem redes em funcionamento e é dentro de tais redes que as oportunidades criminosas são geradas e a colaboração para aproveitar tais oportunidades é organizada e executada” (MORSELLI, 2009). [tradução do autor]

Um desafio importante para o estudo do crime foi estabelecido por Sutherland (1947) *apud* Morselli (2009) com sua formulação do processo de associação diferencial. Não é suficiente simplesmente transpor teorias e modelos de vida social aos locais do crime, pois os fenômenos criminosos exigem suas próprias explicações. Dentro do quadro estabelecido, Morselli (2009) afirma que a primeira tarefa consiste, portanto, em estabelecer porque as redes de criminalidade são diferentes das redes sociais. O crime, afinal, é um fenômeno social, mas o criminoso, as redes e o comportamento criminoso em geral têm características distintas das contrapartes não-criminosas.

Existem muitas sobreposições entre redes não criminosas e criminosas, mas as redes de criminalidade não são simplesmente imagens espelhadas de redes não criminosas. Apesar de capturarem e amplificarem algumas características organizacionais de redes sociais, as redes de criminalidade se opõem a elas pelo caráter proscrito de suas atividades. Todas as redes sociais enfrentam algum nível de controle, mas uma rede de criminalidade enfrenta o controle sistemático de forças externas e internas. Esses controles vinculam seus participantes a algum estatuto de ação proibida no âmbito de uma rede de criminalidade.

Uma rede de criminalidade é estruturada e ajusta-se aos agentes de controle social, formais e informais, como Polícia, serviços públicos e comunidade, além de estar estruturada e ajustada a verificações entre os participantes, onde conflitos não podem ser resolvidos por um controle social legítimo. Este controle governa o ambiente geral, mas os participantes (como indivíduos ou como um coletivo) ajustam sua função ao contexto em que estão inseridos (MORSELLI, 2009).

Embora redes de criminalidade sejam configurações restritas, também é verdade que existe um controle recíproco entre membros. Um debate ao longo de quatro décadas estabeleceu algumas posições, entre elas a defesa da estrutura de crimes de alto nível, referindo-se à presença de organizações criminosas fortemente unidas, hierárquicas, monolíticas e intensamente regulamentadas em várias atividades, como as máfias. ((CRESSEY, 1969) *apud* (MORSELLI, 2009)).

Outros confrontaram esta posição, enfatizando as dificuldades para as coletividades criminosas organizarem-se de forma excessivamente regulada e insistir, em vez disso, na natureza solta e descentralizada da maioria dos grupos criminosos ((BLOCK e CHAMBLISS, 1981), (REUTER, 1983), (HALLER, 1990), (POTTER, 1994) *apud* (MORSELLI, 2009)).

Outro grupo de pesquisadores demonstrou que pode ocorrer descentralização de redes de criminalidade, através da introdução de algum fenômeno criminoso, onde tradicionalmente eram hierárquicas, uma vez que a lealdade e a ordem formal podem ser deslocadas por experiência individual e um espírito empreendedor ((ARLACCHI, 1983), (CRESSEY, 1969) *apud* (MORSELLI, 2009)).

Estudos mais recentes sobre o crime organizado e os modelos de rede sugerem uma estrutura com limites organizacionais associados com a hierarquia e a flexibilidade mantidas dentro de uma estrutura com configuração mais descentralizada ((MCLLWAIN, 1999), (RAAB; MILWARD, 2003) *apud* (MORSELLI, 2009)).

Segundo Waring (1993) e McAndrew (1999) *apud* Morselli (2009), rede é uma alternativa adequada aos termos tradicionais usados para denotar coletivos criminosos, particularmente o grupo. Nos contextos de co-ofensa, muitos fazem parte da mesma operação criminosa, mas eles nunca realmente se encontram. Assim, a estrutura de rede compreende este cenário, o grupo não. Em segundo lugar, a estrutura de rede fornece uma ferramenta para estruturar o agrupamento de recursos que é típico de crimes que exigem um maior nível de habilidade, sofisticação e colaboração complexa. Terceiro, as redes representam coletivos mais adaptáveis que os grupos. Os recursos adaptativos da rede estão na sua flexibilidade, que é favorável ao ambiente hostil e incerto geralmente associado ao crime.

Existem diferentes formas de aplicar o conceito de rede. Von Lampe (2003) *apud* Morselli (2009) distingue duas interpretações. Uma interpretação coloca a configuração de rede no meio de uma reta organizacional, com o indivíduo isolado na extrema esquerda e a

organização criminosa formal na extrema direita. Nessa perspectiva, a rede é uma forma de organização independente de outras formas organizacionais. Na segunda interpretação a rede transcende todas as formas de organizações. Dentro dessa representação, sistemas organizacionais formais podem emergir de uma rede. O que esta alternativa sugere é que uma rede é sustentada por formas organizacionais fixas e finitas que podem se dispersar no tempo.

Esta última interpretação é consistente com Ebel, Davidsen e Bornholdt (2003) *apud* Morselli (2009), que argumentam que redes de criminalidade são configurações complexas que não emergem de projetos predeterminados, mas dentro de processos auto organizados com interações dos participantes. Kleemans (2007) *apud* Morselli (2009), numa descrição das redes de criminalidade na Holanda, também apresenta um "efeito de bola de neve social", no qual as pessoas entram em contato com os participantes numa operação criminal em curso. Esses recém-chegados tornam-se participantes e, em empreendimentos posteriores, servem como vetores de entrada para as pessoas subsequentes que se sentem atraídas por operações criminosas.

Interações contínuas em redes de criminalidade se combinam para criar um contexto de ordem flexível. A ideia de ordem flexível começa com a suposição de que há um terreno comum a ser encontrado na interação entre indivíduos e interesses coletivos. Uma segunda reivindicação enfatiza a força organizacional das interações individuais e que uma autoridade central não é uma condição necessária para alcançar a ordem social. Em resumo, a rede é uma estrutura auto organizada que é essencialmente impulsionada por elementos nela presentes. Tais partes podem incluir uma variedade de atores, subgrupos, clusters e até mesmo hierarquias que são absorvidas na estrutura de rede (MORSELLI, 2009). A ideia não é nova e é consistente com a teoria de ordem social, que vai desde a ordem espontânea (ou emergente) de Hayek (1973) *apud* Morselli (2009) até o equilíbrio de cooperação de Axelrod (1983) *apud* Morselli (2009). A ideia também é coerente com a avaliação mais consistente das redes convencionais, onde a força da rede é a flexibilidade que oferece aos seus membros.

A ideia de uma ordem flexível também é compatível com os infratores oportunistas, de curto prazo e impulsivos. No entanto, os infratores individuais não possuem as competências necessárias para planejar e estruturar suas ações. Assim, estes se aproximam de outros criminosos, que realizam um planejamento extenso e organizado para executar seus crimes. O que o crime exige é a capacidade de reagir rapidamente e as redes são os sistemas organizacionais em que tais reações são mais adequadas onde a flexibilidade é a chave do sucesso das redes de criminalidade. De fora da rede, essa flexibilidade pode parecer um mero oportunismo, de curto prazo, ou o resultado de impulsos descontrolados. A partir de dentro da rede de criminalidade, no entanto, reações e ajustes rápidos são precisamente o que é necessário. (MORSELLI, 2009)

Morselli (2009) obteve acesso a casos que ofereciam oportunidades de análise de rede de criminalidade. Durante 10 anos recolheu dados com investigadores, analistas policiais, procuradores e advogados de 10 investigações policiais e processos judiciais. Estas redes operavam em torno de Montreal e Quebec, no Canadá, além de uma que atuava no leste dos Estados Unidos. Essas investigações combinaram-se para formar a base empírica para cinco casos estratégicos, com os quais várias questões sobre redes de criminalidade foram abordadas. Um caso tratou do contrabando de veículos roubados, e todos os outros de distribuição ilegal de drogas.

Cada rede de criminalidade serviu como uma base empírica para analisar casos estratégicos que permitiram avaliar as alegações relativas aos padrões e redes de criminalidade. Foram, em suma, ocasiões para testar proposições passadas sobre a estrutura do crime e oportunidades para explorar novos caminhos analíticos. Esses casos específicos, ao mesmo tempo, ofereceram o potencial de contribuir para teorias e perspectivas mais gerais sobre o crime organizado, a cumplicidade e a sociologia do crime.

A reconstrução destas redes baseou-se principalmente em dados físicos e computacionais, obtidos nos casos em questão, inclusive por interceptações de comunicação. As redes obtidas variavam em termos de atividades criminosas e dimensão de conteúdo, pois estabeleciam diversas atividades criminosas em torno de uma principal.

Morselli (2009) descreveu estes casos como: *Kreb's Terrorist Network*, *Project Ciel*, *Project Caviar*, *Projects Siren and Togo* e *Operation Springtime 2001*. Com os dados de cada estudo de caso acessados e reunidos, o próximo passo foi construir as redes.

2.3 Elementos de Redes Complexas

O estudo de redes complexas é interdisciplinar e abrange diversas áreas do conhecimento, como física, computação e sociologia. O termo redes complexas refere-se a um grafo que apresenta uma estrutura topológica não trivial, composto por um conjunto de vértices (nós) que são interligados por meio de arestas (laços) (BARABÁSI, 2003).

O estudo de redes na forma de grafos é um dos pilares da matemática discreta e teve início em 1735, quando Euler propôs uma solução para o problema das pontes de Königsberg, originando a teoria dos grafos.

Diversos aspectos do mundo real podem ser representados por meio de redes complexas a partir de analogias para resolução de problemas específicos. Assim, uma rede é então uma descrição de algo que é real e que pode ser representado por um grafo.

Segundo Ziviani (2007), diversas aplicações computacionais necessitam considerar um conjunto de conexões entre pares de objetos. Os relacionamentos oriundos destas conexões podem ser usados para responder diversos questionamentos como caminhos,

distâncias, alcance entre dois objetos. Para modelar tais situações o tipo abstrato chamado grafo é comumente usado.

Para Ziviani (2007), os algoritmos que manipulam grafos têm importância ímpar na computação, pois podem lidar com diversos problemas e apresentar soluções importantes para diversos modelos. São dois os tipos de grafos, direcionados e não direcionados. Segundo Ziviani (2007), “um grafo direcionado é um par (V, A) , em que V é um conjunto finito de vértices e A é um conjunto de arestas com uma relação binária em V ” (Figura 2(a)). Os círculos representam os vértices e as setas representam as arestas. Em grafos direcionados podem existir arestas de vértices para si mesmos, chamados *self-loops*. Um grafo não direcionado é um par (V, A) , em que o conjunto de arestas A é constituído de pares de vértices não orientados (Figura 2(b)). Este último é primordialmente importante porque utilizaremos neste trabalho.

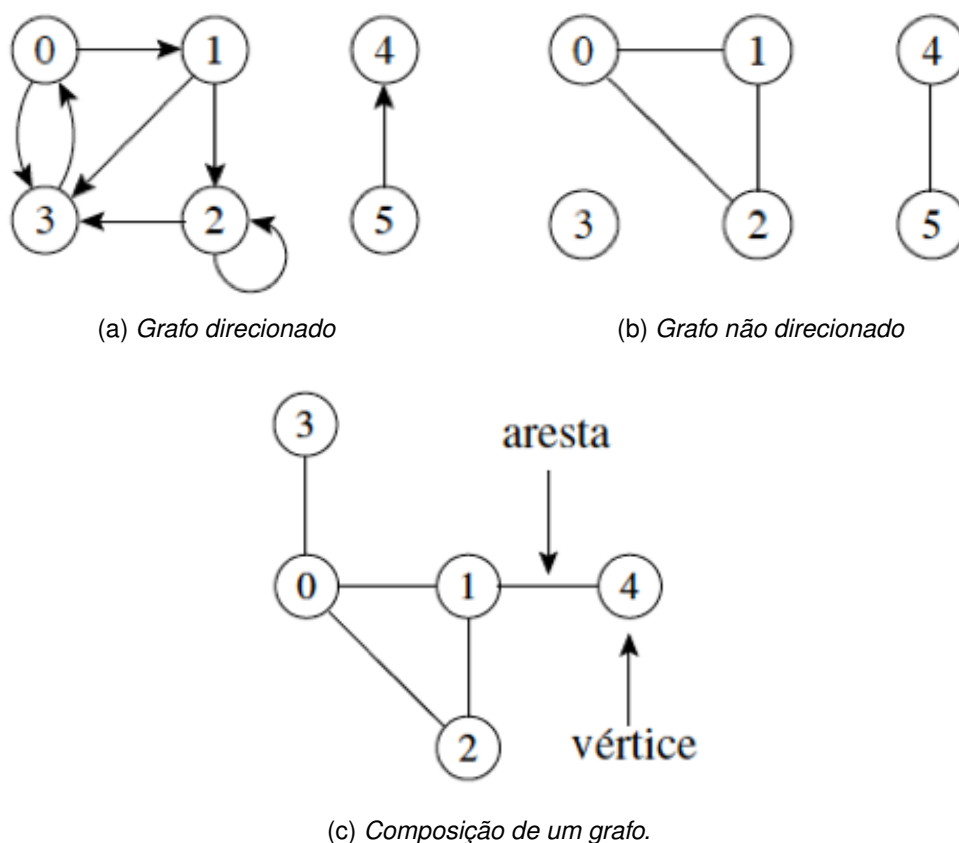


Figura 2 – Representação de grafos.

Doravante quando o termo grafo for usado, refere-se a grafo não direcionado.

Um grafo então é um conjunto de vértices e arestas (Figura 2(c)). Um vértice pode ter um nome e outros atributos. Uma aresta é uma conexão entre dois vértices.

Ziviani (2007) considera importante que os algoritmos em grafos sejam definidos como tipos abstratos de dados, onde um conjunto de operações possa ser associado a uma estrutura de dados e exista uma independência de implementação das operações.

As matrizes de adjacência e as listas de adjacência são duas representações usuais para os grafos. Por suas características e peculiaridades, utilizaremos um grafo, implementado por meio de uma lista de adjacência ou matriz de adjacência neste estudo de redes de criminalidade.

A matriz de adjacência de um grafo $G = (V, A)$ (Figura 3), contendo n vértices é uma matriz quadrada $n \times n$, ou simplesmente M_n , com pesos associados às arestas. Quando não existir peso para a aresta, é atribuído valor 0. A diagonal principal representa o relacionamento de um vértice para o mesmo vértice, também sendo atribuído um valor 0.

	C1	C2	C3	C4	C5	C6
C1	0	1	3	5	4	7
C2	1	0	2	4	3	6
C3	3	2	0	0	1	7
C4	5	4	0	0	5	0
C5	4	3	1	5	0	1
C6	7	6	7	0	1	0

Figura 3 – Representação por matriz de adjacência com pesos associados, onde 0 representa que não existe peso e os valores de 1 a 7 representam pesos associados.

Diversos aspectos do mundo real podem ser representados por meio de rede complexas a partir de analogias para a resolução de problemas específicos. É possível, por exemplo, modelar toda a estrutura de uma rede de criminalidade. Neste caso, os indivíduos conectados a rede referem-se aos vértices da rede, enquanto que os tipos de ligação representam as arestas do grafo.

Ao longo das últimas décadas a sociedade vislumbrou uma nova perspectiva de ver e influenciar as interações humanas, através das redes sociais. Isto sempre existiu, em dimensões e tamanhos diferentes, mas não fazia parte do dia a dia da sociedade. Vemos isto hoje, principalmente pelo uso de aplicativos como WhatsApp®, Facebook®, Instagram® etc. Tudo está conectado em rede, inclusive o crime.

A história humana é vista como uma rede social, que ao longo do tempo se modificou, mas pode realmente ser vivenciada, sentida, explicada e demonstrada pelo desenvolvimento tecnológico computacional. A interação social através de modelos tecnológicos computacionais enfraqueceu laços de interação humana, mas enriqueceu outras dimensões de relacionamento antes impossíveis.

Muita informação que utilizamos sobre criminosos podem ser representadas em uma estrutura de rede. Estas diversas estruturas têm complexidade e representações variadas, como tamanho, tipo de relacionamento, tipo de crime cometido, localização etc. Compreender este ambiente, dentro de uma grande rede, é uma tarefa complexa, que exige modelos e ferramentas capazes de trazer à tona a informação precisa que é requerida. (EASLEY;

KLEINBERG, 2010)

Quando navegamos em um banco de dados que contém informações sobre criminosos encontramos campos que contém referências a outros campos, e o criminoso desta rede move-se de um campo para outro ao seguir seus relacionamentos. Este banco pode ser modelado como um grafo, no qual os objetos são os criminosos e as conexões são os laços.

Um exemplo mais amplo é apresentado na Figura 4, onde estão representados a troca de *e-mails* entre funcionários de uma empresa. Tipicamente uma rede é representada com linhas unindo pares de objetos conectados por algum tipo de relação (laço).



Figura 4 – Redes sociais baseadas na comunicação e na interação a partir de *e-mails*.
Fonte: Easley e Kleinberg (2010)

As redes podem ser entendidas, explicadas e modeladas através da Teoria de Grafos. A Teoria dos Grafos lança as *“ideias fundamentais da análise da rede social, enquadrando uma série de teorias gráficas e conceitos nestes termos”* (EASLEY; KLEINBERG, 2010). A rede da Figura 4 apresenta algumas dessas ideias. Na rede, percebe-se que a comunicação é equilibrada, tendendo a ficar dentro de pequenas unidades organizacionais, mas também ultrapassando unidades organizacionais fronteiriças. Isto demonstra um princípio básico de redes sociais, onde os laços fortes são representados pelos laços sociais mais próximos e frequentes, em áreas fortemente ligadas da rede, enquanto os laços fracos, casuais e distintos, tendem a atravessar regiões representadas por organizações fronteiriças.

Tal dicotomia sugere uma maneira de pensar sobre as redes sociais em termos de seus densos bolsões de laços fortes e as maneiras em que interagem uns com os outros através de laços mais fracos. Em um ambiente profissional, é sugerida uma estratégia para percorrer a paisagem social de uma grande organização, identificando os buracos estruturais entre partes da rede que interagem muito pouco umas com as outras. (EASLEY; KLEINBERG, 2010) [tradução do autor]

Existem centenas de problemas práticos que a modelagem em grafos pode resolver, entre eles:

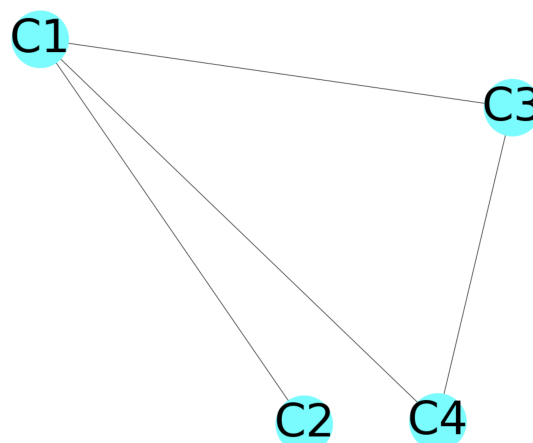
Pessoas concorrem ao processo seletivo em escolas, universidades ou algum tipo de emprego. Neste caso, os objetos são pessoas e instituições, e as conexões são as inscrições. Existem algoritmos em grafos para descobrir os melhores casamentos (do inglês *atching*) entre pessoas interessadas e posições disponíveis. Em um planejamento para visitar as principais cidades de uma região turística, uma pessoa pode estar interessada em saber qual é o caminho mais curto para realizar o roteiro. Nesse caso, os objetos são cidades e as conexões são as distâncias entre as cidades. (EASLEY; KLEINBERG, 2010)

Algoritmos para processamento de grafos na busca por informações relevantes constitui parte importante em busca de relacionamentos que possam ajudar a identificar redes de criminalidade, apoiado pela Análise de Redes Sociais.

Segundo Easley e Kleinberg (2010), Análise de Redes Sociais pode começar com uma matriz (Figura 5(a)), ou uma lista, que pode ser posteriormente visualizada em um sociograma (Figura 5(b)). A rede da Figura (Figura 5(a)) contém quatro nós (C1-C4). As conexões foram codificadas em formato binário, onde 0 indica a ausência de relação e 1 indica a presença de uma relação. Estas relações também podem ser codificados para valores, que representam os diversos tipos de relação que possam existir entre os nós.

	C1	C2	C3	C4
C1	-	1	1	1
C2	1	-	0	0
C3	1	0	-	1
C4	1	0	1	-

(a) Uma matriz de adjacência.



(b) Um grafo.

Figura 5 – Representações de matriz e grafo.

A Figura 5(a) representa uma matriz de adjacência binária e simétrica. C1 é o único nó a ter contato com todos os outros nós. C1 forma uma tríade com C3 e C4. C1 também serve como uma ponte entre C2 e os outros dois nós (Figura 5(b)). Em pequenas redes, a exibição do grafo é menos crucial, pois os padrões de conectividade são visíveis observando a matriz. Porém, redes maiores, como as que são apresentadas neste trabalho, são importantes para visualizar os relacionamentos de toda uma rede.

Para análise de rede social é indicado o uso de grafos bem elaborados, que apresentam substância e proposição, desenvolvidos a partir de representações das redes.

Para o olho treinado, um grafo desencadeia questões centrais: Como é estruturada a rede global? Os relacionamentos são de rede dispersa, densa ou segmentada? [...] Todas estas e várias outras questões vêm à mente ao explorar um grafo pela primeira vez. (ZIVIANI, 2007)

2.4 Redes *Multiplex*

A utilização das redes para modelar sistemas complexos têm crescido rapidamente nas últimas décadas, especialmente pela disponibilidade de novos e mais poderosos recursos computacionais. Cientistas das mais variadas áreas vêm utilizando estas novas metodologias com grande sucesso, tanto em aplicações reais, como em problemas teóricos, graças à forma simples de representar estes sistemas.

Sistemas complexos podem ser definidos como sistemas compostos por muitos constituintes interdependentes que interagem de forma complexa, usualmente não-linear (CRU-CITTI; LATORA; MARCHIORI, 2004). Nesta definição genérica encaixam-se uma infinidade de sistemas reais e artificiais, que vão da esfera dos sistemas logísticos (sistemas de produção, transporte), sistemas biológicos (genes, proteínas, bactérias), até sistemas sociais (organização humana, mobilidade, comunicação, disseminação de doenças).

Nos trabalhos seminais de Watts e Strogatz (1998) e Barabási e Albert (1999) foi mostrado que as relações entre os elementos que formam um sistema complexo podem ser representadas por redes. Muitas destas redes, reais e artificiais, são governadas pelo fenômeno conhecido como mundo pequeno (*small world networks*) e, em geral, possuem uma distribuição de grau que segue uma lei de potência, característica das denominadas redes livres de escala (*scale free networks*). Como resultado do estudo específico das propriedades destas redes, e reconhecendo sua aplicabilidade em uma infinidade de problemas, uma nova área da ciência, conhecida como *Network Science*, é hoje defendida por muitos pesquisadores (BARABÁSI, 2003; BARABÁSI, 2013; NEWMAN, 2010).

Nos últimos anos tem surgido uma nova visão sobre como modelar, de uma forma mais precisa, estes sistemas representados por redes, que não atuam isoladamente, mas numa grande rede de redes. Estas estruturas que contém muitas redes interconectadas são chamadas de *multilayer networks*, já que podem ser representadas como uma estrutura em camadas, onde cada uma delas representa uma rede específica (KURANT; THIRAN, 2006; GAO et al., 2012; BOCCALETTI et al., 2014; KIVELÄ et al., 2014). Cada rede que compõe estas estruturas possui uma natureza diferente e sua própria dinâmica. Redes biológicas, sociais, econômicas, climáticas e de transporte são alguns exemplos onde os seus nós participam, simultaneamente, de diversas dinâmicas, interagindo em diferentes níveis (BARGIGLI et al., 2015; DOMENICO; SASAI; ARENAS, 2016; CANTINI et al., 2015; GALLOTTI;

PORTER; BARTHELEMY, 2016; DONGES et al., 2011). Numa rede de transportes aéreo, por exemplo, os mesmos aeroportos estão conectados por diferentes companhias aéreas, as quais constituem as diferentes camadas; ou numa rede de transporte urbano, onde as camadas representam os diferentes meios de transporte (ônibus, metrô, trem *etc*). O entendimento dos princípios de conexão das redes *multilayers* constitui um problema muito desafiador para esta nova área.

Muitos trabalhos vêm sendo desenvolvidos com diferentes objetivos, como por exemplo, a detecção de comunidades (MUCHA et al., 2010; BATTISTON et al., 2016), a descrição de ferramentas matemáticas apropriadas (BIANCONI, 2013; DOMENICO et al., 2013a; KLEINEBERG et al., 2016; IACOVACCI; BIANCONI, 2016) e a caracterização de fenômenos emergentes destas estruturas (CARDILLO et al., 2013; BASHAN et al., 2013; RADICCHI; ARENAS, 2013; ÇOLAK; LIMA; GONZÁLEZ, 2016; BAGGIO et al., 2016; REQUEJO; DÍAZ-GUILERA, 2016).

As redes *multiplex* constituem um caso particular das redes *multilayer*, onde cada camada é constituída pelo mesmo grupo de nós e onde as suas interações nas diferentes camadas se dá só com a sua réplica. Uma rede social *multiplex*, por exemplo, está composta pelo mesmo grupo de indivíduos os quais participam de diferentes redes sociais (Facebook©, Twitter©, Instagram©) representadas nas diferentes camadas. Os exemplos de redes de transporte aéreo e urbano, descritos no parágrafo anterior, também podem ser modelados como redes *multiplex*. Na figura 6 está representada uma rede *multiplex* composta por 3 camadas. É possível ver nesta figura que as conexões entre os diferentes nós, só existem dentro de uma camada, e as relações entre camadas se dão no mesmo nó.

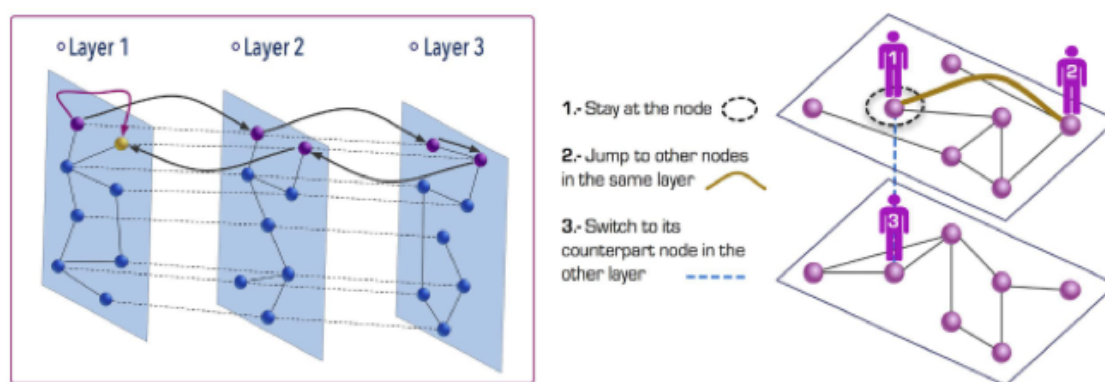


Figura 6 – Ilustração de camadas de Redes *multiplex*.

Fonte: Guo et al. (2016)

Numa rede de criminalidade, por exemplo, é possível modelar os nós como sendo os criminosos, e as ligações como as relações entre eles. As redes *multiplex* possibilitam ter uma visão mais abrangente e mais real, através da caracterização dos diferentes tipos de interações que os participantes da rede possuem. Por um lado temos as formas de comunicação entre eles, que se dá por diferentes formas, através de sistemas online, como

redes de telefonia ou redes sociais. Por outro lado, a propagação de acordos para prática de crimes normalmente é limitada ao conjunto de contatos com os quais um criminoso pode interagir fisicamente.

Como será demonstrado neste trabalho, a utilização de redes *multiplex* em redes de criminalidade permite identificar, por exemplo, os grupos que participam simultaneamente em diferentes crimes, identificar as pessoas que participam de vários crimes com grupos diferentes, como também estudar as similaridades destes grupos no sentido de organização. O desenvolvimento de um conjunto de ferramentas como métricas, algoritmos e métodos teóricos, direcionadas para este tipo de aplicações, foi um dos desafios deste trabalho.

Usando estas novas perspectivas, será possível identificar os pontos mais vulneráveis das redes de criminalidade e implementar ações para o seu desmantelamento.

2.5 Autômatos Celulares

Através dos estudos de John Von Neumann (KOWALTOWSKI, 1996), dentre outros, foram introduzidas técnicas computacionais que permitem a modelagem matemática de sistemas complexos.

Atman (2002) define autômatos celulares como “*modelos matemáticos simples totalmente discretizados – espacialmente, temporalmente e no número de estados de cada sítio*”, podendo estes modelos serem utilizados em diversas aplicações tecnológicas.

Segundo Adamatzky (2012), autômatos celulares são sistemas dinâmicos discretos, frequentemente descritos como representação de equações diferenciais parciais, que podem descrever sistemas dinâmicos contínuos. Por discreto entende-se que as variáveis de estado podem mudar seus estados em instantes de tempo discreto.

Ainda, segundo Atman (2002), autômatos celulares podem descrever fenômenos de diversos tipos de sistemas, entre eles computacionais. Os autômatos celulares têm regras temporais que definem sua própria evolução, a partir do próprio estado e de sua vizinhança. Estas regras podem ser determinísticas ou probabilísticas.

Os autômatos celulares determinísticos foram propostos por Von Neumann e estudados minuciosamente por Wolfram, que propôs a seguinte classificação:

1 Evolução para estado homogêneo; 2 Evolução para estado simples separados ou estruturas periódicas; 3 Evolução para padrão caótico; 4 Evolução para estruturas complexas localizadas. ((WOLFRAM, 1983) *apud* (ATMAN, 2002))

Wolfram (1983) *apud* Atman (2002) demonstrou que autômatos celulares exibem comportamentos complexos mesmo com regras locais. A classificação leva em conta que as

regras podem levar a uma auto-organização, que indicam uma formação espontânea dos padrões.

Autômatos celulares probabilísticos mantêm as mesmas características que um determinístico, exceto que as regras são agora probabilísticas.

Bar-Yam (1997), afirma que autômatos celulares podem ter formas e variedades diversas. O tipo de grade onde é aplicado é uma das principais propriedades. Assim, uma grade pode ser uma matriz unidimensional, ou mesmo uma matriz bidimensional, além de triângulos, hexágonos, redes *etc.*

Os autômatos celulares são compostos por três partes: célula, estrutura e regra de transição (ADAMATZKY, 2012).

A célula é o elemento básico dos autômatos celulares. Os estados ou valores das células são alterados conforme um conjunto de regras de transição, que depende da vizinhança ou da própria célula, ou seja, das células em torno da célula que será atualizada. O estado que autômatos celulares podem assumir deve ser também especificado. Tipicamente pode conter dois estados, 0 ou 1, ou uma cor, branco e preto, ambos binários. Autômatos celulares com maior alcance e complexidade podem conter outros valores, de acordo com a necessidade.

As estruturas dos autômatos celulares definem como as células serão organizadas numa rede. Autômatos celulares de uma dimensão são mais simples e fáceis de se manipular. Autômatos celulares são então uma coleção de células em uma grade, unidimensional, bidimensional ou mesmo multidimensional, que sofre evolução em espaços de tempo discreto, baseados em regras de conformidade com as células vizinhas.

Estas regras, aplicadas iterativamente, podem ser usadas em quantos passos de tempo for necessário, afetando seus estado. A vizinhança de autômatos celulares também afeta seu estado, pois de acordo com tipo de vizinhos, adjacentes ou não, o estado de uma célula pode variar. As regras de transição definem o estado do sistema. Uma regra define o próximo estado das células, ou seja, a mudança do estado da célula de acordo com sua vizinhança. Assim, o uso de autômatos celulares busca simular as interações entre as células por meio de regras simples, ou seja, deixar a interação entre os indivíduos surgir por meio de regras simples. O desafio aqui é representar sistemas e fenômenos por meio de modelos matemáticos.

Autômatos celulares também podem ser vistos como modelos matemáticos capazes de representar sistemas e fenômenos, de forma simples, porém rica na variedade de comportamentos. Isto os torna uma excelente ferramenta para estudar o comportamento de sistemas dinâmicos complexos. (BAR-YAM, 1997)

Autômatos celulares já são utilizados no combate ao crime. Oatley et al. (2008), afirmam que crimes com uso de armas no Reino Unido são um problema de difícil solução. Apesar

de severas penas, este crime é recorrente e vem aumentando. Este tipo de crime leva ao que chamam de “cultura de armas”, onde a conexão entre armas, droga e gangues violentas cria uma espiral de violência e crime. Projetos de pesquisa criaram uma série de metodologias para combater estas conexões.

Uma metodologia em especial associa diversas informações sobre armas, drogas e gangues para chegar a uma proposta de combate ao crime. A proposta utiliza autômatos celulares de forma a permitir aos tomadores de decisão que simulem diferentes cenários e vejam seus possíveis efeitos nos padrões de crime. Deste modelo surgem informações que foram incorporadas de diversas entidades, como locais, nomes, câmaras de TV *etc* (OATLEY et al., 2008).

A escolha da técnica de autômatos celulares para implementar a abordagem de modelo baseado em agentes parece ser a mais indicada para o propósito de modelar redes de criminalidade e analisar sua evolução e interligações, devido a sua flexibilidade, permitindo, ao final, simulações que permitam direcionar a atuação das forças policiais no combate ao crime organizado.

3 Metodologia

Tecnologias vêm sendo desenvolvidas para modelar e simular as relações humanas, aliando mundo real e computação, com o propósito de verificar e desenvolver modelos que permitam representar como estão estabelecidos estes relacionamentos (BOCCARA, 2010).

A possibilidade de entender comportamentos e utilizar modernas tecnologias permite uniformizar, com agilidade e precisão, os comportamentos que possam ser identificados e sirvam de referência para identificação de redes de criminalidade (BAYLEY, 2001). Compreender a interação entre seres humanos em torno de uma atividade em comum é uma tarefa de grande relevância e alta complexidade, pois envolve diversas questões culturais, econômicas, ambientais, psicológicas e de poder, dentre outras (SANTO; MEIRELLES, 2003).

As tarefas de modelar e simular ações humanas de grande complexidade apresentam abordagens diversas, que levam a estudos que combinam algumas delas. Dentre estas, usou-se nesta pesquisa: elementos de redes complexas, redes multiplex e autômatos celulares. Buscou-se identificar as redes de criminalidade, através dos dados contidos no Cadastro de Vínculos de Ocorrências da Polícia Militar de Minas Gerais. Assim, foi possível criar um ambiente computacional que fez o tratamento das informações coletadas, permitindo a simulação de aspectos dinâmicos, utilizando algoritmos que forneceram uma base de conhecimento para os objetivos estabelecidos.

3.1 Delineamento da pesquisa

O estudo de redes partiu de dois pontos fundamentais: o ser humano e a tecnologia. O ser humano assumiu papel importante neste contexto, interagindo com outros e com a tecnologia. O desafio de compreender comportamentos humanos, como eles atuam, agem, interagem, remeteu ao conhecimento de formas de representação para os agentes.

A ideia da rede social tornou-se comum com o recente e rápido desenvolvimento de sites de redes sociais e o crescimento das mídias sociais. As redes sociais incluem não somente redes digitais, mas também incluem redes de relacionamentos presenciais, associações e conexões políticas, transações econômicas entre empresas comerciais e relações geopolíticas entre estados/nações e agências internacionais. Ao longo dos anos, os sociólogos conceberam uma variedade de maneiras de examinar e interpretar relações de todos os tipos e, assim, sujeitá-las a formas sistemáticas de análise (LAZEGA; HIGGINS, 2014). O que veio a ser chamado de Análise de Redes Sociais (*Social Network Analysis* – SNA) não é um guia prático para fazer amigos ou construir contatos comerciais, embora

possa ajudar nessas atividades (SCOTT, 2017). Ainda, segundo Scott (2017), a referência a padrões sugere que SNA está particularmente interessada na construção de imagens e diagramas que revelam os padrões que geralmente não são aparentes para os observadores humanos. Isso é, de fato, verdade, mas a SNA procura ir além da visualização das relações sociais para examinar suas propriedades estruturais e suas implicações para as relações em redes.

A SNA vem sendo usada para abordar uma variedade de campos de pesquisa em diferentes contextos, com seus métodos sendo usados nas ciências sociais e comportamentais (ROSTAMI; MONDANI, 2015), para estudar a estrutura e evolução entre regiões (WAL; BOSCHMA, 2009) e comportamento organizacional (TICHY; TUSHMAN; FOMBRUN, 1979). No caso de redes de criminalidade, as aplicações variam de criminalidade em geral, redes terroristas, crime organizado e gangues de rua. A SNA tornou-se um método importante para compreender, avaliar e controlar as redes de criminalidade e tem implicações para uma política criminal. A importância dos métodos SNA reside na estrutura dos relacionamentos em uma rede, em vez de focar nas características dos atores individuais (RESSLER, 2006). SNA fornece uma estrutura para a abstração e representação de um fenômeno em termos de unidades interagindo e suas relações (KLOTZ et al., 2013). Compreende um conjunto de métodos e ferramentas para reunir, processar, visualizar e modelar redes sociais (WASSERMAN; FAUST, 1994). Neste contexto, a SNA tem sido uma ferramenta chave para análise de inteligência criminal desde a década de 1970 (MASYS, 2014), a partir de uma técnica básica na forma de análise de ligações de inteligência criminal e investigações, para a implementação mais recente de conceitos e medidas fundamentais de SNA em estratégias de resolução de problemas e avaliações de inteligência criminal (MASYS, 2014; LEINFELT; ROSTAMI, 2012).

A SNA vem servindo de guia na elaboração de políticas de segurança pública pelo mundo (CALDERONI; MORSELLI, 2010); consequentemente a análise de inteligência baseada na SNA tem implicações para a legislação e a política criminal de um Estado/Nação. Por conseguinte, é crucial compreender melhor a complexidade de diferentes dados/fontes, pois tem implicações para os resultados de estudos e avaliações de redes, uma vez que as redes de criminalidade são, por definição, difíceis de acessar; os dados dessas redes são complexos, na medida em que eles vêm de diferentes fontes e sofrem de diferentes vieses na coleta e análise, muitas vezes subjetivas.

A SNA utiliza medidas para identificar importantes indivíduos, baseado em sua posição social na rede, sua vizinhança, seus relacionamentos e a estrutura da rede (SCOTT, 2017). Sayama (2015) identifica 5 medidas de centralidade com esta finalidade: *Degree centrality*, *Betweenness centrality*, *Closeness centrality*, *Eigenvector centrality* e *PageRank*, onde cada medida de centralidade tem sua definição e indicação de uso na SNA.

As medidas de centralidade surgem no cenário da SNA e nos remetem a ideia de que,

numa rede, os indivíduos mais centrais são aqueles a partir dos quais podemos atingir qualquer outro com mais facilidade ou rapidez (LANDHERR; FRIEDL; HEIDEMANN, 2010). As medidas de centralidade identificam a posição de um elemento relativamente a outros na sua rede. A centralidade traduz também a ideia de poder. Assim, quanto mais central o indivíduo, maior influência e poder terá na sua rede (GAMA et al., 2015).

Estruturas de rede criminosas são conhecidas por serem sistemas muito complexos. Como descreve Morselli, *"as redes criminosas não são simplesmente redes sociais que operam em contextos criminosos"*. As configurações secretas que os cercam exigem interações específicas e recursos relacionais dentro e fora da rede. As redes criminosas, portanto, diferem das redes jurídicas, pois enfrentam um compromisso constante entre segurança e eficiência que afeta diretamente sua estrutura de rede. Por um lado, as atividades ilegais precisam ficar escondidas do governo ou da concorrência criminosa. Isso significa que a comunicação direta entre co-conspiradores em relação a atividades ilegais precisa ser restrita a um mínimo. Por outro lado, os riscos devem ser tomados em tempos de ação, exigindo muitas vezes comunicação altamente eficiente e confiança entre os participantes. As redes criminosas, portanto, equilibram continuamente entre eficiência e segurança de acordo com as circunstâncias dadas das atividades ilegais (DUIJN; KASHIRIN; SLOOT, 2014).

Muitos pesquisadores de redes criminosas concordam que estudar a dinâmica em redes criminosas é provavelmente o obstáculo mais desafiador enfrentado por qualquer um que se aproxime dessa área. Embora reconheçamos a complexidade e a dificuldade que está associada ao estudo da mudança nas redes sociais, buscamos neste trabalho capturar essas dinâmicas dentro de uma estrutura computacional (DUIJN; KASHIRIN; SLOOT, 2014).

O estudo de criminosos em rede é fascinante e desafiador, pois revela a demanda de respostas novas e mais adequadas no combate ao crime. Até o momento, as abordagens utilizadas na literatura consideravam as redes de criminalidade como redes unidimensionais.

A confiança entre indivíduos é a base de uma rede de criminalidade. Nela se sustenta o sucesso ou o fracasso das ações ilegais praticadas por seus indivíduos. Os relacionamentos múltiplos tendem a mostrar relações de confiança. A multiplexidade, propriedade de vários tipos de relacionamentos existirem entre pares de indivíduos, permite analisar como os indivíduos podem estar ligados através de mais de um tipo de relacionamento, ocupando posições que oferecem diferentes relações (SMITH; PAPACHRISTOS, 2016).

Para viabilizar a proposta, o estudo seguiu a seguinte metodologia para sua realização:

1. Revisão bibliográfica sobre modelagem matemática e computacional, técnicas de modelagem e simulação, métodos estatísticos e computacionais;
2. Mineração de dados em um Banco de Dados, com análise e uniformização destes dados para gerar os arquivos necessários para o estudo;

3. Modelagem para identificação de redes de criminalidade;
4. Simulação de redes de criminalidade;
5. Modelagem de redes *multiplex*.

3.2 Coleta e tratamento de dados

O dados para este projeto foram oriundos do CVO, implantado na REINT. O Acesso aos dados foi explicitamente autorizado pelo Chefe do Estado Maior da Polícia Militar de Minas Gerais, cuja cópia do memorando de autorização encontra-se no Anexo A.

Para este projeto, a escolha da linguagem de programação Python deu-se por ser uma linguagem baseada em Software Livre, simples e clara. Apesar da simplicidade, é uma linguagem poderosa para desenvolvimento de grandes projetos de sistemas. Por ser Software Livre, regida pela Licença Pública Geral (GPL – *General Public License*¹), pode ser utilizado de forma gratuita, tendo o código fonte a disposição.

Várias áreas da computação têm-se beneficiado pela linguagem Python, como inteligência artificial, banco de dados, animação 3D, web *etc*. Além disso, Python é uma linguagem completa, com uma biblioteca diversificada, desenvolvida e testada por inúmeros colaboradores (MENEZES, 2010).

Analisada e identificada a linguagem a ser utilizada, a próxima etapa foi preparar o ambiente de desenvolvimento.

O Python 2.7 é um padrão de desenvolvimento a longo tempo e receberá atualizações até 2020. Já a versão 3 introduziu alterações importantes na linguagem, que muitas vezes não são suportadas pela versão 2.7. Assim, com base na evolução constante, o termino de atualização e nas bibliotecas existentes, todo código foi implementado para ser funcional na versão 3.6 do Python.

Todo ambiente foi instalado no MAC OSX Sierra, sendo este ambiente composto:

- Python versão 3.6 e suas bibliotecas, como Numpy, Pandas, Networkx, Matplotlib, IGraph *etc*;
- Setuptools, pip, virtualenv e anaconda, para facilitar a instalação e uso de bibliotecas Python;
- IDE PyCharm e Jupyter, que permitiram conclusão de código quase perfeita, bom suporte para ambientes virtuais e bom suporte para frameworks web, além de serem Software Livre;

¹ GPL baseia-se em 5 liberdades: a liberdade de executar o programa, para qualquer propósito (liberdade nº 0); a liberdade de estudar como o programa funciona e adaptá-lo às suas necessidades (liberdade nº 1). O acesso ao código-fonte é um pré-requisito para esta liberdade; a liberdade de redistribuir cópias de modo que você possa ajudar ao seu próximo (liberdade nº 2); a liberdade de aperfeiçoar o programa e liberar os seus aperfeiçoamentos, de modo que toda a comunidade beneficie deles (liberdade nº 3); o acesso ao código-fonte é um pré-requisito para esta liberdade (liberdade nº 4).

- Máquina virtual Parallels;
- MS-Windows 10 na máquina virtual;
- MS-SQL 2008 na máquina virtual.

Como metodologia de desenvolvimento de software, foi utilizado o *Test Driven Development* (TDD). Com TDD especificamos o código em detalhes, criando testes executáveis e rodando-os de maneira que eles mesmos testaram o código. TDD serviu para diagnosticar precocemente *bugs* que poderiam vir a ser problemas na finalização do projeto. Genericamente, quando escrevemos um código, começamos escrevendo o teste, uma classe que testou o código, assim, testamos o código e o remodelamos até que os testes não falharam mais. Então a TDD pode ser entendido como uma técnica de programação onde todo o código produzido é criado em resposta a um código que falhou. (JANZEN; SAIEDIAN, 2005)

4 Trabalhos Relacionados

Neste Capítulo são descritos alguns trabalhos relacionados, a relação entre eles e o trabalho proposto, além da relação com os objetivos mencionados no Capítulo 3. Em particular, consideramos os trabalhos de Rostami e Mondani (2015), Duijn, Kashirin e Sloot (2014) e Smith e Papachristos (2016).

4.1 A complexidade de rede de dados criminosos: um estudo de caso de suas consequências para o crime, controle e estudo de redes

Rostami e Mondani (2015) afirmaram que a partir de diferentes fontes de dados podemos estudar diversas perspectivas de redes. O objetivo de seu trabalho foi estudar como diferentes conjuntos de dados influenciam o resultado de rede criminosos. Foi utilizado um caso de gangue de rua sueca, onde foi ilustrado a complexidade e confiabilidade de fontes empíricas na análise de redes criminosas numa perspectiva de rede.

A Análise de Redes Sociais foi utilizada para analisar diversas questões e seu uso comprovado para análise de redes criminosas. Os métodos estabelecidos em Análise de Redes Sociais se mostraram eficientes para detecção, redução e ruptura de atividades criminosas, evidenciando como agências policiais estão aplicando estes métodos para conter o crime.

Os dados do estudo foram extraídos do *National Swedish Police Intelligence*, cuja função é a coleta de dados sobre associação de gangues. Inicialmente foi criado um conjunto de dados com 28 membros de gangues e a partir destes indivíduos foram identificados outros que tinham ligações com estes, no período de 2006 a 2010. Foram então criados três conjuntos de dados para análise: rede baseada em inteligência (IN), rede baseada em vigilância (SN) e rede baseada em comparsas (CN).

Foram analisados os conjuntos de dados usando três técnicas: visualização, similaridade e medidas de rede. A visualização permitiu representar as diferentes estruturas de forma a facilitar a compreensão e comparação de propriedades. A similaridade permitiu desenvolver métodos para verificar/comparar as redes. As medidas de centralidade permitiram verificar características particulares das redes criminosas.

Indivíduos interagindo em um grupo social levam consigo diferentes características pessoais, podendo realizar diferentes atividades e ter relacionamentos com diversos outros indivíduos. Analisar estes relacionamentos permitiu identificar os indivíduos mais impor-

tantes ou mais importantes que outros. As medidas de centralidade permitiram determinar quão importante é um indivíduo dentro de uma rede. No estudo foram usadas duas medidas de centralidade: *degree* e *betweenness*.

Além de medidas de centralidade, o estudo abordou o coeficiente de *clustering*, uma medida que apresenta como resultado a razão entre o número de pares de nós adjacentes e suas conexões.

Para o estudo foi utilizado o software livre Gephi, que possibilitou a visualização, comparação e medidas.

A importância do trabalho foi a comparação de diferentes redes de inteligência disponíveis, buscando entender a complexidade das redes, analisando a similaridade dos gráficos obtidos, bem como as três medidas de rede.

Com as técnicas de Análise de Redes Sociais foi possível realizar análises sofisticadas dos dados, onde os resultados mostraram que diferentes conjuntos de dados para o mesmo fenômeno produzem imagens fundamentalmente diferentes; os mesmos indivíduos têm diferentes classificações de importância, dependendo do conjunto de dados; as medidas de rede têm forte importância para controle do crime. Por fim, o estudo revelou que agências de policiamento podem estabelecer estratégias para controle de gangues, usando a Análise de Redes Sociais.

4.2 A ineficiência relativa da interrupção da rede criminosa

Duijn, Kashirin e Slood (2014) afirmaram que o crime organizado constitui uma grande ameaça para sociedade. Em especial no estudo, as organizações criminais internacionais de drogas tendem a se infiltrar em diversos ramos legais da sociedade.

Agências policiais de todo mundo buscam formas eficientes de interromper estas organizações, preferencialmente em seu estágio inicial. Estas organizações criminosas devem ser consideradas como redes sociais que formam coletivos, em vez de organizações com características únicas, como relações internas flexíveis e hierarquizadas.

No estudo de redes criminosas, fixou-se o objetivo de atacar o líder, como forma de dismantelar uma rede. Novos estudos surgiram e mostraram que este objetivo não deve ser o principal. A fluidez e flexibilidades das redes criminosas sugerem o uso de novas estratégias.

As redes criminosas não são estáticas, mas dinâmicas, podendo sofrer alterações em sua estrutura por diversas razões, até mesmo ataques visando o controle destas redes. Estas mudanças a caracterizam como sistemas adaptativos complexos.

O objetivo do estudo, diante do quadro exposto, foi desvendar a dinâmica da interação entre ruptura e resiliência nas redes criminosas e encontrar estratégias para interrupção

de rede criminosa. Para isto, foram combinados métodos de Modelagem Computacional e Análise de Redes Sociais para simular o comportamento de uma rede criminosa envolvida no cultivo de *cannabis*, através de dados de inteligência da Polícia Holandesa.

A ruptura de uma rede criminosa pode ser obtida através de três pontos: uma redução da taxa de fluxo de informações na rede, uma redução na capacidade de conduzir suas tarefas ou uma falha ou desaceleração no processo de tomada de decisão. Para criação de estratégias de interrupção de redes criminosas, duas são as abordagens principais: a abordagem do capital social e a abordagem do capital humano. A primeira visa posições estratégicas em que os indivíduos ocupam nas redes criminosas, a segunda visa o estoque de competências, conhecimentos, atributos sociais, conhecimentos e personalidade.

Na abordagem do capital social a identificação dos indivíduos pelo grau de centralidade foi fundamental. Já na abordagem do capital humano a identificação os indivíduos pelas suas tarefas na estrutura da rede e sua eventual substituíbilidade foi critério importante para interrupção.

Como consequência da interrupção, uma rede criminosa desenvolve a capacidade de absorver e suportar sua ruptura, adaptando-se a mudanças, que é chamado de resiliência da rede. A resiliência depende da redundância da estrutura de rede, que permite que seus membros assumam outras tarefas na estrutura da rede. Substituições são muito encontradas em redes criminosas onde houve uma tentativa de ruptura, caracterizada como a interrupção da rede.

Na tentativa de desvendar a dinâmica dentro de redes criminosas, o estudo passou por simulações e observações dos mecanismos de ruptura e de resiliência em uma rede criminosa envolvida no cultivo de *cannabis*.

O banco de dados continha 29.346 indivíduos e 47.127 ligações, entre o período de 2008 e 2011, divididos em dois conjuntos, de registros de detenção e atividades criminosas.

A primeira tarefa foi calcular a distribuição de grau da rede. Se a distribuição de grau segue a lei de potência, é uma rede livre de escala. Isto significa que a rede depende de vários atores com grau relativamente alto, os chamados *hub*. Se esses *hub* forem atacados, a rede se dividirá em sub-redes.

Para testar a eficiência de diferentes estratégias para interromper a rede, foram realizadas simulações de interrupção de rede, visando frustrar a cadeia de valor da atividade criminosa, removendo atores principais da rede. A ordem de remoção dependeu da estratégia utilizada: interrupção aleatória, estratégia de *degree*, estratégia de *betweenness*, estratégia de grau de cadeia de valor e estratégia do papel da cadeia de valor específico. Todas as cinco estratégias foram simuladas no estudo, medindo o efeito que elas tiveram na rede.

A resiliência da rede foi simulada por algoritmos de desmantelamento da rede: algoritmo

de recuperação aleatória, algoritmo de recuperação de distância e algoritmo de recuperação de graus. No primeiro algoritmo, os candidatos foram escolhidos aleatoriamente, sem nenhuma preferência. No caso do segundo algoritmo, os indivíduos com menor distância foram mais propensos a substituição. Já no terceiro algoritmo os indivíduos com mais alto grau foram os primeiros a serem escolhidos para substituição.

Depois que as estratégias de interrupção e recuperação foram aplicadas ao mesmo tempo, foi medido o impacto que isto tem na estrutura da rede, em termos de eficiência e segurança. O trabalho introduziu duas medidas: de eficiência e densidade. A métrica de eficiência mostra quão eficiente os atores dentro da rede podem se comunicar e trocar valores entre si. Já a métrica de densidade destina-se a dar uma ideia de como os caminhos de comunicação na rede são capazes de levar as informações para os participantes da rede. Os valores estão entre 0 e 1, onde 1 a rede está completa e 0 indica que a rede está completamente desmontada.

O estudo apresentou o impacto da recuperação dinâmica da rede na eficiência de diferentes estratégias de interrupção de redes criminosas. Diferentes mecanismos de recuperação foram investigados, de forma a avaliar seus efeitos sobre a estrutura da rede. Indivíduos alvos para estratégias de interrupção de rede são aqueles com alto grau e em posições conhecidas na rede criminal. O estudo também indicou que o processo criminal de cultivo de *cannabis* é organizado em uma estrutura flexível e adaptável, sendo altamente resiliente contra a interrupção da rede.

4.3 Confie em teu vizinho desonesto: multiplexidade nas redes de crime organizado de Chicago

Smith e Papachristos (2016) exploraram a multiplexidade em um período da história dos EUA, a Era da Proibição de Chicago, quando as fronteiras entre os mundos criminoso e legítimo mudaram drasticamente, um período onde Chicago foi dominada pelo crime organizado.

Deixando para trás a análise unidimensional do crime, o estudo focou nas inter-relações entre redes criminosas, redes legítimas e redes pessoais, onde o crime organizado existiu e transitou nestes três mundos.

A multiplexidade é conhecida como a propriedade de rede onde vários tipos de relacionamentos podem existir entre um par de indivíduos. A multiplexidade acrescenta profundidade às relações sociais, baseando-se no laço existente entre um par. A multiplexidade pode fornecer uma base de confiança onde um novo relacionamento se sobrepõe aos relacionamentos anteriores, diminuindo incertezas e aumentando a reciprocidade.

Como uma característica importante do crime organizado, a multiplexidade gerou caráter

único e um único conjunto de problemas, organizando a busca de grupos criminosos através de diversos tipos de conexões, ultrapassando o caráter criminoso e entrando nas relações pessoais e legítimas na sociedade. O cultivo de laços *multiplex* mostra que indivíduos corruptos confiam em seus vizinhos, representando um caso único para análise do crime organizado.

O estudo teve dois pontos focais: mapear como a multiplexidade definia o crime organizado em Chicago e como a multiplexidade contribuiu estruturalmente para as redes naquela época. As descobertas trouxeram implicações para o estudo do crime organizado e o estudo das redes sociais. O estudo destacou como a multiplexidade ligou o submundo e a sociedade, a dificuldade de localizar fontes confiáveis e demonstrou como a multiplexidade pode integrar grupos sociais diferentes, especificamente sob condições de incerteza e risco.

O mapeamento sistemático sobre das redes permitiu expandir o foco além de *gângsters*, fornecendo um caminho para compreensão da estrutura do crime organizado, bem como o papel da multiplexidade para a sociedade legítima.

Os dados do estudo foram extraídos de diversas fontes no período de 1900 a 1950, gerando um banco de dados com 3.000 indivíduos e 15.000 ligações sociais que denotavam algum aspecto relacionado com o crime organizado. O estudo dividiu este banco de dados em três esferas: criminal, pessoal e legítima, criando assim três redes que foram analisadas.

Como resultado da sobreposição destas três redes, foi analisada a propriedade de multiplexação, onde foi mapeada a prevalência da multiplexidade. Tomadas duas a duas, estas redes foram analisadas, demonstrando a importância de colegas, associados e membros de famílias na composição do crime organizado.

Foram criados gráficos que estimularam padrões, tendências e dependências dos dados relacionais. O líder destas redes, o notório e conhecido Al Capone, teve uma forte influência nos modelos criados, estando presente nas redes criminal, pessoal e legítima. Tinha um alto grau nestas redes, porém com maior significância na rede criminosa.

A multiplexidade produziu grandes e relevantes estimativas nos modelos criados. As multiplexidade criminal e pessoal e a multiplexidade criminal e legítima explicaram, em parte, a estrutura de dependência do crime organizado em Chicago. Pares e membros de famílias também desempenharam papel importante neste mundo, onde a multiplexidade criminal e pessoal serviu de ponte entre os dois conjuntos. Em todos os modelos criados, a multiplexidade operou como mecanismo que ajudou a gerar a estrutura global das redes observadas. O crime se organizou quando entrou em esferas legítimas, como contribuições de campanhas políticas, controle de empresas e, até mesmo, quando membros da sociedade usaram suas posições de influência dentro da esfera criminal, como quando juízes e as forças policiais aceitaram subornos.

O estudo afirmou que a multiplexidade é rara na sociedade moderna, onde fortes

laços multiplexados representam apenas uma fração do total de conexões de uma pessoa. Apesar desta pouca multiplexidade, foram os laços multiplex que ligaram as atividades e empreendimentos do submundo de Chicago à sociedade legítima.

A multiplexidade implicou em uma base de confiança e obrigação que levou a ação social e integrou as relações sociais. Mesmo raros, os laços multiplex foram importantes, pois fomentaram estruturalmente as redes. Os laços multiplex forneceram a confiança necessária para interligação entre vizinhos em uma rede.

5 Resultados

Neste estudo, tivemos a oportunidade de acessar o Banco de Dados do Cadastro de Vínculos de Ocorrências da Polícia Militar de Minas Gerais. O conjunto de dados extraído são as fontes de informações de redes de criminalidade, caracterizados como dados de inteligência, infratores, comparsas, grupos criminosos, gangues¹ etc. Neste estudo, exploramos diferentes conjuntos de dados da rede e sua influência nos resultados dos estudos de redes de criminalidade e suas consequências para avaliação de inteligência de segurança pública. Isto foi feito construindo grafos com os conjuntos de dados extraídos, comparando-os e aplicando diversas técnicas oriundas da Física Estatística.

Segundo Lazega e Higgins (2014), *“Tecnicamente, a análise de redes pode estudar várias redes separadamente. Entretanto, ela deve também sobrepor várias redes e reconstruir uma visão de conjunto transversal da estrutura relacional”*. O estudo que segue faz exatamente isto, identificando as redes e os líderes, decompondo as redes em camadas para identificação de relacionamentos baseados em tipos de crimes e sua evolução temporal.

5.1 Desenvolvimento de Protocolo para Identificação de Rede de Criminalidade

Com o ambiente preparado, a primeira tarefa foi importar o banco de dados do CVO no MS-SQL 2008, versão que a REINT utiliza. Feita a importação foram analisadas todas as tabelas e relacionamentos, de forma a estabelecer quais dados seriam úteis para o trabalho. Neste ponto, as tabelas do CVO foram identificadas para uso no trabalho. A tabela de indivíduos, que contém dados de 152.973 criminosos; tabela de vínculos, que contém 55.191 vínculos entre os criminosos; a tabela de gangues, que contém a identificação de 11.978 criminosos e suas respectivas gangues de atuação; a tabela de organização criminosa, que contém a identificação de 1.297 criminosos e suas respectivas organizações criminosas.

Para criar um arquivo texto contendo os criminosos e seus relacionamentos foi preciso estabelecer regras e políticas próprias de mineração e extração de dados, utilizando algoritmos previamente desenvolvidos em Python, utilizando as bibliotecas Numpy, Pandas etc. A Figura 7 ilustra a $matriz_n$ dentro do arquivo, onde $n = 152.973$, representa o número de criminosos extraídos do banco de dados. Esta matriz de adjacência vai gerar grafos não direcionados. O fato de que a matriz é simétrica remete a possibilidade de ela ser percorrida somente na diagonal superior ou inferior para gerar o grafo, representando isto uma redução

¹ Associação de malfeitores; bando, quadrilha

no tempo de execução do algoritmo a ser gerado. Por definição neste trabalho, a diagonal principal, identificada pelas células C_{ii} , conterão '-' como conteúdo, uma vez que não há relacionamento de um criminoso com ele mesmo.

	C1	C2	C3	C4	C5	C6	C7	C8
C1	-	1	1	1	1	1	1	1
C2	1	-	0	0	0	0	0	0
C3	1	0	-	1	1	1	1	1
C4	1	0	1	-	1	1	1	1
C5	1	0	1	1	-	0	1	1
C6	1	0	1	1	0	-	1	1
C7	1	0	1	1	1	1	-	1
C8	1	0	1	1	1	1	1	-

Figura 7 – Ilustração da matriz de adjacência obtida pelo relacionamento de indivíduos do CVO.

As tabelas do banco de dados foram migradas para arquivos com extensão CSV, através de *queries* no MS-SQL. Os arquivos passaram por análises e uniformização, através de códigos em Python, para adequá-los às necessidades do projeto.

Os arquivos CVS que contém as informações para o estudo foram importados através de códigos já escritos, conforme Figura 8, que ilustra o vínculo entre indivíduos.

	idind1	idind2	vin1	vin2	lancd
0	6425CD95-5577-43E0-9CF4-FA3C50F8BC93	7C7E01D5-9E6C-4AAE-90ED-89FA13A5DF2A	NAMORADO	NAMORADA	2013-10-04 10:17:00
1	70559A60-12C8-4961-98D7-6B63E98D8E20	24ECB17A-9A4D-4001-B154-CF41875790CE	TRÁFICO DE DROGAS	TRÁFICO DE DROGAS	2006-01-01 00:00:00
2	E093D080-492A-4795-92D8-9243DE4763B8	377F91D9-0B32-4EAC-872A-7D34BA1019D6	COMPARSA	COMPARSA	2013-05-08 11:46:00
3	D56C579C-5ECA-42EB-A266-D23513116663	632A AFC5-09A9-4BB9-9C2D-FB9ECA2C3B39	COMPARSA	COMPARSA	2013-07-01 17:42:00
4	FCDD5763-3CF1-4BA0-AE93-752486012F43	976A126A-C976-48F6-8FA3-62356C611B39	COMPARSA	COMPARSA	2011-11-03 09:13:00
5	82749EAC-4F20-4198-9118-7F6AF2C7B303	CD83F3D6-5358-464B-99E8-8A2BF1FAD9EA	COMPARSA EM ASSALTOS	COMPARSA EM ASSALTOS	2009-04-23 22:50:00
6	91841D89-F397-4416-B6FC-901D223D319E	7F66F3C5-563E-47E2-9B8A-4C7EE519C311	COMPARSA	COMPARSA	2010-11-30 17:04:00
7	03DD21AE-C134-42DA-95C8-2790783FBFB6	AC3E91A0-E568-4655-8F8F-87DE65C86495	TRAFICO DE DROGAS	TRAFICO DE DROGAS	2013-03-03 19:11:00
8	6AD07D61-4825-4045-BEE0-18E70ADC8FCB	2D8B24EA-39EB-484A-B163-C291259032EE	COMPARSA	COMPARSA	2009-04-30 17:31:00
9	2799A5EB-0AF5-4528-BDB7-0BE7A64ECB95	3265983F-9C86-4120-B3D0-4743808DDE02	COMPARSA	COMPARSA	2013-01-13 23:02:00
10	E95A2E69-23BC-4D28-9473-DA762B370461	31F6C80F-070F-4BB6-AA53-F7EBAB28FDA0	QUADRILHA DE ROUBO A BANCOS NO ESTADO DE MINAS...	QUADRILHA DE ROUBO A BANCOS NO ESTADO DE MINAS...	2007-11-26 10:16:00

Figura 8 – Ilustração dos vínculos de indivíduos, onde são apresentados os identificadores únicos de cada indivíduo, os tipos de vínculos estabelecidos e a data do lançamento

As informações extraídas do banco de dados, depois de tratadas e analisadas por algoritmos desenvolvidos para o estudo, identificaram redes de criminalidade com 46.239 vínculos e 34.505 indivíduos. A complexidade das redes de criminalidade identificadas e

modeladas a partir de redes reais com muitos nós e elevada densidade de relações, faz com que a sua visualização se torne confusa e difícil de interpretar.

Para efeito de criação do modelo de estudo, foi utilizada uma rede com menos vínculos e indivíduos. Assim, foi escolhida uma rede que no ano de 2013 foi alvo de uma operação de inteligência e posterior prisão de criminosos. À época, a identificação da rede só foi possível após três meses de trabalho, consumindo muitos recursos, humano e material, sendo identificados 58 indivíduos e 77 laços entre eles.

No projeto foram implementados algoritmos para cumprir os objetivos propostos em conjugação com uma plataforma de visualização para a exploração de uma rede de criminalidade.

Foi desenvolvido um algoritmo que permite filtrar redes de criminalidade, de acordo com parâmetros desejados e pré-estabelecidos. Neste trabalho a busca de rede de criminalidade teve como parâmetros as seguintes características de um indivíduo: prática de crimes² de homicídio, sequestro, extorsão mediante sequestro, roubo e estupro, além de participação em uma organização criminosa.

Este algoritmo gerou um arquivo de 187 linhas, que identifica os indivíduos desta rede, que mantêm vínculos entre si e serão objeto de modelagem e estudo neste projeto. As 187 linhas do arquivo contêm vínculos repetidos, além de vínculos bidirecionais, como exemplo [(3,5), (5,3)]. Como o estudo está focado em grafos não direcionais, os vínculos bidirecionais e repetidos não serão diferenciados.

Funções que analisam e tratam estes dados foram escritas de forma a isolar os vínculos repetidos e bidirecionais.

Com a implementação de funções dentro do algoritmo, foi possível identificar, de forma rápida, que a rede de criminalidade contém 92 indivíduos (*nodes*) e 123 laços (*edges*) únicos. Todos os indivíduos e laços identificados constavam na operação de inteligência de 2013, tendo agora identificado mais indivíduos e laços em decorrência da automatização do processo, que gerou também mais assertividade. Todos os dados foram anonimizados antes da análise, de tal maneira que cada indivíduo recebeu um número de identificação único, sequencial, de 1 a 92.

Para efeito de comparação, através dos códigos desenvolvidos, o trabalho de Inteligência que deu origem a este estudo, que durou 3 meses para ser finalizado em 2013, foi reduzido para poucos segundos.

Através dos algoritmos e análises desenvolvidos, foi possível identificar graficamente a rede de criminalidade, vista nas Figuras 9 e 10

No estudo, identificamos 4 conjuntos de dados sobre rede de criminalidade: o primeiro

² Crimes que compõem o Índice de Crimes Violentos (ICV)

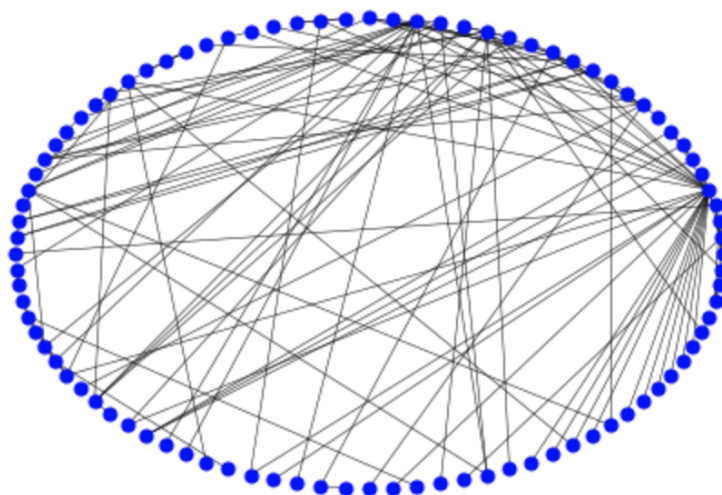


Figura 9 – Ilustração gráfica da rede de criminalidade utilizando gráfico tipo circular.

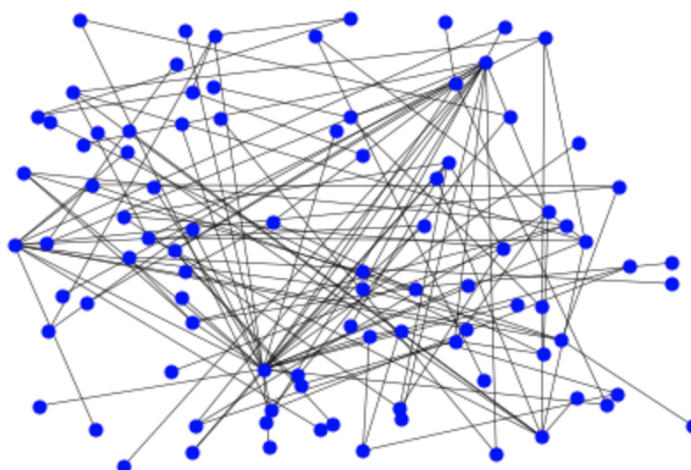


Figura 10 – Ilustração gráfica da rede de criminalidade, utilizando gráfico tipo randômico.

composto pelos infratores e comparsas, que recebeu o nome de Rede de Inteligência (RI); o segundo, uma sub-rede da RI, composto pelos infratores, que recebeu o nome de Rede de Autores (RA); o terceiro, também uma sub-rede da RI, composto pelos já condenados na justiça, que recebeu o nome de Rede de Condenados (RC); o quarto, composto por membros de gangue, que recebeu o nome de Rede de Gangue (RG).

5.2 Estatísticas de Rede de Criminalidade

A rede de criminalidade inicial deste estudo é a Rede de Inteligência (RI), vista na Figura 11. Esta rede tem 92 indivíduos e 123 ligações, sendo: 81 autores de infração e 11 comparsas; 83 indivíduos do sexo masculino e 9 indivíduos do sexo feminino; a idade média dos indivíduos desta rede é de 31 anos, sendo o mais novo com 19 anos e o mais velho

com 55 anos; é uma rede com estrutura totalmente conectada.

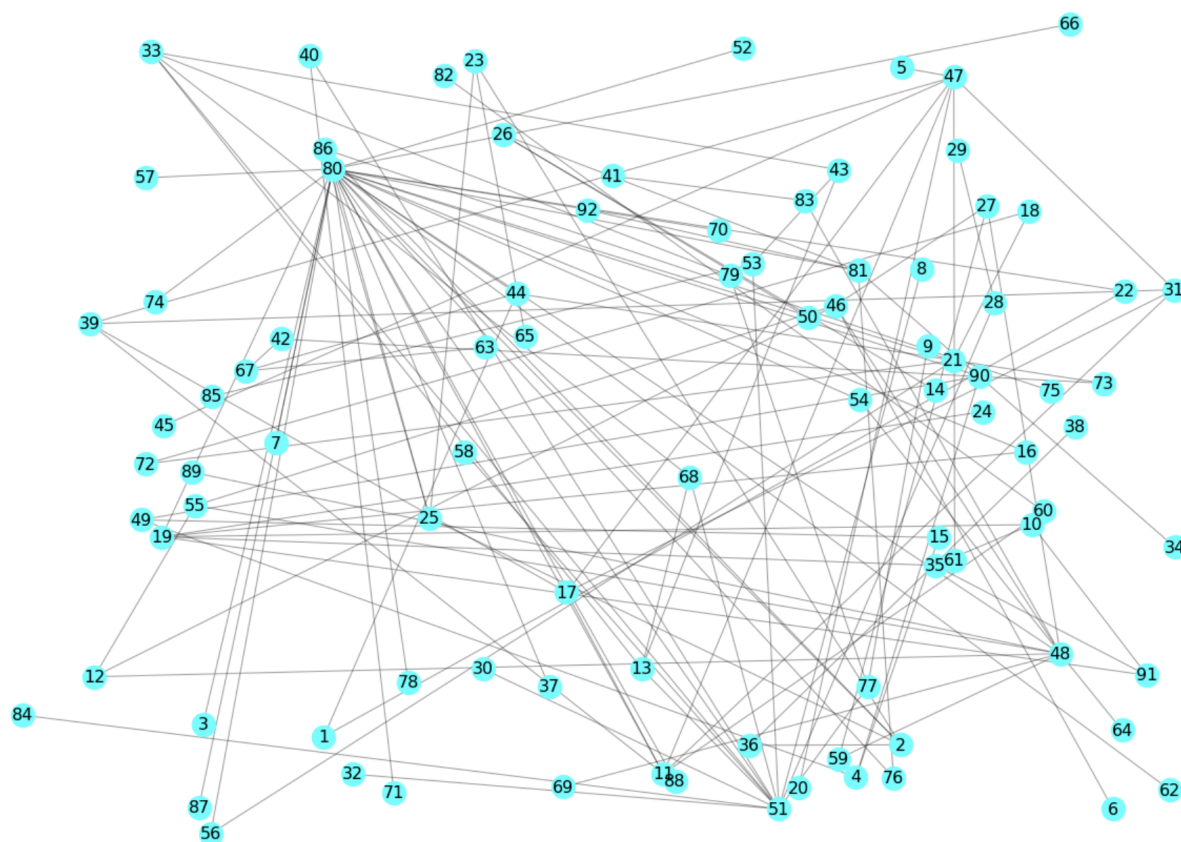


Figura 11 – Rede de Inteligência (RI).

A segunda rede de criminalidade deste estudo é a Rede de Autores (RA), vista na Figura 12. Esta rede tem 80 indivíduos e 102 ligações, sendo: 80 autores de infração; 74 indivíduos do sexo masculino e 6 indivíduos do sexo feminino; a idade média dos indivíduos desta rede é de 32 anos, sendo o mais novo com 22 anos e o mais velho com 55 anos; é uma rede com estrutura totalmente conectada.

Outra rede de criminalidade deste estudo é a Rede de Condenados (RC), vista na Figura 13. Esta rede tem 67 indivíduos e 78 ligações, sendo: 67 condenados por infrações; 61 indivíduos do sexo masculino e 6 indivíduos do sexo feminino; a idade média dos indivíduos desta rede é de 32 anos, sendo o mais novo com 24 anos e o mais velho com 55 anos; é uma rede com duas estruturas, uma principal com 63 indivíduos e 75 ligações, e outra com 4 indivíduos e 3 ligações.

A Rede de Gangue (RG) é a quarta rede de criminalidade deste estudo, vista na Figura 14. Esta rede tem 17 indivíduos e 24 ligações, sendo: 17 condenados; 16 indivíduos do sexo masculino e 1 indivíduo do sexo feminino; a idade média dos indivíduos desta rede é de 33 anos, sendo o mais novo com 24 anos e o mais velho com 44 anos; é uma rede com estrutura totalmente conectada.

Não há uma maneira definida de empreender uma análise de redes sociais, muito menos

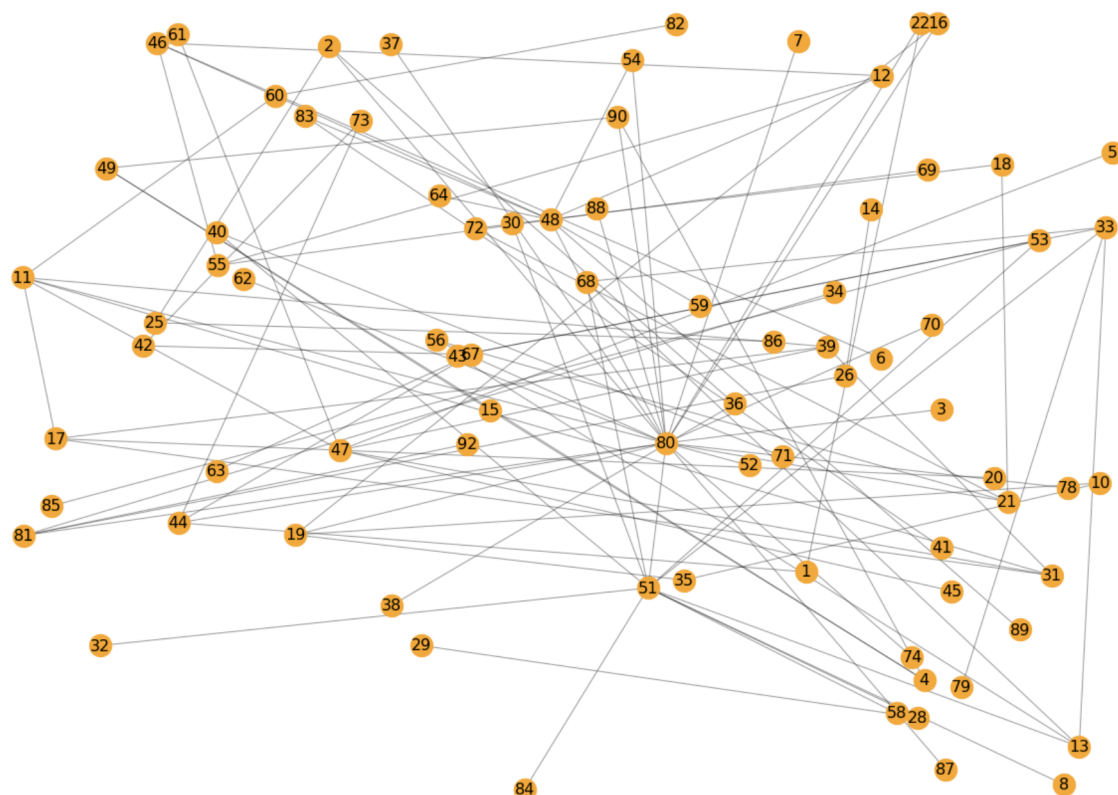


Figura 12 – Rede de Autores (RA).

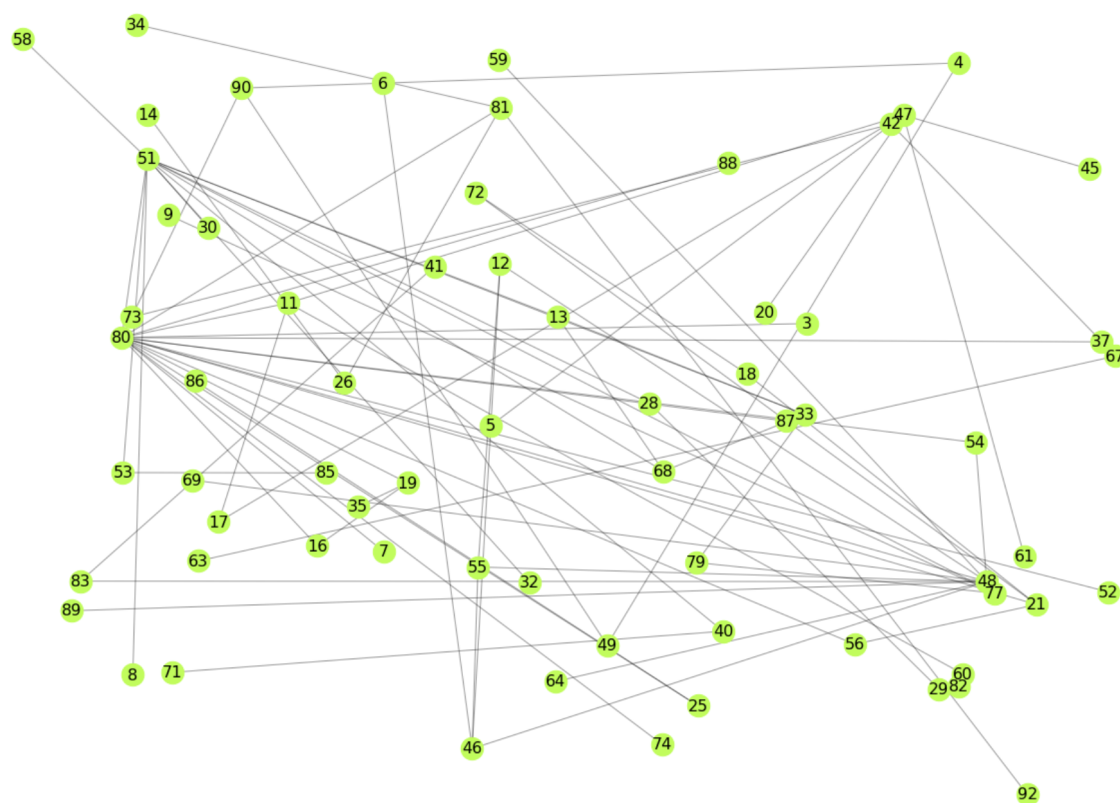


Figura 13 – Rede de Condenados (RC).

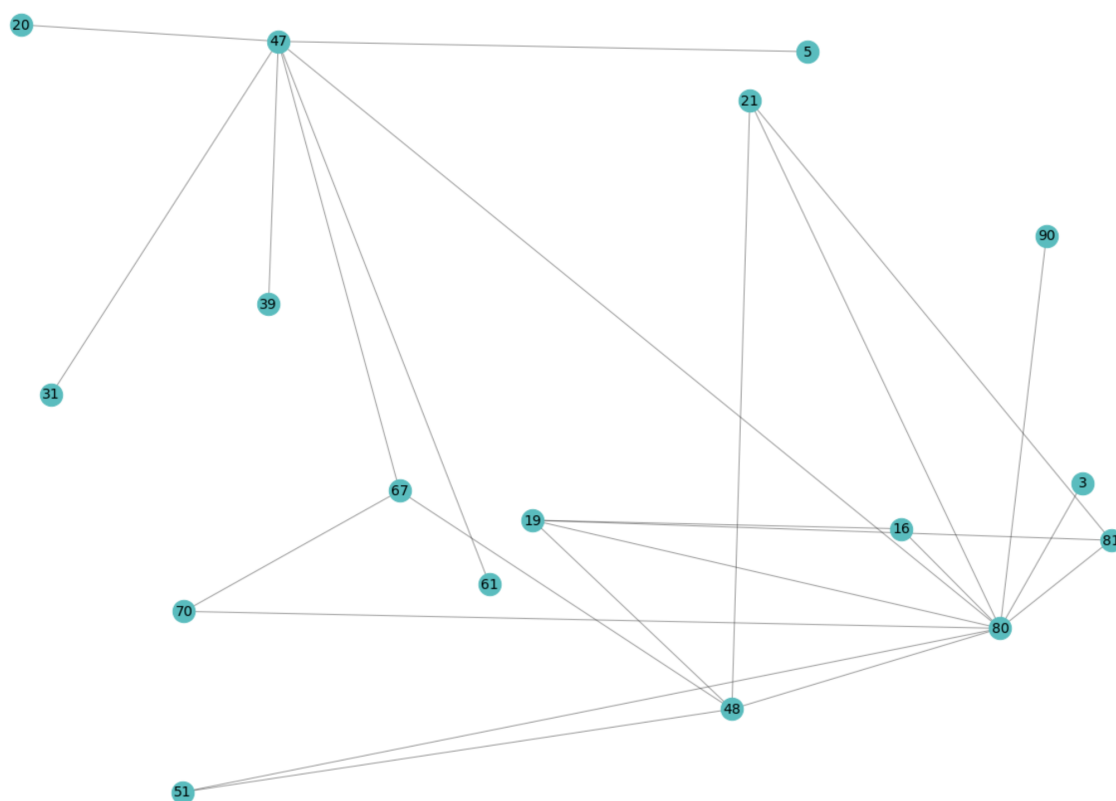


Figura 14 – Rede de Gangue (RG).

de redes de criminalidade, pois tudo depende das questões que estão sendo investigadas. A Tabela 1 fornece informações dos principais termos e estatísticas de SNA produzidos neste trabalho. Estatísticas chave são usadas para descrever e interpretar as redes de criminalidade aqui estudadas.

Tabela 1 – Principais Estatísticas das Redes.

Estatísticas	RI	RA	RC	RG
Tamanho				
Número de indivíduos	92	80	67	17
Número de ligações	123	102	78	24
Coesão				
Componentes	1	1	2	1
Dímetro	6	6	6	3
Densidade	0,029384	0,032278	0,035278	0,176471
Densidade do componente principal	-	-	0,038402	-
Assortatividade	-0,233052	-0,248581	-0,260614	-0,534114
Assortatividade do componente principal	-	-	-0,284559	-
Transitividade	0,151515	0,150000	0,120690	0,191489
Transitividade do componente principal	-	-	0,121387	-

Os dados de inteligência contêm informações explícitas sobre as duas redes de criminalidade, a Rede de Inteligência (RI) e a Rede de Gangue (RG), além das duas sub-redes da primeira, Rede de Autores(RA) e Rede de Condenados (RC). A maior rede é a RI, composta

por infratores e seus comparsas (associados, familiares, cônjuges *etc*), que totalizam 92 indivíduos e 123 ligações entre eles. Por ser uma sub-rede da RI, a RA é menor, com 80 indivíduos e 102 ligações entre eles, sendo este conjunto formado apenas por infratores, ou seja, indivíduos que foram presos pela prática de crimes. Já a RC é composta por 67 indivíduos e 78 ligações entre eles; estes indivíduos são aqueles que já foram condenados pela justiça pela prática de algum crime. A menor rede, a RG, contém 17 indivíduos e 24 ligações entre eles.

As ligações entre os indivíduos provêm de dois repositórios de dados de inteligência, um de vínculos e outro de gangues. O primeiro repositório forneceu informações para identificação das ligações entre os indivíduos da RI, RA e RC, outro para RG. Os indivíduos são os mesmos na RI e RG. Este tamanho diferente das redes demonstra a importância de ter diferentes ligações para compreender as redes de criminalidade, ou seja, a análise com diferentes fontes de dados pode gerar um resultado mais completo e melhor.

As ligações dos indivíduos da RI não são iguais da RG, demonstrando que as redes podem se conectar por laços diferentes. Já a RI, RA e RC tem os mesmos laços, porém em diferentes quantidade por causa do estreitamento do número de indivíduos nas sub-redes.

A densidade mostra o quão é conectada uma rede (SCOTT, 2017). Se estamos comparando populações e notamos que há muitos atores em uma que não estão na outra, podemos concluir que a 'vida social' é diferente nas duas populações. A densidade, segundo (SAYAMA, 2015), é dada pela Equação 1, onde G representa uma rede não direcionada, m o número de laços e n o número de nós.

$$\rho(G) = \frac{m}{\frac{n(n-1)}{2}} = \frac{2m}{n(n-1)} \quad (1)$$

Comparando a densidade das redes, vemos que a densidade da RG (0,176471) é maior que as outras (Tabela 1). Isto induz que os indivíduos são mais ativos na RG do que nas outras redes (suas ações são mais visíveis nos dados de inteligência).

A assortatividade é uma medida de correlação que mostra se nós com grau alto se conectam a nós de mesmo grau ou parecidos (assortativa) ou se nós de grau alto se conectam com nós de graus diferentes (disassortativo)(SCOTT, 2017). O coeficiente de assortatividade é a correlação entre graus de vértices adjacentes. A assortatividade, segundo (SAYAMA, 2015), é dada pela Equação 2:

$$r = \frac{\sum_{(i,j) \in E} (f(i) - \bar{f}_1)(f(j) - \bar{f}_2)}{\sqrt{\sum_{(i,j) \in E} (f(i) - \bar{f}_1)^2} \sqrt{\sum_{(i,j) \in E} (f(j) - \bar{f}_2)^2}} \quad (2)$$

onde E é o conjunto de arestas direcionadas, e $\bar{f}_1$ e $\bar{f}_2$ definidos por:

$$\bar{f}_1 = \frac{\sum_{(i,j) \in E} f(i)}{|E|}, \bar{f}_2 = \frac{\sum_{(i,j) \in E} f(j)}{|E|} \quad (3)$$

A tendência de os nós se conectarem a outros nós com propriedades diferentes em uma rede, disassortatividade, ou assortatividade negativa, é o que encontramos em todas as redes no trabalho (Tabela 1). A maior disassortatividade da RG sugere que indivíduos da gangue tendem a estabelecer ligações sem preocupar-se com uma hierarquia formal, o que confere uma característica das gangues.

Scott (2017) argumenta que muitas das questões mais interessantes e básicas da estrutura social surgem em relação a transitividade (triádes). Transitividade é uma medida da tendência das arestas em um grafo para formar triângulos, onde os nós em um grafo tendem a se agrupar. A transitividade, segundo (SAYAMA, 2015), é dada pela Equação 4, onde o denominador é o número de trincas de nós conectados (isto é, um nó, i e dois de seus vizinhos, j e k , enquanto o numerador é o número de trios em que j também está conectado a k .

$$C_T = \frac{|((i,j,k) \mid d(i,j) = d(i,k) = d(j,k) = 1)|}{|((i,j,k) \mid d(i,j) = d(i,k) = 1)|} \quad (4)$$

O fechamento triádico e sua influência é um bom guia para aplicações práticas como recomendação de indivíduos e convite a novos indivíduos. Os resultados desta medida (Tabela 1) sugerem que os indivíduos da RG são os que mais podem influenciar no crescimento das redes, trazendo novos indivíduos, sejam de qualquer natureza de relacionamento.

O maior número de componentes (Tabela 1) na RC destaca que grupos aparentemente distintos em SNA estão de fato conectados quando se considera diferentes tipos e origem de dados. Apesar dos indivíduos da RC não se apresentarem altamente conectados a outros indivíduos, se transpostos para RI fica evidente a alta relação com os demais indivíduos da rede, demonstrando a importância de considerar vários tipos de ligações para ajudar a entender um problema em específico, seja elas de qualquer natureza.

O diâmetro da RI, RA e RC são iguais, com tamanho 6. Já a RG tem um diâmetro de 3. Isto demonstra quantos saltos máximos são necessários para se alcançar qualquer indivíduo na mesma rede.

Observar as redes e explorar seu alcance ajuda a identificar indivíduos potencialmente associados as redes de criminalidade. Isto fornece uma indicação do 'estado' da rede do ponto de vista dos dados da Inteligência de Segurança Pública. Para isto, são necessárias medidas e identificações específicas utilizadas na SNA.

5.3 Análise de Redes de Criminalidade

Os dados deste estudo foram extraídos do CVO, cuja responsabilidade é da Inteligência da PMMG. Cada região do Estado de Minas Gerais tem sua Unidade de Inteligência, que tem a tarefa de coletar informações dos policiais, unidades e outras fontes de inteligência, relevantes para identificar a associação e informações de infratores, comparsas e condenados. Todas as informações coletadas devem ser confirmadas por diferentes fontes, tais como informantes, policiais disfarçados, equipes de vigilância, interceptações telefônicas, fontes abertas e outras fontes técnicas, ou testemunho de policiais onde eles observaram os indivíduos em atividades infracionais.

Os dados da rede de criminosos em geral têm limitações e tendências. Uma limitação geral é que o acesso a esses dados é restrito devido à sensibilidade da informação, tanto no que diz respeito a coletar dados de populações de difícil acesso, quanto obter acesso a dados de organizações de segurança pública. Outra limitação geral que os conjuntos de dados da rede de criminalidade têm em comum é que a interação entre a Polícia e a população observada afeta a estrutura e dinâmica da rede.

Uma outra limitação é que os dados da rede de criminalidade sofrem de vários filtros de seleção, como a dependência em dados de comparsas, que muitas vezes são incompletos. Isso significa que muitos crimes que nunca foram descobertos ou relatados não são cobertos pelos dados. Outro problema com os comparsas é o fator de inocência, o que significa que uma pessoa suspeita ou acusada pode, de fato, ser inocente e ter sido registrado de forma incorreta.

Uma limitação final, e muito importante, é a interpretação subjetiva de quem coleta a informação, que pode ser tendenciosa a diminuir ou aumentar o potencial do crime praticado.

Segundo Lazega e Higgins (2014):

Ajudar a reconhecer as propriedades estruturais dos conjuntos sociais é uma das contribuições da sociologia. Para tanto, o método dito “estrutural” parte da observação das interdependências e da ausência das mesmas entre membros de um ator coletivo ou de um meio social organizado. Os indicadores das interdependências sociais utilizados pelo método estrutural são as relações sociais. Uma relação social será entendida aqui, ao mesmo tempo como um canal para transferência ou troca de recursos, bem como um engajamento intencional em relação a um ou vários parceiros de troca; engajamento inseparável do sentido da relação para os parceiros. [...] este método estrutural o faz de modo sistemático, formalizando suas análises através de modelos matemáticos ou estatísticos.

Assim, nossa análise, partirá de dados extraídos do conjunto de dados do CVO, com análise quantitativa e qualitativa, buscando modelar os dados para gerar conhecimento de inteligência, para atuação policial preventiva e repressiva (Figura 15).

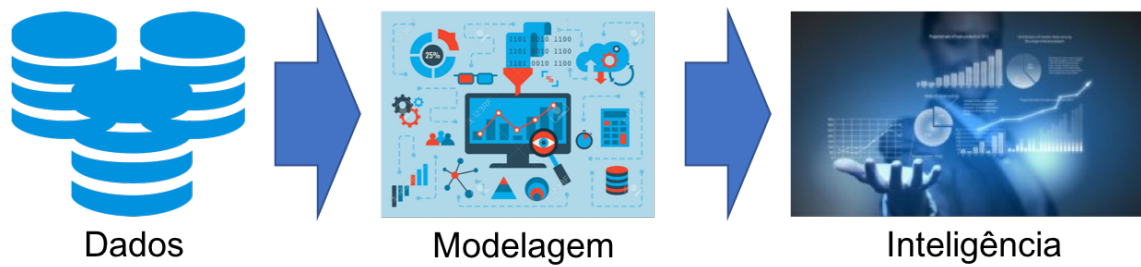


Figura 15 – Ilustração da conversão de dados em inteligência, onde os dados de redes de criminalidade são modelados em conhecimento para Inteligência de Segurança Pública

Através da mineração de dados, foram identificados 4 líderes da rede de criminalidade em estudo. Estas identificações iniciais aconteceram através da observação de agentes de inteligência, que as inseriram no banco de dados do CVO. Estes líderes são os elementos 47, 48, 51 e 80. Partindo desta análise qualitativa, passamos a uma análise quantitativa.

A caracterização de uma rede social, em particular uma rede de criminalidade, depende de uma série de fatores, tais como dados dinâmicos ou estáticos. O foco aqui é estudar o fenômeno das redes de criminalidade em suas diferentes representações, mantendo uma possibilidade de comparação simples e objetiva. Foram calculadas as medidas de centralidade (Apêndice A) da RI: na classificação de *Degree centrality* e *PageRank* os líderes aparecem nas quatro primeiras posições, na classificação de *Betweenness centrality*, os líderes aparecem nas sete primeiras posições. Já na classificação de *Eigenvector centrality* e *Closeness centrality* os líderes aparecem, respectivamente, na trigésima e quadragésima primeiras posições.

Assim, foram escolhidas três medidas de centralidade não direcionadas e estáticas, que melhor podem identificar os líderes da rede de criminalidade: *Degree centrality*, *Betweenness centrality* e *PageRank*.

Degree centrality nos diz que a centralidade de um indivíduo é o número de contatos diretos que ele possui (SCOTT, 2017). Um indivíduo que se encontra numa posição que permite o contato direto com muitos outros é visto pelos demais como um canal maior de informação, razão pela qual se diz ser mais central. A *Degree centrality*, segundo Sayama (2015), é dada pela Equação 5, onde o grau normalizado é o grau real dividido pelo grau máximo possível ($n - 1$), cujos resultados estão no Apêndice B.

$$C_D(i) = \frac{deg(i)}{n - 1} \quad (5)$$

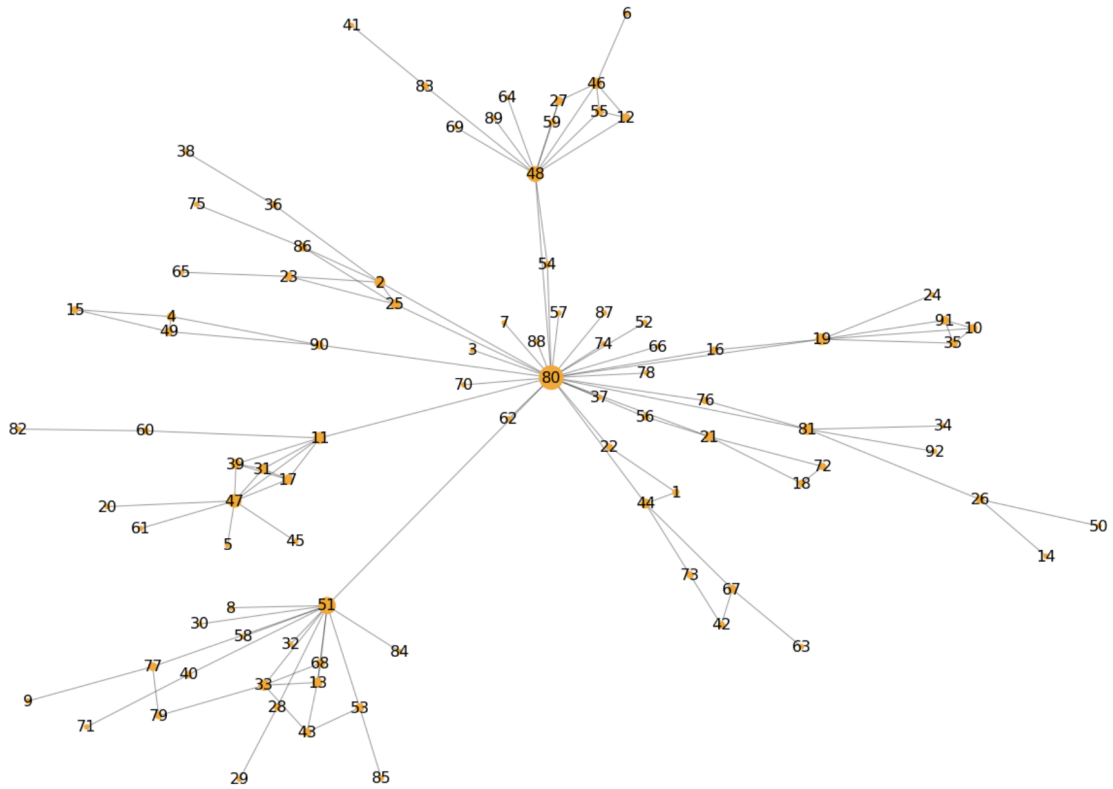


Figura 16 – *Degree centrality* da Rede de Inteligência, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos de maior grau na rede.

Assim, *Degree centrality* nada mais é que a contagem do número de adjacências de um indivíduo, normalizada (Figura 16). Quanto maior o número de indivíduos vizinhos interligados, maior será esta medida.

Betweenness centrality quantifica o número de vezes que um indivíduo aparece como ponte ao longo do caminho mais curto entre dois outros indivíduos, o que possibilita medir a capacidade que um elemento tem de poder influenciar os seus pares em uma rede (SCOTT, 2017). A *Betweenness centrality*, segundo Sayama (2015), é dada pela Equação 6, onde o numerador é o número de caminhos mais curtos do nó j ao nó k , e o denominador é o número dos caminhos mais curtos do nó j ao nó k que passam pelo nó i , cujos resultados estão no Apêndice B.

$$C_B(i) = \frac{1}{(n-1)(n-2)} \sum_{j \neq i, k \neq i, j \neq k} \frac{N_{sp}(j \xrightarrow{i} k)}{N_{sp}(j \rightarrow k)} \quad (6)$$

O conceito desta medida pode ser compreendido com a seguinte analogia: uma rede de criminalidade integrada por vários caminhos entre seus indivíduos terá uma grande vantagem estratégica, o que nos remete a ideia que um indivíduo importante faz parte de muitos caminhos (Figura 17).

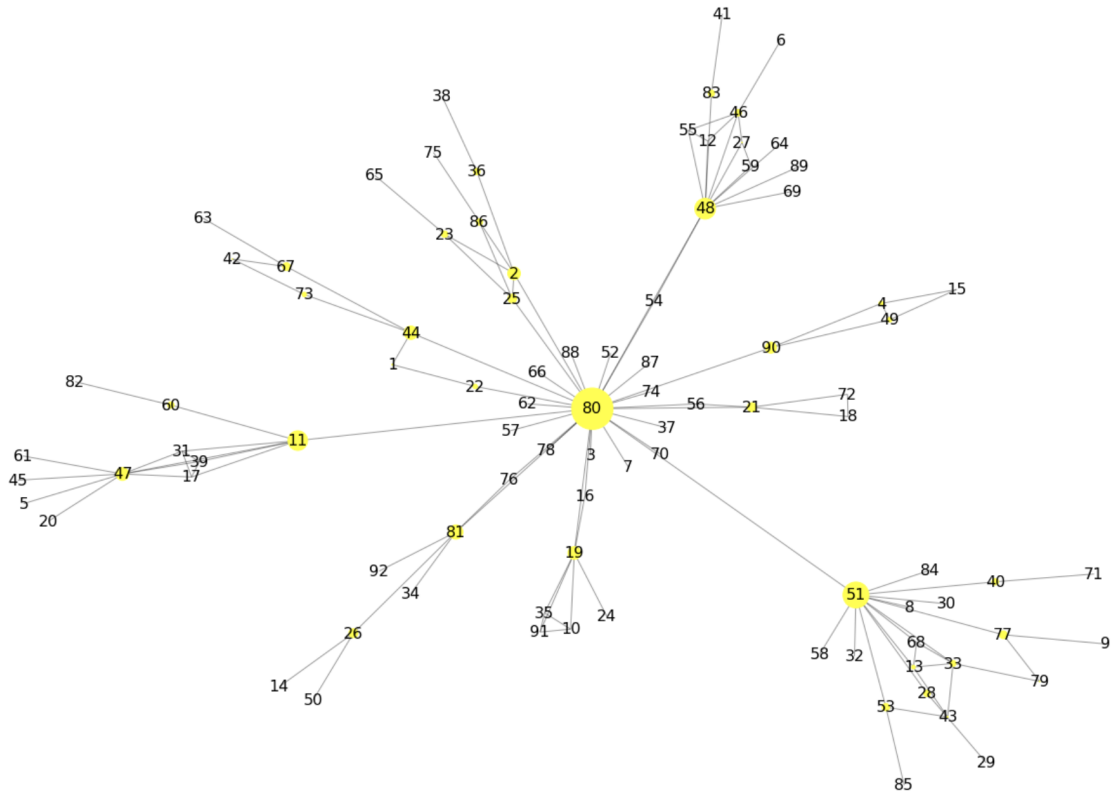


Figura 17 – *Betweenness centrality* da Rede de Inteligência, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos de maior intermediação da rede.

PageRank é uma variação de *Eigenvector centrality*, que foi originalmente desenvolvida por Larry Page e Sergey Brin, os fundadores do Google®, para classificar páginas da web (SAYAMA, 2015). O *PageRank*, segundo Sayama (2015), é dado pela Equação 7, onde A é a matriz de adjacência da rede, D é uma matriz diagonal onde o i -ésimo componente diagonal é $1/\deg(i)$, J é uma matriz $n \times n$, e α é o parâmetro de amortecimento, cujos resultados estão no Apêndice B.

$$T = \alpha AD^{-1} + (1 - \alpha) \frac{J}{n} \quad (7)$$

PageRank é uma maneira eficaz para catalogar a relevância de um indivíduo dentro de uma rede (SCOTT, 2017) (Figura 18). Avalia o conceito que um indivíduo tem em sua rede de atuação, através dos indivíduos concorrentes. O sistema utiliza uma forma de 'eleição', onde cada indivíduo recebe um voto de acordo com a segmentação.

Como as medidas de *Degree centrality*, *Betweenness centrality* e *PageRank* foram calculadas já normalizadas, sua classificação (Apêndice B) de média nos permite identificar os indivíduos centrais da RI (Figura 19), onde os dez primeiros são os indivíduos: 80, 51, 48, 11, 47, 81, 19, 2, 44 e 90.

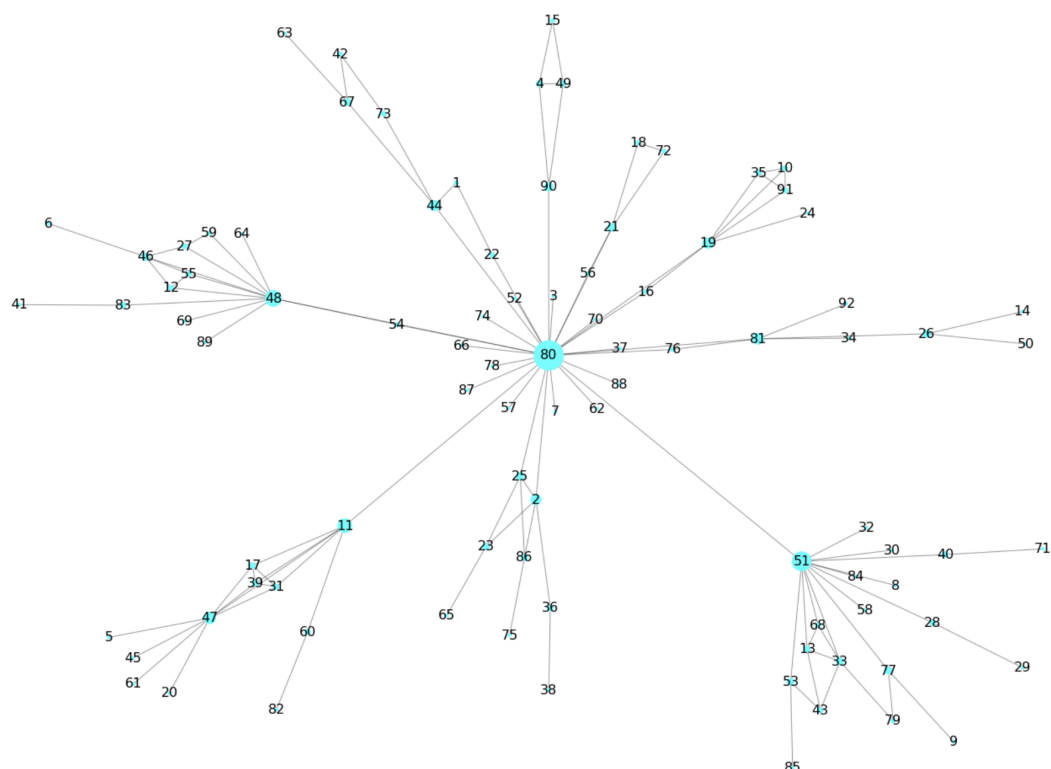


Figura 19 – *Média Degree centrality + Betweenness centrality + PageRank* da Rede de Inteligência, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos mais centrais da rede

11, 47, 81, 21, 90, 46, 77. Conforme já debatido, a forma de identificação dos dados pode afetar diretamente a SNA. Se tivéssemos nos detido ao conjunto de indivíduos condenados, que é uma coleção de dados bem significativa, tenderíamos a desprezar o componente secundário por ser pouco representativo, o que ocasionaria em uma análise distorcida da rede criminosa como um todo. Isto reflete a importância de dados de Inteligência de Segurança Pública, mais abrangentes e significativos para SNA, que os dados do sistema de justiça.

A RG provem de fonte de dados diferente da RI, RA e RC, onde, apesar de seus indivíduos estarem presentes nas outras redes, as ligações ocorrem de forma diversa, representando a ligação destes indivíduos em duas gangues e com as características estatísticas salientadas na Tabela 1. Estas medidas estatísticas (Apêndice E) mostram o quão importante é a Rede de Gangues para SNA neste estudo. Os indivíduos desta rede são aqueles que de alguma forma criaram uma segunda camada de ligações, e que atuam na RI. A Figura 22 identifica os indivíduos de maior atuação da RG quanto a *Degree centrality*, *Betweenness centrality* e *PageRank*, e a média destes, onde o tamanho dos nós é proporcional ao resultado obtido. Os dados de inteligência, aqui tratados, identificam uma gangue atuante, cujos membros conhecidos 80, 47, 19, 48, 81, 51 e 90, representam parte do núcleo da comunidade como um todo, sendo fortemente envolvidos nas partes

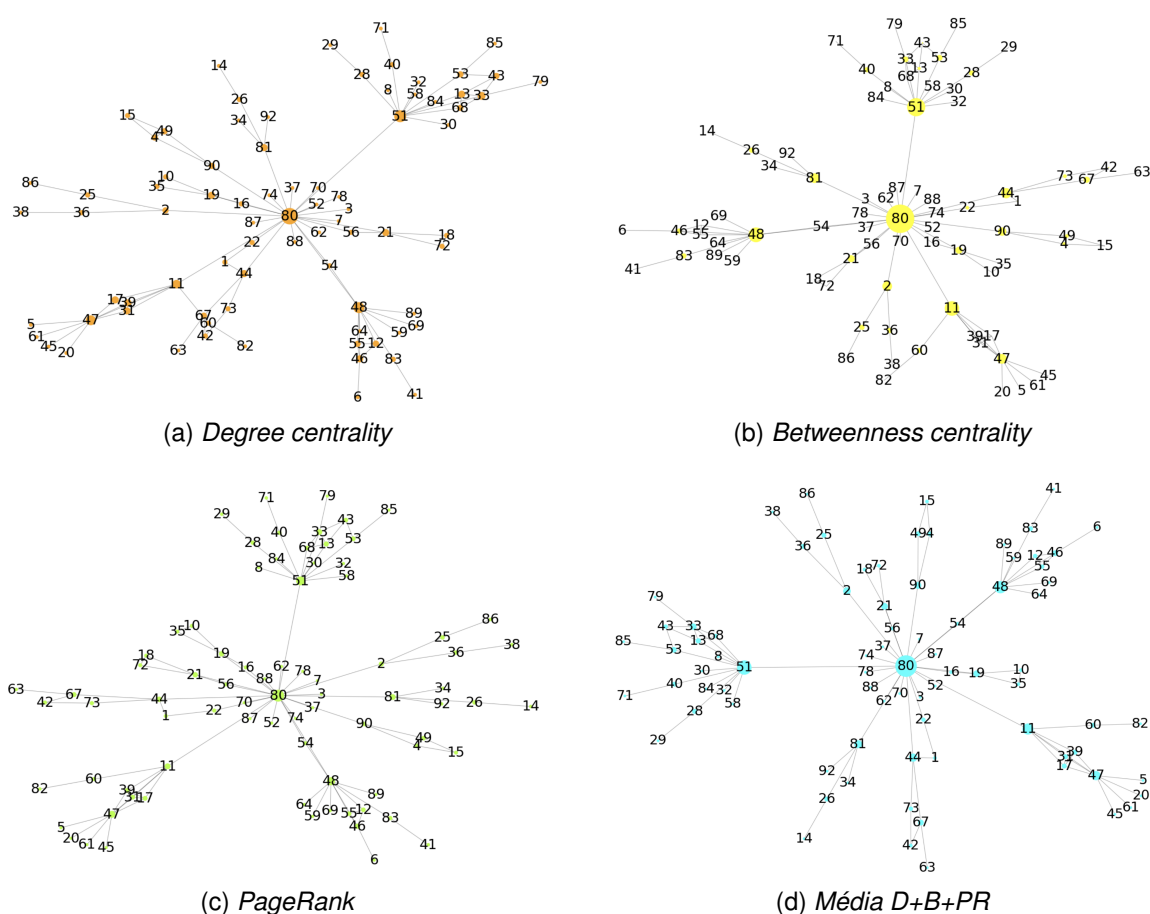


Figura 20 – Medidas de Centralidade da sub-Rede de Autores, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos de maior relevância da rede.

estratégias de todo o conjunto.

Muitos sistemas de interesse científico são representados como redes, onde exemplos incluem a Internet, redes de alimentos, redes de comunicação e redes sociais (CLAUSET; NEWMAN; MOORE, 2004). Dentre os estudos de redes, uma questão tem recebido considerável atenção, a detecção e caracterização da estrutura da comunidade em redes. Segundo Clauset, Newman e Moore (2004), a comunidade em redes significa *"a identificação de grupos de vértices densamente conectados, com conexões apenas esparsas entre os grupos"*. A capacidade de detectar esses grupos tem importância prática dentro da SNA, pois podem corresponder a unidades sociais, comunidades, ou mesmo quadrilhas criminosas.

Trabalhos para descobrir métodos que decompõem uma rede em grupos dividem-se em duas linhas principais: particionamento de grafos, usado na ciência da computação e áreas afins, como computação paralela e design de circuitos integrados; e detecção de estrutura de comunidade, buscada por sociólogos, físicos, biólogos e matemáticos, com aplicações especialmente voltadas para redes sociais. (CLAUSET; NEWMAN; MOORE, 2004)

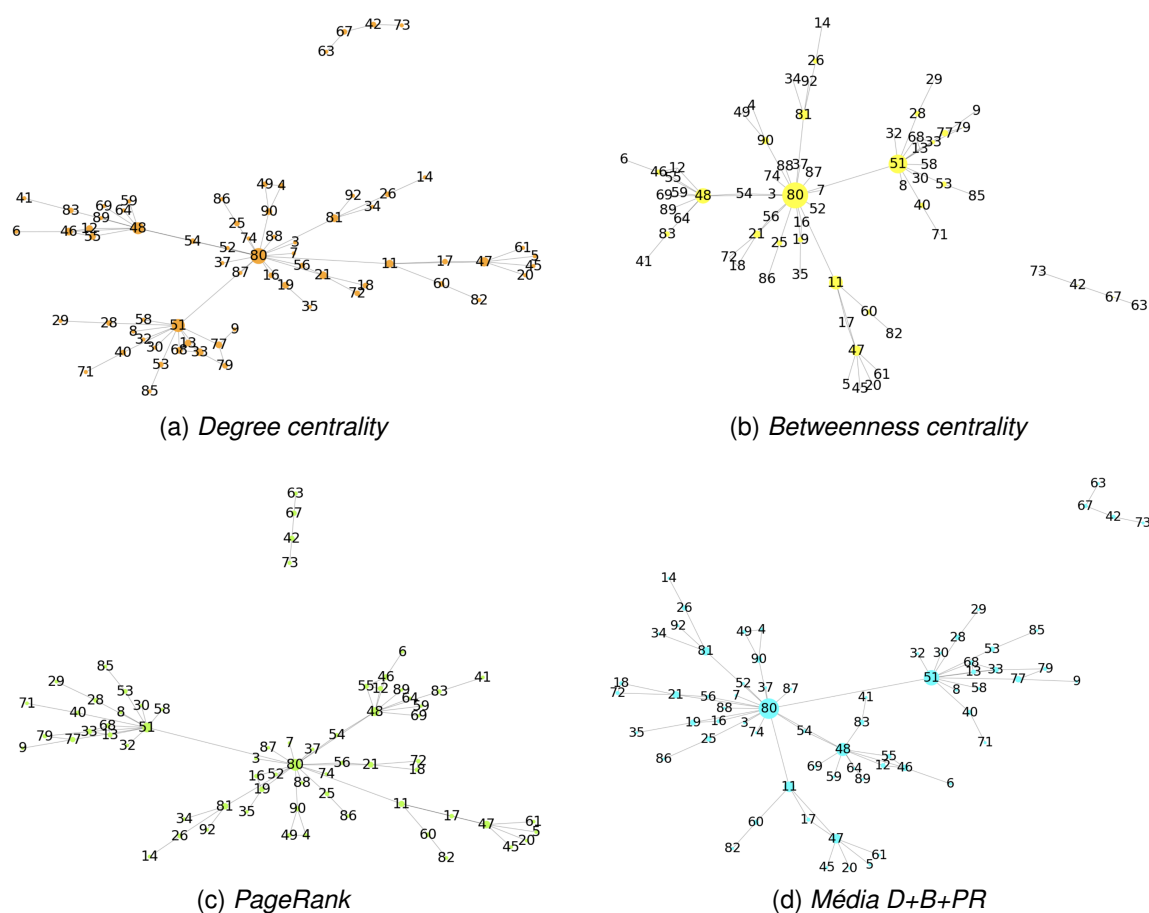


Figura 21 – Medidas de Centralidade da sub-Rede de Condenados, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos de maior relevância da rede.

A detecção da estrutura de comunidade é uma técnica de análise de dados usada para esclarecer a estrutura de conjuntos de dados de rede em grande escala, como redes sociais, dados de Internet e da Web, ou redes bioquímicas. Os métodos de estrutura de comunidade normalmente pressupõem que a rede de interesse se divide naturalmente em subgrupos e que o trabalho do experimentador é encontrar esses grupos. O número e o tamanho dos grupos são assim determinados pela própria rede e não pelo experimentador. Detectar a estrutura da comunidade em redes é enquadrado como uma tarefa de otimização na qual se pesquisa o valor máximo da quantidade conhecida como modularidade sobre possíveis divisões de uma rede. (CLAUSET; NEWMAN; MOORE, 2004) [Tradução do autor]

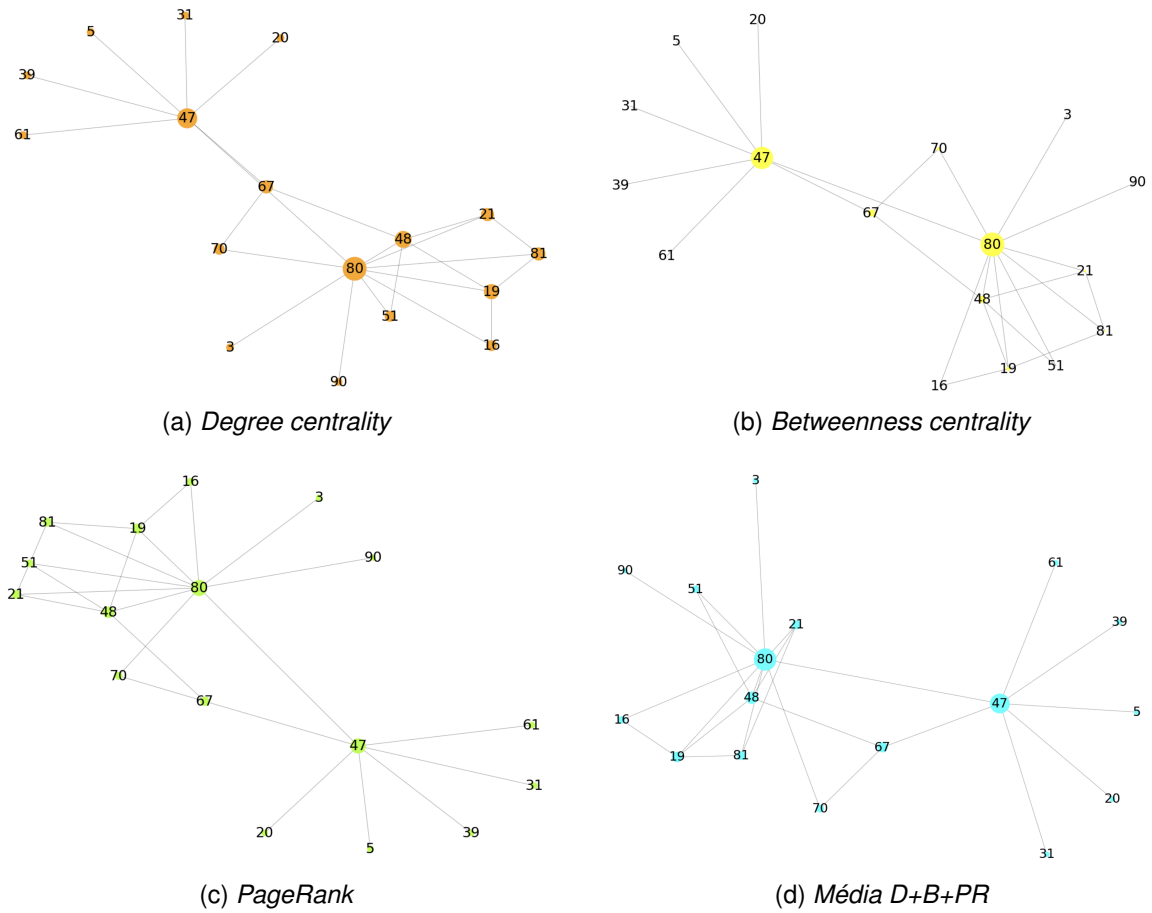


Figura 22 – Medidas de Centralidade da Rede de Gangue, onde o tamanho dos nós é proporcional ao resultado obtido, identificando os indivíduos de maior relevância da rede.

Algoritmos foram propostos para encontrar partições razoavelmente boas e rápidas. Segundo Sayama (2015), o método Louvain, proposto por Blondel et al. (2008) é um algoritmo rápido e eficiente. A Equação 8 define a modularidade de um determinado conjunto de comunidades em uma rede (SAYAMA, 2015), usado no método *Louvain*, onde, $|E|$ é o número de arestas, $|E_{in}|$ é o número de arestas dentro da comunidade (ou seja, aquelas que não ultrapassam limites entre comunidades), e $\langle |E_{in}| \rangle$ é o número esperado de arestas dentro da comunidade se a topologia for puramente aleatória.

$$Q = \frac{|E_{in}| - \langle |E_{in}| \rangle}{|E|} \quad (8)$$

Blondel et al. (2008) definem o método como a decomposição das redes em subunidades ou comunidades, que são conjuntos de nós altamente conectados.

A identificação dessa comunidades é de importância crucial, pois elas podem ajudar a descobrir módulos funcionais a priori desconhecidos, como tópicos em redes de informação ou comunidades virtuais em redes sociais. Além disso, a meta-rede resultante, cujos nós são as comunidades, pode

então ser usada para visualizar a estrutura de rede original.(BLONDEL et al., 2008) [Tradução do autor]

O algoritmo Louvain encontra partições de alta modularidade de grandes redes em um curto espaço de tempo e desdobra uma estrutura de comunidade hierárquica completa para a rede, dando acesso a diferentes resoluções de detecção de comunidade. (BLONDEL et al., 2008)

Na literatura de SNA (BLONDEL et al., 2008; BARRAT; BARTHELEMY; VESPIGNANI, 2008; NEWMAN, 2010), uma das áreas de investigação mais desafiadoras nos últimos tempos é a análise da comunidade, cujo objetivo é revelar possíveis sub-redes (grupos de indivíduos chamados de comunidades ou módulos), caracterizados por ter, comparativamente, grande conectividade interna, ou seja, os indivíduos tendem a se conectar muito mais com outros indivíduos do grupo do que com o resto da rede.

Mais notadamente, a análise da comunidade revela ser uma ferramenta poderosa para entender profundamente as propriedades de vários sistemas complexos do mundo real em praticamente qualquer campo da ciência, como biologia (JONSSON et al., 2006), ecologia (KRAUSE et al., 2003), economia (PICCARDI; CALATRONI; BERTONI, 2010), informação (FLAKE et al., 2002; FORTUNA; BONACHELA; LEVIN, 2011) e ciências sociais (GIRVAN; NEWMAN, 2002; ARENAS et al., 2004).

As redes de criminalidade tendem a se agrupar para reduzir os riscos de detecção e vazamento de informações. No entanto a literatura que explora a relevância dos subgrupos para sua estrutura interna é, até agora, muito limitada.

Acadêmicos e agências de segurança pública estão aplicando cada vez mais SNA em redes de criminalidade. Enquanto as aplicações atuais enfocam principalmente a identificação dos criminosos-chave através de medidas de centralidade (VARESE, 2006; MORSELLI, 2009; MASYS, 2014) e outros atributos individuais (CARLEY; LEE; KRACKHARDT, 2002; MORSELLI; ROY, 2008; MALM; BICHLER, 2011; BRIGHT et al., 2015; AGRESTE et al., 2016), a análise dos subgrupos e sua influência nas atividades criminosas receberam atenção muito limitada até o momento.

Subgrupos são uma ocorrência natural em redes de criminalidade, que podem ser agrupadas em unidades hierárquicas, conforme apresentado no Apêndice F. Como resultado deste trabalho, é possível ver na Figura 23 que a RI está agrupada e que subgrupos estão associados, de uma maneira não trivial a organização interna da RI. Os subgrupos criam uma limitação ao compartilhamento de informações para evitar vazamentos e detecção, uma vez que os subgrupos criminosos enfrentam uma relação específica entre eficiência versus segurança (MORSELLI; GIGUÈRE; PETIT, 2007). Além disso, quanto maior a rede de criminalidade, mais provável e relevante é a presença de subgrupos. Essas considerações sugerem que a análise de subgrupos em redes de criminalidade podem fornecer uma visão

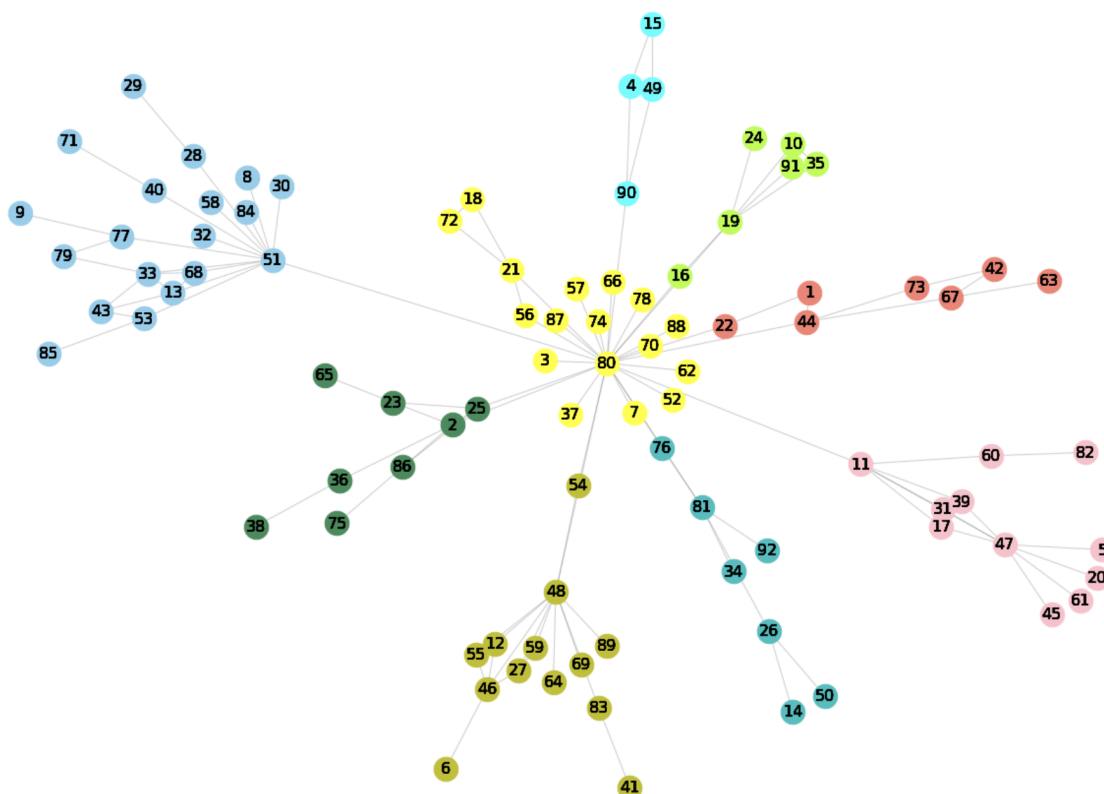


Figura 23 – Subgrupos da Rede de Inteligência, onde os indivíduos são agrupados hierarquicamente em comunidades de rede.

tanto da estrutura interna quanto das melhores estratégias preventivas e repressivas contra eles.

Os resultados da análise de comunidade evidenciam que a RI está significativamente agrupada em 9 subgrupos, sugerindo que estes subgrupos desempenham um papel importante em sua organização interna. Se combinarmos os dez líderes-chave obtidos na análise de centralidade (Apêndice B) com a análise de comunidade, teremos a composição mostrada na Figura 24. Os líderes, já identificados na análise de centralidade, estão presentes nos 9 subgrupos, o que nos induz a certeza que são indivíduos estratégicos para rede.

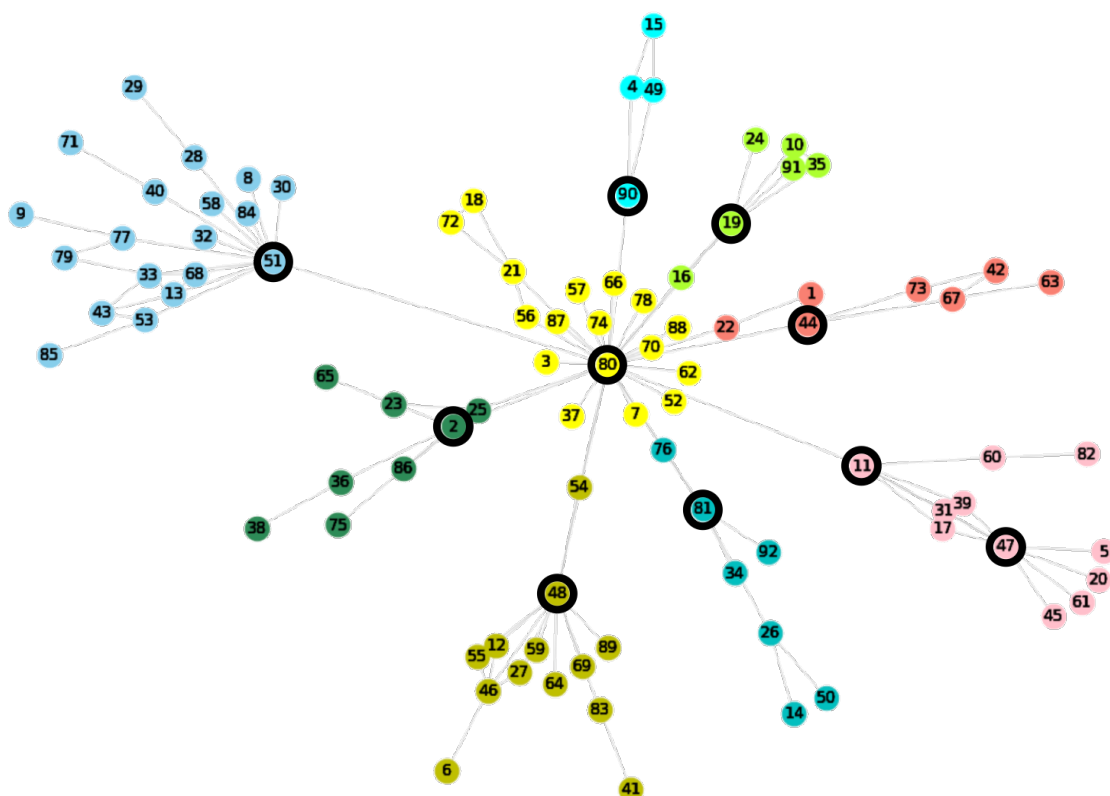


Figura 24 – Subgrupos da Rede de Inteligência, onde são evidenciando os líderes identificados através das medidas de centralidade.

Já a análise de comunidade da RG mostra 3 subgrupos, tendo como líderes os elementos 80 e 47 (Figura 25). Estes dois elementos são líderes-chave tanto na RI quanto na RG, o que evidencia que são bem posicionados na hierarquia das redes, com elevada interconexão, tendo papéis estratégicos na tomada de decisões. A terceira comunidade é composta pelos elementos 67 e 70, que não se apresentam como líderes, mas são importantes no papel de ligação, principalmente no crime de Tráfico de Arma, que será objeto de estudo na seção Multiplexidade de Redes de Criminalidade.

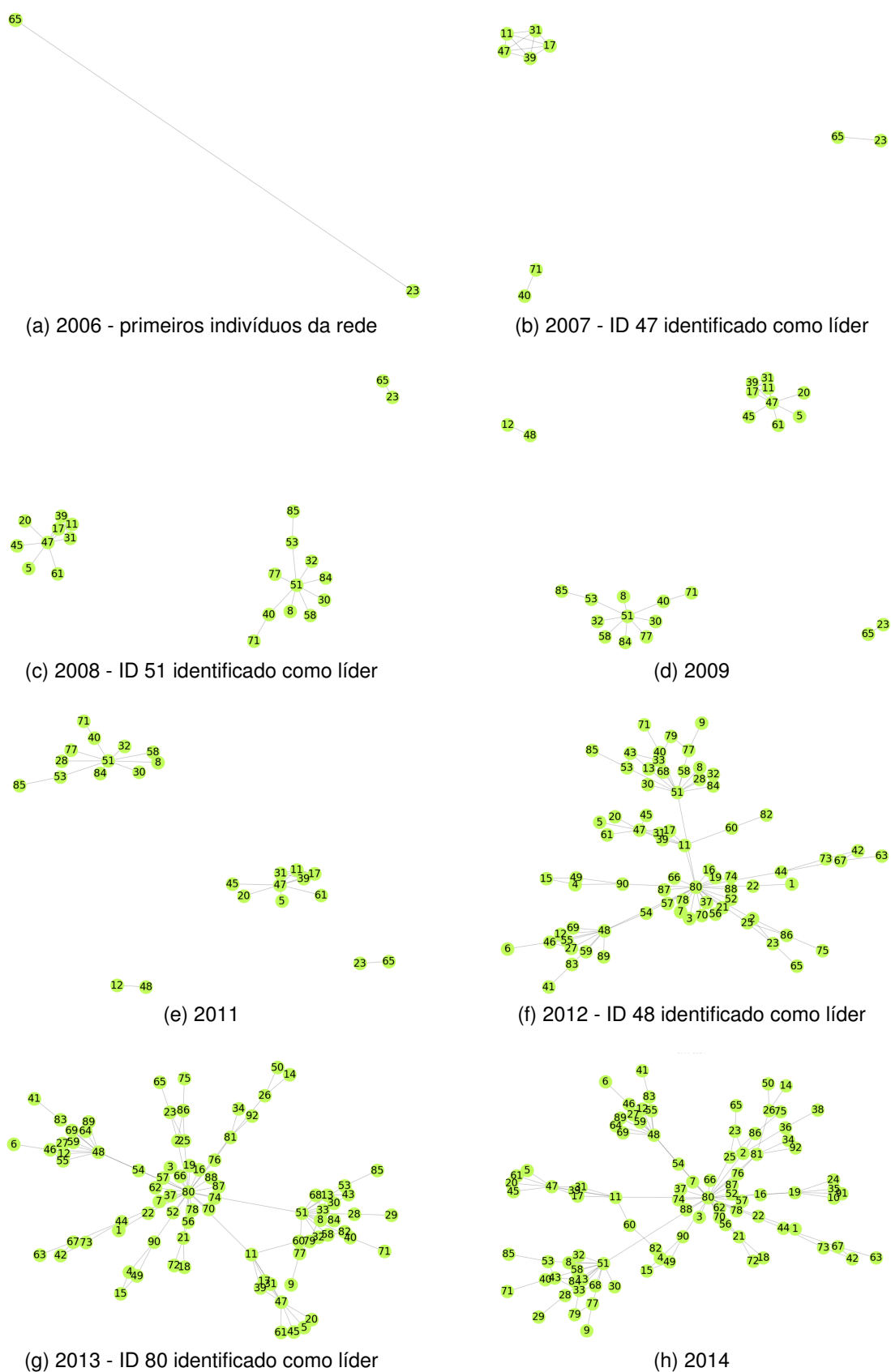


Figura 26 – Evolução temporal da Rede de Inteligência - 2006 a 2014 - com a identificação de líderes pelo serviço de Inteligência.

5.4 Simulação de Ruptura e Resiliência de Rede de Criminalidade

É notório que agências de segurança de todo mundo buscam maneiras de romper as organizações criminosas de forma eficaz, preferencialmente nas fases iniciais de organização da rede de criminalidade.

Os estudos porém se concentram na identificação do líder (*hub*) da rede, que se encontra no topo da pirâmide organizacional do crime, na perspectiva que removendo-o, a rede de criminalidade será interrompida. Porém a fluidez e flexibilidade das redes de criminalidade as tornam muito resilientes contra este tipo de estratégia tradicional (DUIJN; KASHIRIN; SLOOT, 2014).

O que se percebe é que as redes de criminalidade são afetadas diretamente pelo equilíbrio entre eficiência e segurança interna, buscando esconder suas atividades ilegais aos olhos das agências Policiais.

As redes de criminalidade são flexíveis e difíceis de serem interrompidas, principalmente por não serem estáticas, mas dinâmicas. Estas mudanças podem ocorrer por várias razões, como resultado de negócios, competição, estagnação ou adaptação da rede. Os efeitos da ruptura de uma rede podem ser então compreendidos dentro de sua dinâmica, adaptativa e complexa.

Compreender os conceitos e como uma rede de criminalidade se adapta a sua ruptura pode levar a um melhor entendimento da eficácia de estratégias de ruptura e resiliência de rede.

Segundo Duijn, Kashirin e Slood (2014), a ruptura de rede de criminalidade indica sua desestabilização por três caminhos: redução da taxa de fluxo de informações na rede; redução na capacidade de conduzir suas tarefas; uma falha no processo de tomada de decisão. *"A ruptura de rede pode ser definida em geral como o estado de uma rede que não pode difundir com eficiência informações, bens e conhecimento"*.

Duas são as estratégias principais para ruptura de redes de criminalidade: a abordagem do capital social e a abordagem do capital humano.

A abordagem do capital social busca identificar as posições estratégicas que os indivíduos ocupam na rede, através de seus contatos sociais, sendo, portando, muito utilizada com base na SNA, buscando identificar os atores centrais, suas influências e pesos na rede (DUIJN; KASHIRIN; SLOOT, 2014). As medidas de centralidade são estratégias eficazes e comuns de identificar o capital social.

A abordagem do capital humano é definida como *"um estoque de competências, conhecimento, atributos sociais e de personalidade, incluindo a criatividade, incorporados na*

capacidade de executar o trabalho de modo a produzir valor econômico" (DUIJN; KASHIRIN; SLOOT, 2014). Ainda segundo Duijn, Kashirin e Slood (2014), como nos negócios legais, o mercado criminal é um processo que envolve diferentes etapas de produção ou atividades.

Diferentes informações, bens e capital humano são trocados e adicionados seguindo uma estrutura em forma de cadeia, definido como uma cadeia de valor.

Segundo Duijn, Kashirin e Slood (2014), como resultado de serem interrompidas, as redes de criminalidade absorvem a capacidade de suportar interrupções, adaptando-se quando necessário a esta mudança, o que é conceituado como resiliência da rede. A resiliência consiste em dois aspectos: primeiro, a capacidade de absorver e, assim, resistir à ruptura e, em segundo lugar, a capacidade de se adaptar, quando necessário, às mudanças decorrentes dessa ruptura.

O primeiro aspecto do conceito de resiliência depende do nível de redundância que é habitado em sua estrutura de rede criminosa. Quanto mais sua estrutura de rede é caracterizada por altos níveis de redundância no sentido de diversidade de relações entre os atores, mais opções existem para compensar as perdas em "capital humano" ou encontrar novos métodos para continuar a cadeia de valor. A redundância permite que os membros da rede assumam tarefas de atores que são alvo de operações bem-sucedidas de aplicação da lei. Mesmo que algumas conexões sejam quebradas, a diversidade de diferentes laços entre os atores permite que a rede funcione. A redundância na rede está associada a fortes laços entre os membros da rede. Laços criminosos fortes oferecem confiança recíproca, o que é essencial dentro do ambiente criminal incerto e hostil. Substituições com uma reputação confiável são, portanto, encontradas com frequência nas conexões sociais que envolvem diretamente os atores envolvidos no processo comercial criminoso. Esses coletivos criminosos coesos geralmente iniciam a partir de redes sociais já estabelecidas, por exemplo, parentesco, amizade ou laços afetivos. Isso significa que as substituições são frequentemente encontradas em curtas distâncias sociais, a partir desse núcleo coeso. (DUIJN; KASHIRIN; SLOOT, 2014) [Tradução do autor]

Ao se adaptar as configurações de segurança alteradas, controlar o fluxo de informações torna-se a prioridade número um dentro de redes ilegais. Com base em estudos anteriores, isso é geralmente obtido por meio de "compartimentalização", o que significa que informações importantes são isoladas dentro de diferentes compartimentos ou "células organizacionais". Essa estratégia evita que toda a rede fique exposta, se um compartimento for detectado e interrompido. Como descrito acima, essa compartimentalização é frequentemente encontrada em redes terroristas com mais tempo para executar as tarefas. Além disso, Baker e Faulkner também encontraram um nível de compartimentalização entre o núcleo e a periferia dentro de redes ilegais de fixação de preços, como resultado da ruptura. Ao separar deliberadamente o fluxo de informações entre os membros dentro da periferia e o núcleo "visível", a rede de fixação de preços diminuiu a chance de os 'líderes' ficarem expostos após uma única prisão. Esses estudos mostram que, para se adaptar às mudanças nas circunstâncias após a ruptura, as redes criminosas tendem a organizar uma forma de não redundância dentro de seu fluxo interno de informações, a fim de proteger seus membros importantes de serem descobertos. (DUIJN; KASHIRIN; SLOOT, 2014) [Tradução do autor]

Passamos agora a desvendar a dinâmica de resiliência dentro da rede de criminalidade, como consequência da ruptura da rede. Isto foi feito simulando e observando os mecanismos de ruptura e resiliência da Rede de Inteligência. São apresentadas quatro estratégias para ruptura da rede, baseadas nas abordagens do capital social e humano. Com base na simulações destas estratégias, é apresentado o melhor modelo para recuperação e ruptura da rede de criminalidade, de acordo com os princípios de resiliência e ruptura.

O efeito de diferentes estratégias de interrupção depende da topologia da rede. Conforme descrito, uma medida importante para a topologia de rede é a distribuição de graus da rede. Uma rede sem escala é uma rede cuja distribuição de graus segue uma *Power Law*, pelo menos assintoticamente. Isso significa, além de outras implicações, que a robustez da rede depende de indivíduos com um grau relativamente alto, os chamados *hub*. Se esses *hub* forem atacados, a rede se dividirá em sub-redes. (DUIJN; KASHIRIN; SLOOT, 2014)

Power Law representam parâmetros funcionais que podem descrever distribuições de probabilidade, onde pode ocorrer com muita frequência o que é chamado de rede de mundo pequeno. Uma *Power Law* é definida pela Equação 9.

$$P(k) \sim^{-\gamma}, \quad (9)$$

onde onde $P(k)$ é a probabilidade de um nó ter o grau k e γ é o expoente de escala.

Analizando os resultados na Figura 27 e o valores extraídos da distribuição, podemos perceber que a distribuição de graus não caracteriza uma *Power Law*, mas se aproxima. Isso leva a crer que a rede pode ser vulnerável a ataques deliberados e direcionados, visando os *hub* da rede. (ALBERT; JEONG; BARABÁSI, 2000)

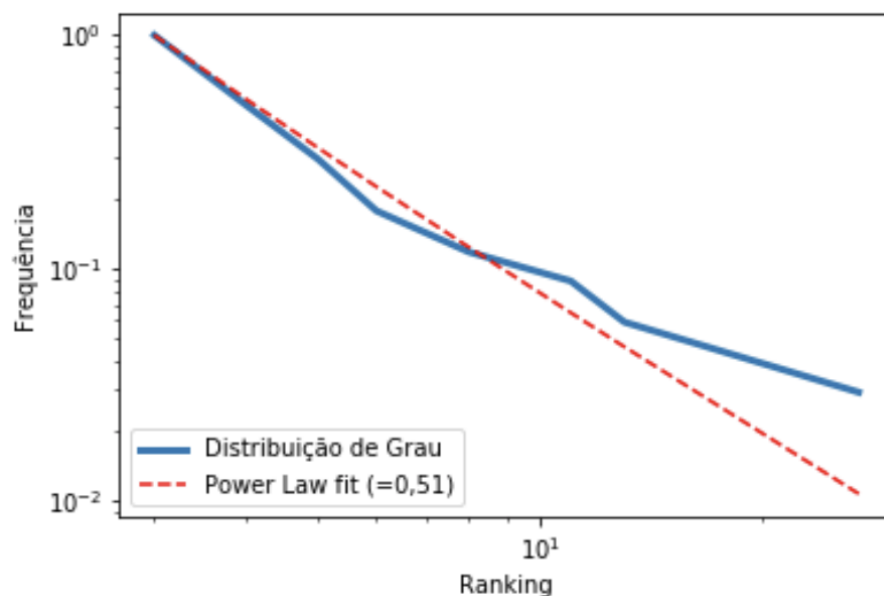


Figura 27 – Frequência de classificação para os dados e aproximação por distribuições de *Power Law*.

A resiliência da rede de criminalidade contra a ruptura depende da redundância da rede. Redes de criminalidade redundantes oferecem diversas alternativas para substituir indivíduos dentro da rede. Agora passaremos a simular diferentes estratégias para interromper a rede de criminalidade, com a convicção que a rede tentará se recuperar substituindo os indivíduos retirados e suas respectivas ligações na rede de criminalidade. Modelar este conjunto é necessário para efetuar as simulações.

A ruptura da rede de criminalidade busca impedir ou frustrar a cadeia de valor de atividades criminosas, removendo indivíduos desta rede. Isto é feito direcionando e prendendo indivíduos estratégicos na cadeia de valor da rede de criminalidade. A ordem sequencial a ser seguida depende da estratégia de ruptura aplicada. Neste estudo quatro estratégias de ruptura são estabelecidas:

1. Estratégia de *Degree*;
2. Estratégia de *Betweenness*;
3. Estratégia de *PageRank*;
4. Estratégia de Média de Centralidades (*Degree+Betweenness+PageRank*);

Ao simular as estratégias estabelecidas, foi medido o efeito que elas tem na rede de criminalidade. Para cada estratégia, diversos passos foram realizadas, com indivíduos sendo removidos da rede.

Para entender a resiliência da rede de criminalidade é necessário entender o efeito da ruptura da rede. A capacidade de uma rede de criminalidade recuperar sua estrutura de cadeia de valor depois da aplicação de uma estratégia de ruptura precisa ser simulada. Um indivíduo de maior grau na classificação da estratégia é retirado e deve ser substituído pelo próximo elemento da classificação. Ao efetuar esta substituição, o ator substituído assume as ligações do indivíduo substituído. Assim, ao modelar a recuperação da rede de criminalidade, mostramos a interação dinâmica entre a rede de cadeia de valor e a rede de criminalidade, na busca de substitutos adequados para recuperação da rede. A cada passo, um indivíduo é direcionado pela estratégia de ruptura escolhida.

Depois de realizadas as simulações de ruptura e recuperação, simultaneamente, com as estratégias estabelecidas, foi medido o impacto que ocasionou na estrutura da rede de criminalidade. A medida de eficiência dentro da rede de cadeia de valor é estabelecida por Duijn, Kashirin e Slood (2014), com a Equação 10:

$$E(G) = \frac{1}{n(n-1)} \sum_{(i < j \in G)} \frac{1}{d(i,j)} \quad (10)$$

Nessa métrica G é a sub-rede, $d(i,j)$ corresponde à distância entre os atores i e j do G e n é igual à quantidade de atores no G . O denominador cria uma medida que varia de 0 a 1, onde 1 é a conectividade completa e 0 representa que a rede está completamente

separada. Os resultados estão no Apêndice G.

Uma segunda métrica é necessária para estimar a influência da interrupção da rede no sigilo dentro da cadeia de valor. Segundo Duijn, Kashirin e Slood (2014), *"as estruturas de rede de criminalidade organizam um nível de sigilo ao minimizar a transferência direta de informações, reduzindo assim o risco de expor o envolvimento direto em atividades ilegais de membros individuais à vigilância policial ou a serviços de inteligência. O sigilo está fortemente associado à métrica de densidade de rede"*, fato esperado uma vez que ocorre a redução no número de indivíduos. A medida de densidade da rede é calculada com a Equação 1. Os resultados estão no Apêndice H.

Cada simulação foi realizada com o objetivo de interromper a cadeia de valor da rede de criminalidade, com a estratégia de interrupção direcionada aos indivíduos em ordem de classificação, até o momento que ocorre a ruptura da rede, sendo, *Degree* no 52º passo, *Betweenness* no 56º passo, *PageRank* no 43º passo e a Média das Centralidades no 45º passo.

A Figura 28 apresenta a eficiência da rede de cadeia de valor com recuperação para cada estratégia. A medida que as estratégias de interrupção são aplicadas, a eficiência da rede aumenta. Isto induz que, quando os indivíduos estão sendo direcionados da cadeia de valor, mais eficiente a rede se torna após cada recuperação. De uma perspectiva topológica, isso implica que a rede é altamente resiliente e flexível na restauração dessas facetas cruciais da cadeia de valor a partir de sua estrutura de rede. Isto demonstra que a rede pode se recuperar encontrando substitutos próximos, mais fáceis e visíveis de se encontrar.

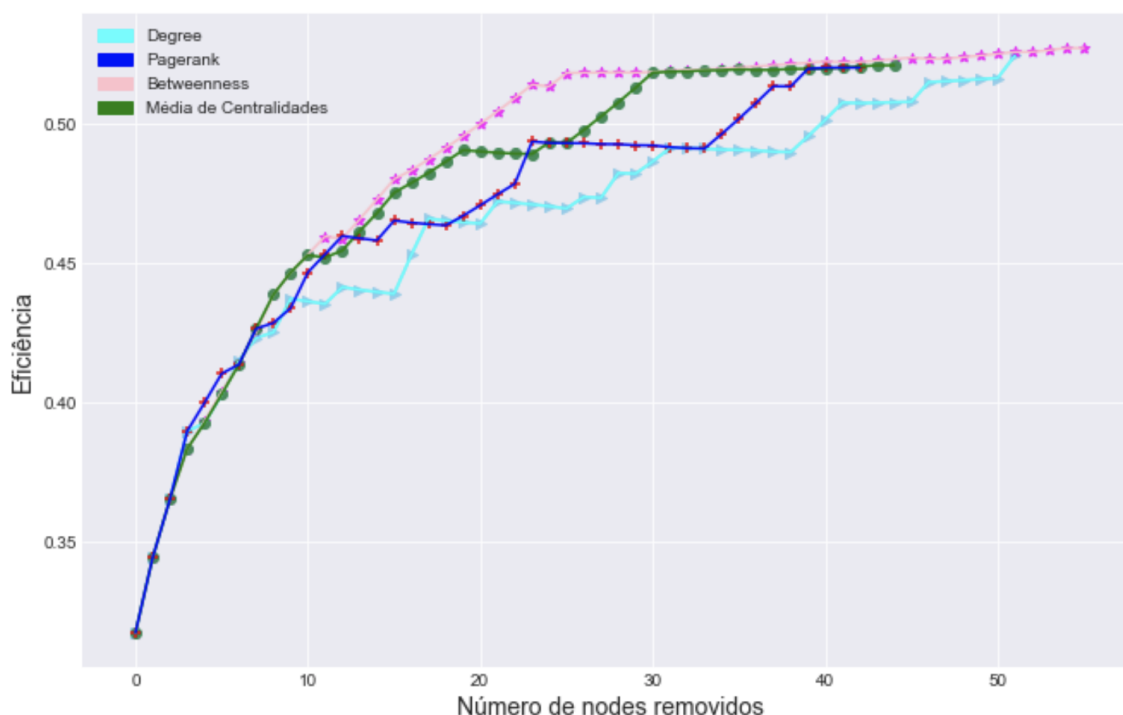


Figura 28 – Eficiência da cadeia de valor de cada estratégia na rede de criminalidade.

A Figura 29 demonstra o que acontece com a densidade (segurança) da rede de cadeia de valor, antes e depois de aplicar as estratégias de resiliência. A segurança da rede da cadeia de valor aumenta a cada intervenção, como já esperado. Isto induz que os indivíduos da rede tentam continuar as atividades criminosas, sendo levados a se comunicar de forma mais eficiente como resultado da estratégia de ruptura estabelecida. Para recuperar a cadeia de valor, estes indivíduos passam a atuar como intermediários para estabelecer novas relações da cadeia de valor. Como resultado, a densidade da rede aumenta, tornando-se mais redundante a cada nova ruptura.

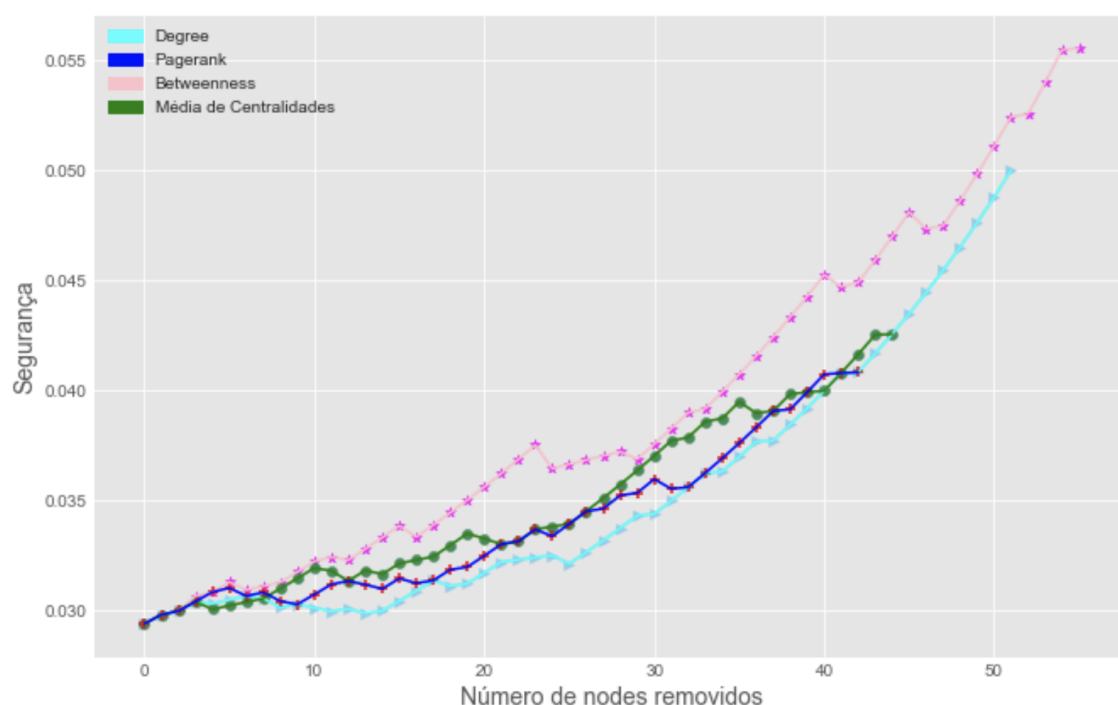


Figura 29 – Segurança da cadeia de valor de cada estratégia na rede de criminalidade.

Para identificar a melhor estratégia foi analisada a eficiência e segurança de cada uma. No momento de ruptura, temos os seguintes graus de eficiência para cada estratégia: *Degree* = 0.524; *Betweenness* = 0.527; *PageRank* = 0.520; Média de Centralidades = 0.520. Os menores valores das estratégias de *PageRank* e Média de Centralidades indicam que os indivíduos estão mais expostos com estas estratégias. Os graus de segurança destas duas estratégias são: *PageRank* = 0.040; Média de Centralidades = 0.042. O maior valor da estratégia de Média de Centralidade indica que seus indivíduos estão mais expostos. Assim, a estratégia de Média de Centralidades é a mais indicada para resiliência da rede de criminalidade e, portanto, também a melhor estratégia para ruptura.

Os resultados para simulação da recuperação por Média de Centralidades são mostrados nas Figuras 30 e 31.

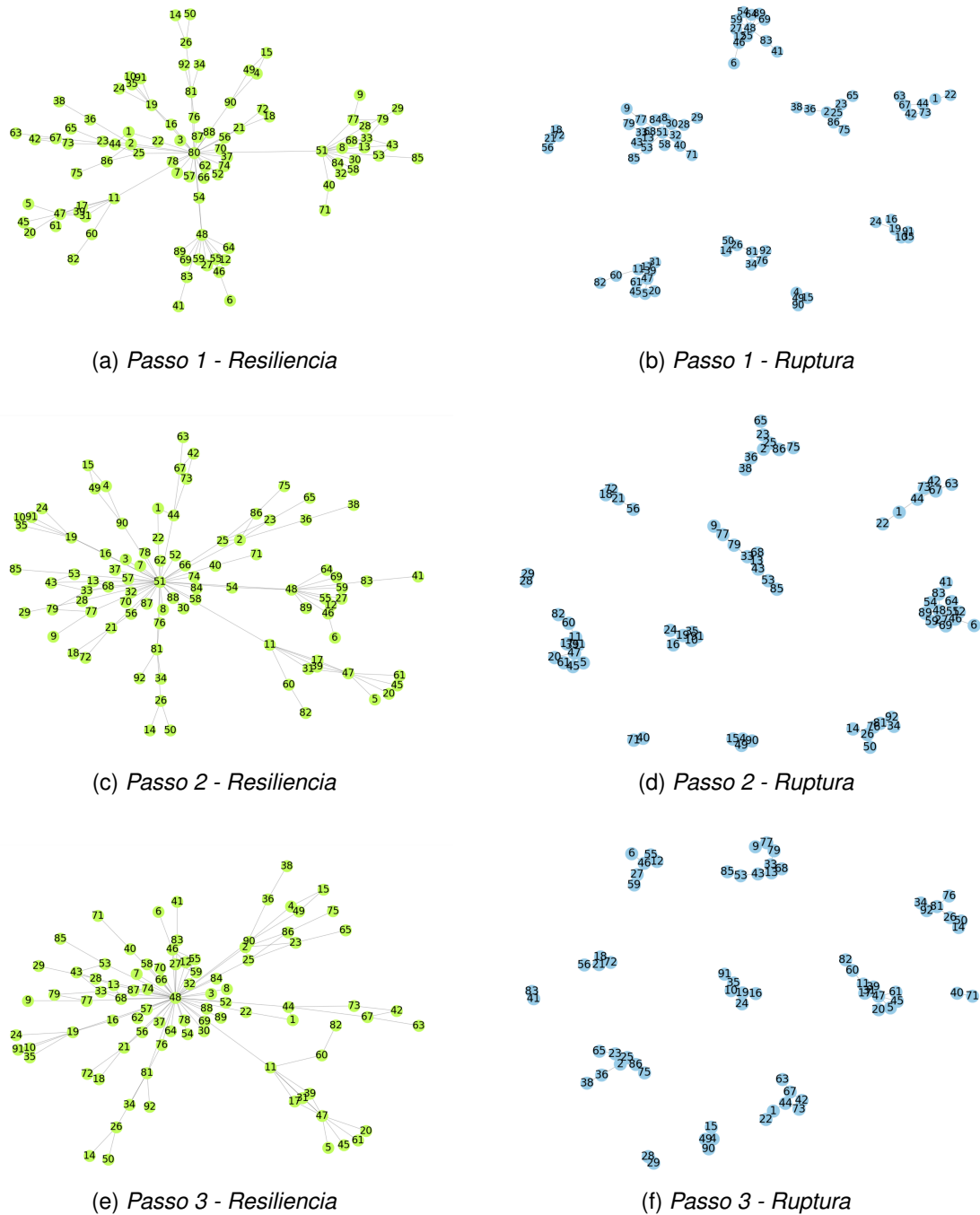


Figura 30 – Representação dos passos da simulação com estratégia de Média de Centralidades, mostrando o resultado dos três primeiros passos, onde os passos consistem em identificar o indivíduo de maior valor na classificação da estratégia e retirar, sendo substituído pelo próximo elemento da classificação. No passo 1 foi identificado o indivíduo 80 com maior valor na classificação, sendo então retirado. Ao ser retirado, a rede sofre uma ruptura, porém mantém sub-redes. No passo 2 o indivíduo de maior valor, no caso o indivíduo 51, assume as ligações do indivíduo 80, substituído. Sendo retirado o indivíduo 51, a rede sofre nova ruptura, mas mantém sub-redes. No passo 3 o indivíduo 48, de maior valor, assume as ligações do indivíduo 51. Ao se retirar o indivíduo 48 a rede sofre outra ruptura, mantendo sub-redes.

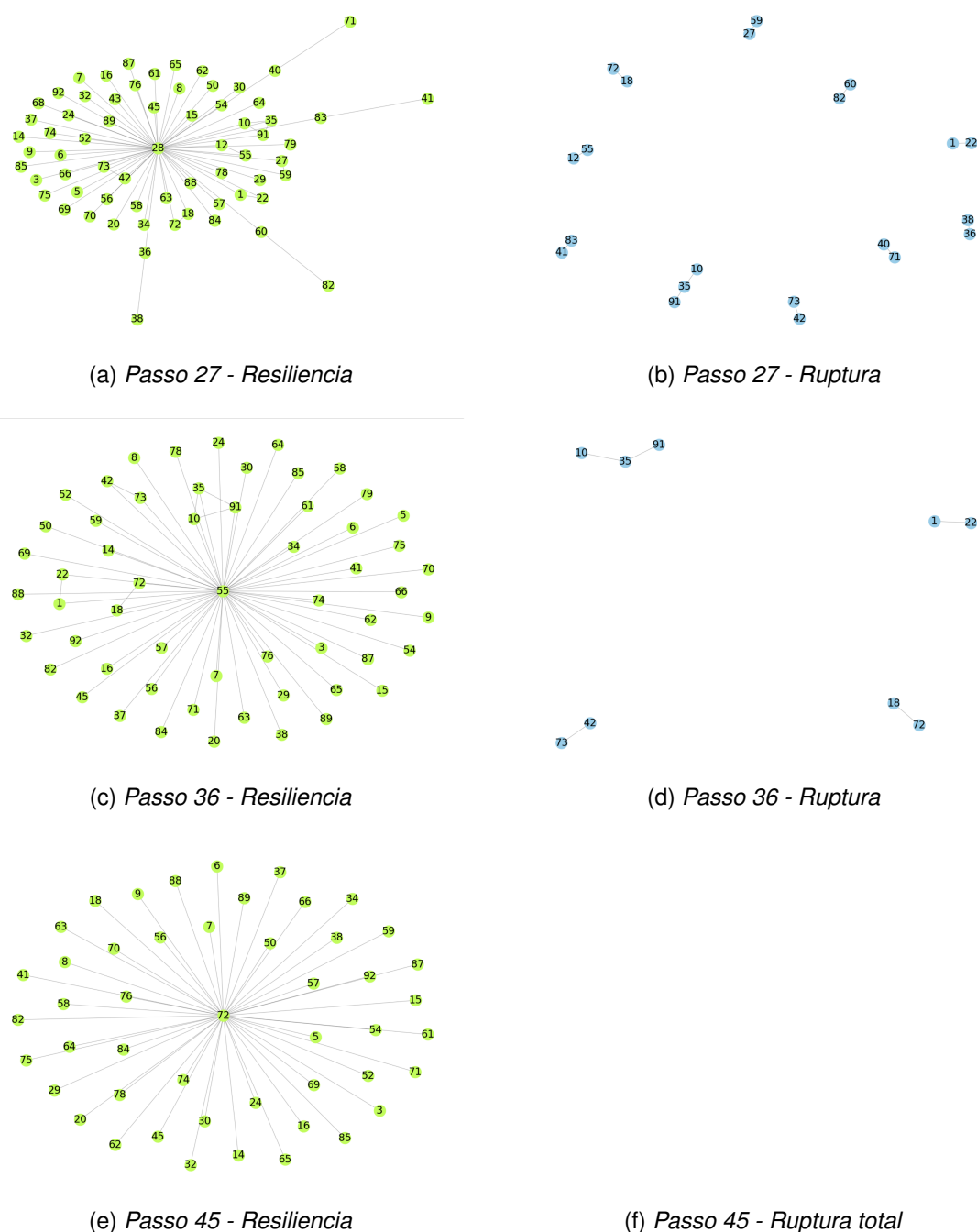


Figura 31 – Representação dos passos da simulação com estratégia de Média de Centralidades, mostrando o resultado dos passos 27, 36 e 45, onde as sub-redes se mantêm até o 45º passo, quando o indivíduo 72 é retirado e a rede sofre uma ruptura total, ou seja, não mantém mais nenhuma ligação. Na simulação dessa estratégia a eficiência e segurança se mantêm até o 45º passo, quando ocorre a interrupção da rede.

Independente de qual estratégia utilizada, o custo material e humano para ruptura da rede é muito elevado, pois representa o número de indivíduos a serem presos para interrupção da rede: *Degree* = 52 indivíduos presos; *Betweenness* = 56 indivíduos presos; *PageRank* = 43 indivíduos presos; Média de Centralidades = 45 indivíduos presos. Isto

inviabilizaria a aplicação de qualquer destas estratégias em Inteligência de Segurança Pública para redução da criminalidade.

Através da análise de subgrupos, discutida anteriormente, uma abordagem viável seria a intervenção de Inteligência de Segurança Pública para identificação e prisão dos *hub* de cada comunidade, perfazendo um total de dez prisões, o que traria os custos materiais e humanos a um patamar aceitável, mantendo uma ótima eficiência nesta abordagem.

A Figura 32 demonstra que ao retirar os dez primeiros elementos da classificação a medida de eficiência decai (Apêndice I).

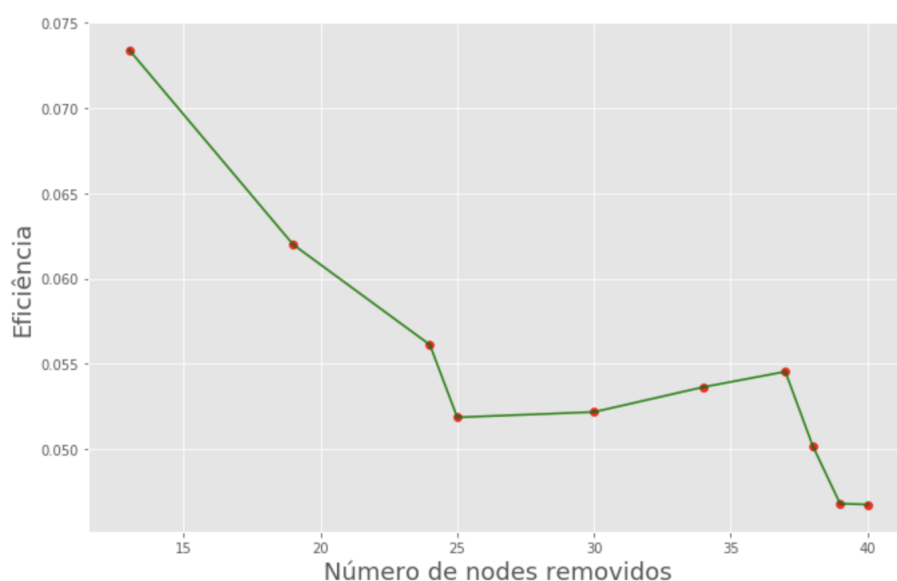


Figura 32 – Eficiência da ruptura da rede usando classificação da análise de subgrupos.

Na medida que os indivíduos são removidos, vai ocorrendo a ruptura na rede, vista nas Figuras 33 e 34, com a rede dividida em 15 componentes isolados e sem uma liderança aparente e visível após a décima ruptura.

Tornando estes indivíduos, que se concentram em posições de alto grau, em alvos de uma abordagem de interrupção, estabelecemos uma forma eficiente e segura de interromper uma rede de criminalidade.



Figura 33 – Representação das redes após rupturas parciais, mostrando o resultado das rupturas 1 a 6, indicando um bom impacto para uma abordagem de intervenção de Inteligência de Segurança Pública atuando especificamente dentro da cadeia de valor de uma rede de criminalidade. Os dez indivíduos mais 'visíveis' são vulneráveis a abordagem de análise de subgrupos. São indivíduos que tem alta pontuação nas medidas de centralidade, atuando como *hub* da rede.

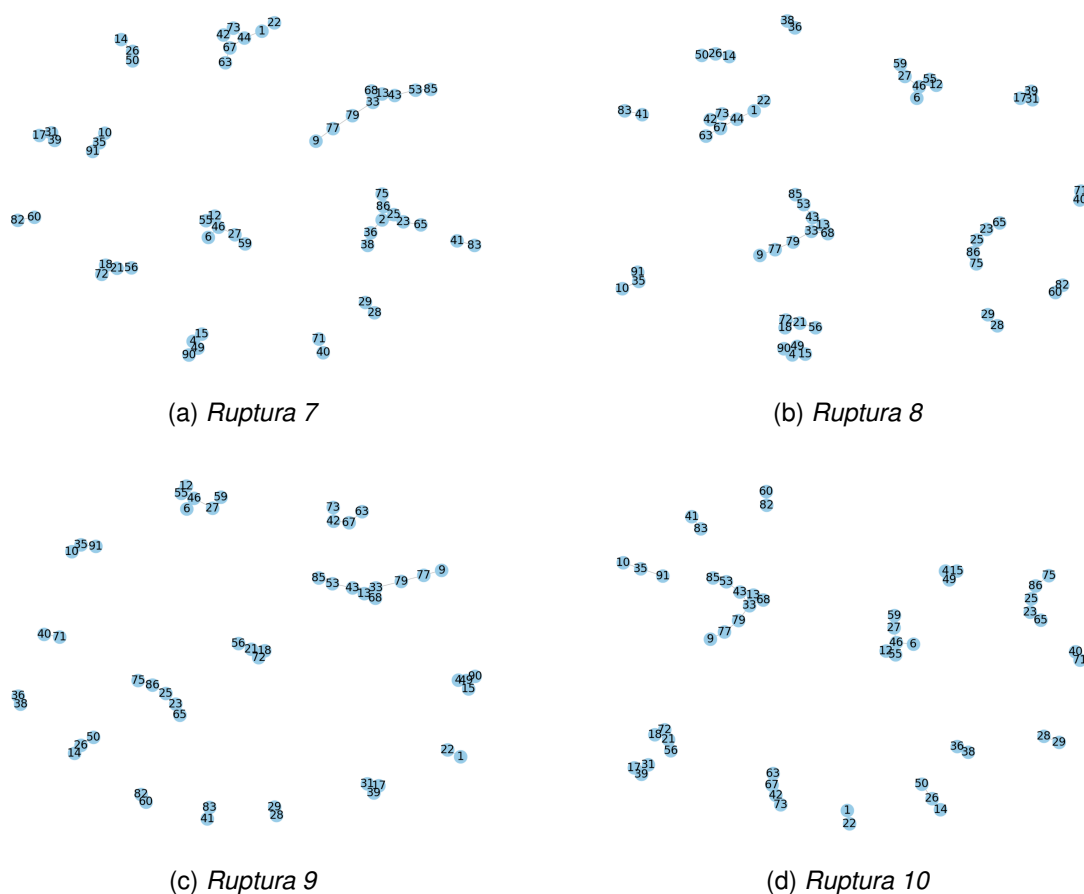


Figura 34 – Representação das redes após rupturas parciais, mostrando o resultado das rupturas 7 a 10, onde os indivíduos centrais e não tão ocultos, ao serem retirados da rede, afetam sua topologia, dividindo-as em conjuntos isolados. O impacto desta abordagem reduz a recuperação dinâmica da rede, reduzindo sua eficiência.

5.5 Multiplexidade de Redes de Criminalidade

Seguindo o objetivo do estudo, foi organizado um conjunto de dados relacionais, contendo informações dos crimes praticados pelos indivíduos das Rede de Inteligência e Gangue, que podem ser vistos, de forma unidimensional, na Figura 35. Os criminosos e seus crimes respectivos estão discriminados no Apêndice J.

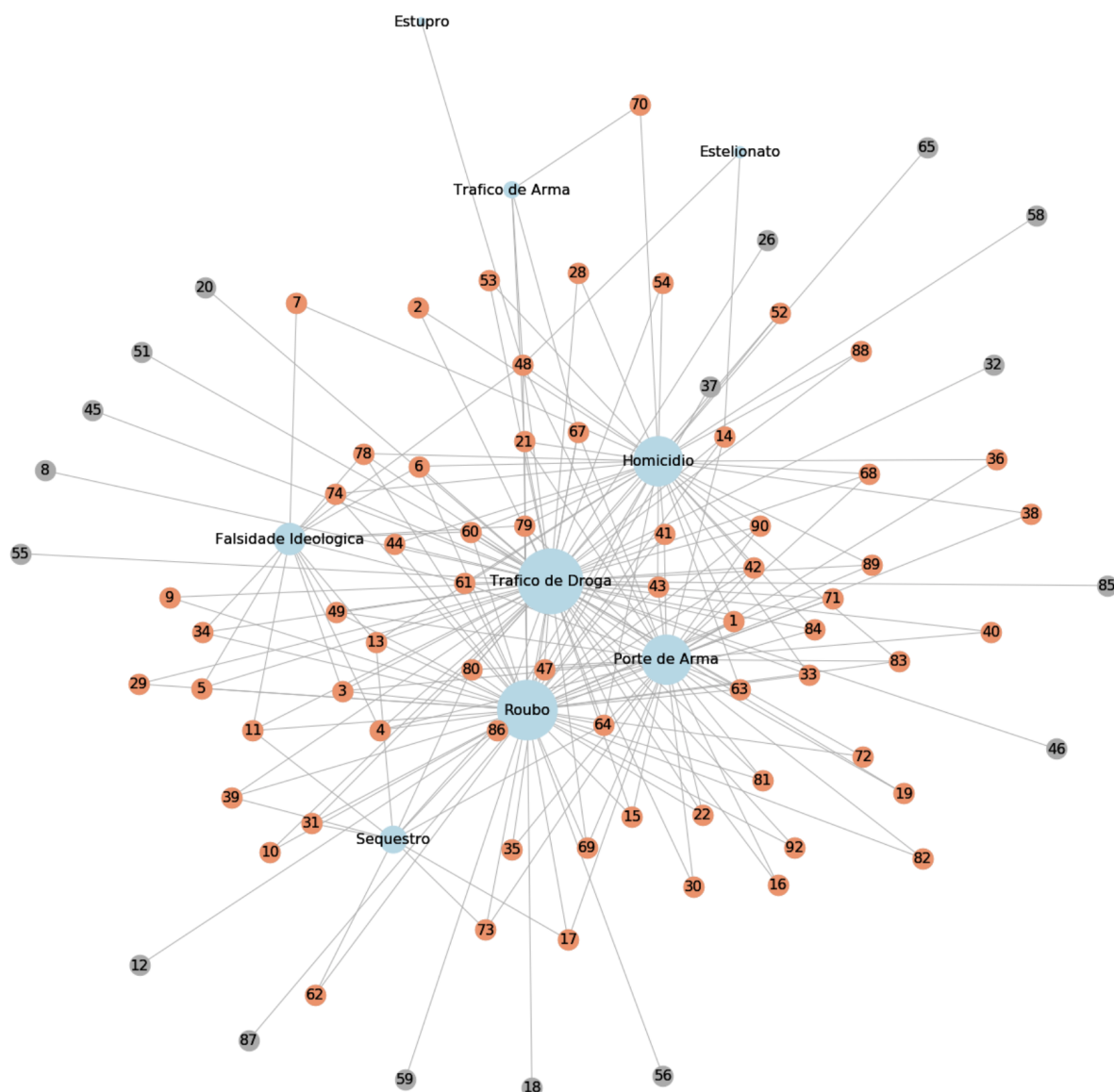


Figura 35 – Identificação das nove modalidades de crime da rede com seus respectivos participantes. Os indivíduos apresentados na cor laranja participam de mais de um crime simultaneamente.

A Figura 36 mostra a rede de Inteligência e Gangue, de forma multidimensional. É possível visualizar nesta Figura que todos os indivíduos da Rede de Gangue estão presentes na Rede de Inteligência, mas os seus relacionamentos são diferentes dentro de cada rede.

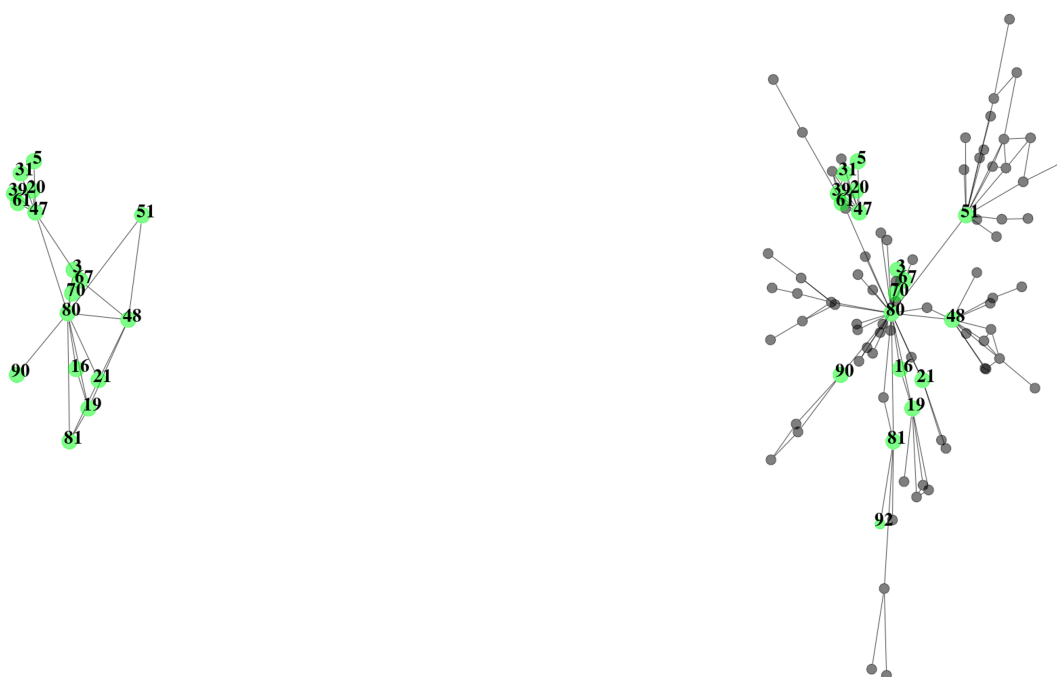


Figura 36 – Rede *multiplex* de Gangue e Inteligência.

Com o objetivo de realizar uma análise mais minuciosa da participação dos indivíduos nos diferentes crimes, para identificar relações fortes que podem implicar relações de confiança, foram considerados os crimes de Tráfico de Drogas, Roubo, Homicídio, Porte de Arma, Sequestro, Tráfico de Armas e Falsidade Ideológica como redes independentes. No entanto, os crimes de Estelionato e Estupro não foram considerados por não apresentarem atores que se relacionam na respectiva esfera. Assim, a combinação dos crimes geram a Figura 37, que representa a rede *multiplex* de criminalidade utilizada neste estudo.

Os laços tendem a ser fortes na medida que o relacionamento social tem múltiplas bases, gerando confiança e reciprocidade em ações criminosas. A Figura 38 apresenta o número de criminosos atuantes em cada camada.

Além de limitarmos os sete componentes da rede *multiplex* de criminalidade, também limitamos a visualização das camadas *multiplex* àqueles indivíduos que têm vínculos criminosos, eliminando os indivíduos sem vínculos criminosos. Na Figura 39 pode-se visualizar a rede *multiplex* de criminalidade, com 77 indivíduos e 232 ligações múltiplas. A estrutura *multiplex* define uma rede de criminalidade, na medida que evidencia sua organização.



Figura 37 – Rede *multiplex* de criminalidade, representando os crimes, contendo todos os 92 indivíduos com suas ligações em cada camada.

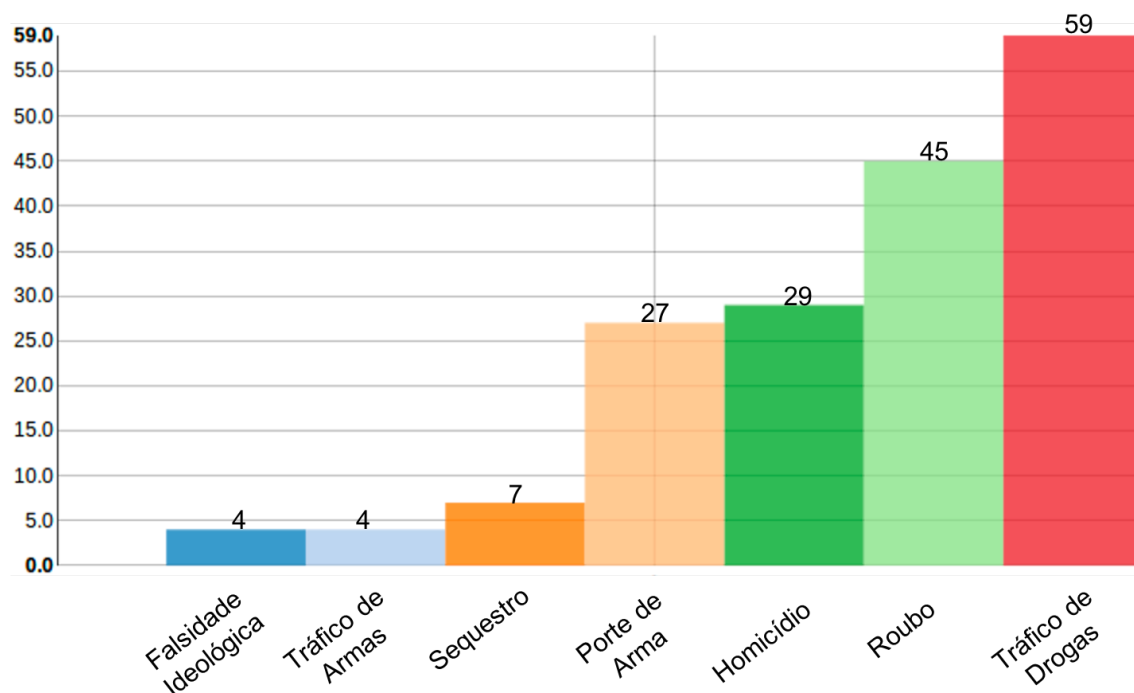


Figura 38 – Número de criminosos ativos em cada uma das sete camadas.

O estudo baseou-se em subconjuntos de laços do banco de dados das Redes de Inteligência e Gangue, onde a análise, especificamente, se concentra em 7 esferas criminais citadas. Em Domenico et al. (2013b), Arruda et al. (2017) foi proposta uma medida de multiplexidade, chamada *Multiplexity*, que é definida como o número N de camadas em que o nó participa dividido pelo número total de camadas C , ou seja, os valores dizem respeito a participação global de um indivíduo na rede *multiplex*, cujos resultados estão no Apêndice K. Na Figura 40 é possível identificar os 10 maiores valores de *Multiplexity* da rede.

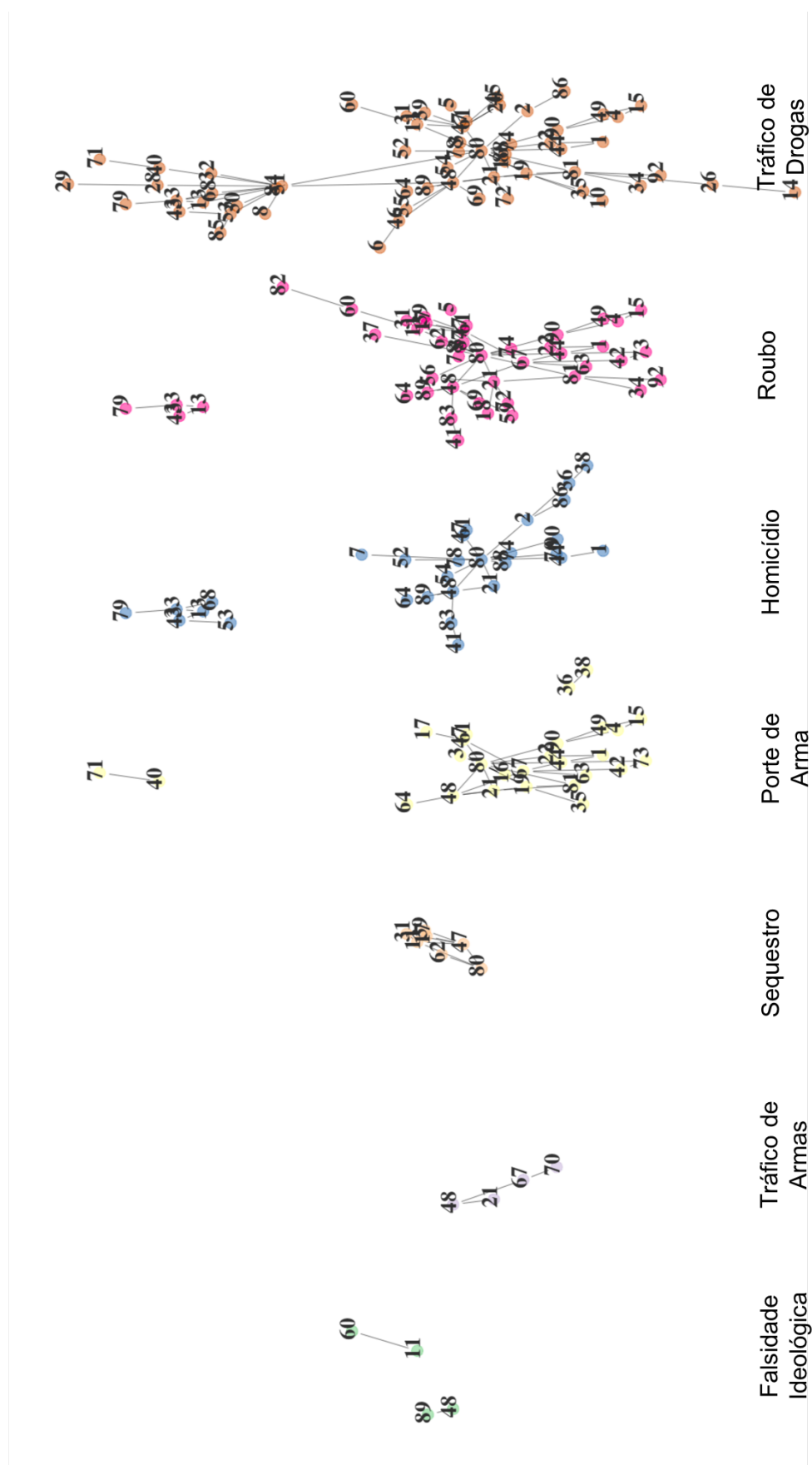


Figura 39 – Rede *multiplex* de criminalidade em sete camadas representando os diferentes crimes, contendo somente os indivíduos com suas ligações em cada camada. Esta visão, com a retirada dos nós isolados, permite uma melhor identificação de cada indivíduo nas camadas de rede *multiplex*.

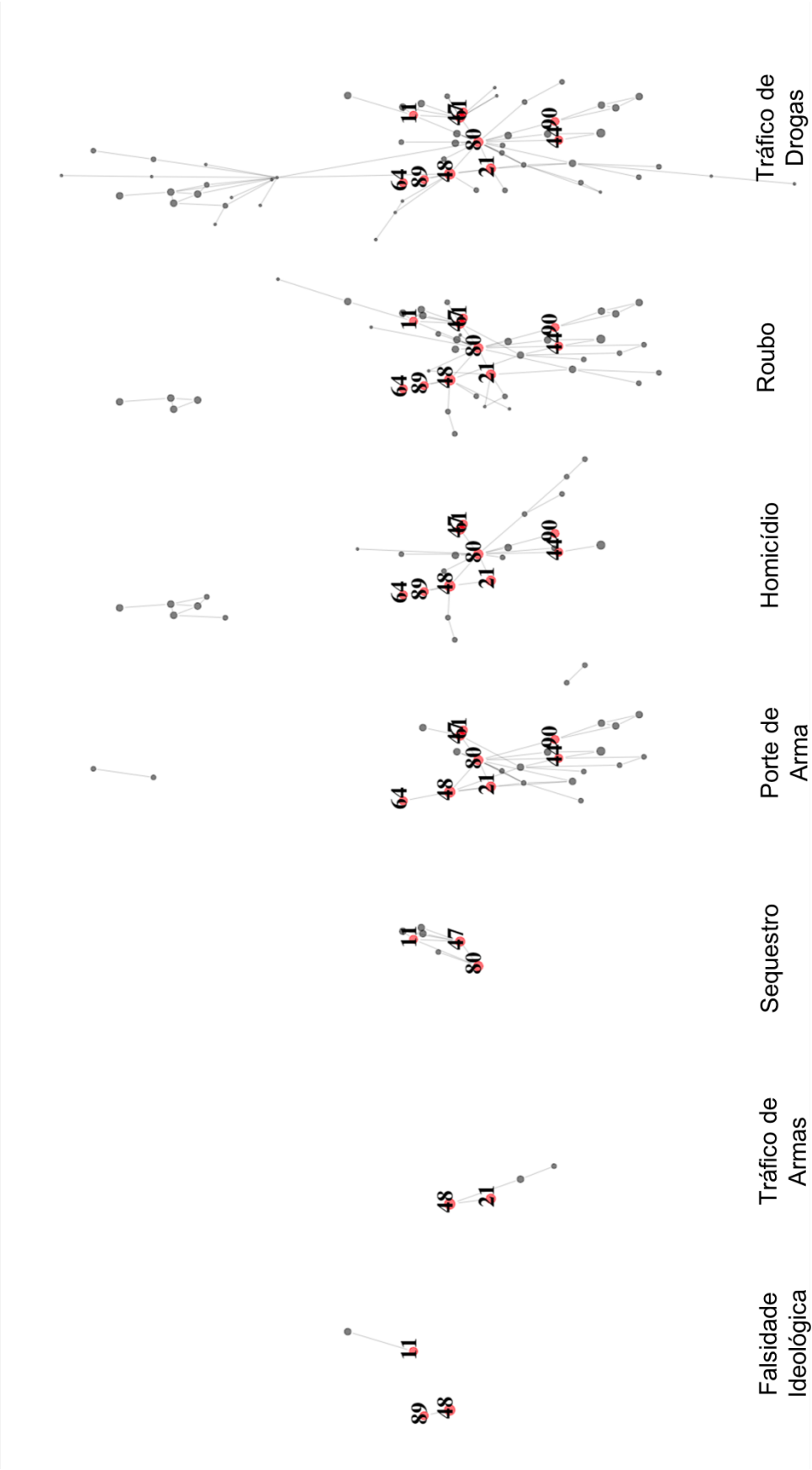


Figura 40 – Rede *multiplex* de criminalidade em sete camadas, evidenciando os 10 maiores valores de *Multiplexity*.

Um conceito frequentemente utilizado em contextos científicos e não científicos com o intuito de representar a variedade de entidades ou formas um determinado sistema possui é a diversidade. Várias medidas tem sido propostas na literatura com o objetivo de capturar diferentes aspectos da diversidade (WEITZMAN, 1992; BOSSERT et al., 2001; STIRLING, 2007; GAO; BARZEL; BARABÁSI, 2016; EMMERT-STREIB; DEHMER, 2012; FU; HUANG; SUN, 2015; MIN et al., 2014; MOUGI; KONDOH, 2012; RADUCHA; GUBIEC, 2018; WANG et al., 2016).

Carpi et al. (2018) estabelecem uma medida, baseada nos conceitos propostos por Weitzman (1992) e Bossert et al. (2001), que quantifica, no contexto de redes complexas, a diversidade dos padrões de conexões, a partir das medidas de dissimilaridade das camadas da estrutura *multiplex*.

Neste contexto, diversidade refere-se à variedade de configurações de conectividade que possuem os elementos que constituem a rede (ex., nós e camadas). Segundo Duijn, Kashirin e Slood (2014), diversidade de relações em redes criminosas tem sido relacionado com o conceito de resiliência.

Foi mostrado em Duijn, Kashirin e Slood (2014) que, quando redes criminosas são perturbadas elas desenvolvem a capacidade de absorver e de resistir a essas perturbações, adaptando-se à mudança quando necessário; isso é chamado de resiliência de rede. Quanto mais uma estrutura é diversa em termos de padrões de conexões dos seus indivíduos, mais resiliente se torna, já que existem mais opções para compensar mudanças por perdas de capital humano, ou para encontrar novos métodos para continuar operando eficientemente.

A importância das medidas de diversidade nas redes é a de identificar os elementos que são críticos para manter a funcionalidade do sistema e desta maneira estabelecer estratégias para dismantelar a rede. Em Carpi et al. (2018) foi proposto um método para calcular diversidade em redes *multiplex*, baseado no cálculo de dissimilaridades de camadas e de nós, e nos métodos propostos por Weitzman (1992) e Bossert et al. (2001).

Tendo como referência a rede *multiplex* de criminalidade, foi computada a diversidade em dois níveis diferentes, *diversidade local* (U_i) que se refere à diversidade das conexões de um nó nas diferentes camadas; e *diversidade global* (U), que se refere à diversidade de conexões no sistema.

Para isto foram calculadas primeiro a distância de um nó nas diferentes camadas, onde $\mathcal{D}_i(\bar{p}, \bar{q})$ é a distância do nó i nas camadas $\bar{p}$ e $\bar{q}$, chamada como dissimilaridade de Nó (ND) e entre camadas $\mathcal{D}(\bar{p}, \bar{q})$, chamada como dissimilaridade das Camadas (LD).

Dissimilaridade de Nó quantifica as diferenças dos padrões de conectividade do nó i

nas camadas $\bar{p}$ e $\bar{q}$, Equação 11.

$$\mathcal{D}_i(\bar{p}, \bar{q}) = \frac{\sqrt{\mathcal{J}(\mathcal{N}_i^{\bar{p}}, \mathcal{N}_i^{\bar{q}})} + \sqrt{\mathcal{J}(T_i^{\bar{p}}, T_i^{\bar{q}})}}{2\sqrt{\log(2)}}, \quad (11)$$

onde, $\mathcal{J}$ é a divergência de Jensen-Shannon que mede a dissimilaridade entre funções de distribuição de probabilidade (probability distribution functions - *PDFs*) (SCHIEBER et al., 2017). $\mathcal{N}_i^{\bar{p}}$ é a Distribuição de Distância (NDD) do nó i na camada $\bar{p}$: $\mathcal{N}_i^{\bar{p}}(d)$ é a fração de nós que estão a distância d (caminho mínimo) do nó i na camada $\bar{p}$. $T^{\bar{p}}$ corresponde à Matriz de Transição da camada $\bar{p}$. $T^{\bar{p}}$ é a Matriz de Adjacência da camada $\bar{p}$, re-escalada pelo grau de cada nó.

Quando $\mathcal{D}_i(\bar{p}, \bar{q}) = 0$ as *PDFs* são idênticas, ou seja, o nó i possui iguais padrões de conexões nas camadas p e q . Já quando $\mathcal{D}_i(\bar{p}, \bar{q}) = 1$ as dissimilaridades de i nas camadas p e q são extremos, onde o nó i encontra-se desconectado em uma camada (não ativo) e conectado de alguma forma a todos os nós da outra.

Dissimilaridade das Camadas quantifica as diferenças entre padrões de conectividade das camadas $\bar{p}$ and $\bar{q}$. Dissimilaridade das Camadas é simplesmente $\mathcal{D}_i(\bar{p}, \bar{q})$ considerando todos os nós, Equação 12,

$$\mathcal{D}(\bar{p}, \bar{q}) = \langle \mathcal{D}_i(\bar{p}, \bar{q}) \rangle_i \quad (12)$$

$\mathcal{D}(\bar{p}, \bar{q}) = 0$ indica que as camadas p and q são idênticas e $\mathcal{D}(\bar{p}, \bar{q}) = 1$ indica que uma das camadas está totalmente conectada, enquanto que a outra está totalmente desconectada. $\mathcal{D}$ tem propriedades de métrica.

O modelo proposto por Weitzman (1992) e reformulado por Bossert et al. (2001) caracteriza a medição da diversidade como uma função de dissimilaridade, que pode ser definida como uma distância. Na continuação será definida a função de dissimilaridade segundo Carpi et al. (2018).

Seja $\tilde{S}$ o conjunto de todas as entidades, que no contexto de redes *multiplex* pode ser o conjunto de nós ou o conjunto de camadas. Assumindo que temos o conjunto $S \subset \tilde{S}$ e que podemos computar as distancias entre todas elas, definimos a distância entre o elemento $\bar{g} \notin S$ e o conjunto S , $\mathcal{D}(\bar{g}, S)$, como a menor distancia entre $\bar{g}$ e qualquer elemento do conjunto S :

$$\mathcal{D}(\bar{g}, S) = \min_{s_i \in S} \mathcal{D}(\bar{g}, s_i) \quad (13)$$

A distância de um elemento que não pertence ao conjunto é definida como a mínima

distância desse elemento ao conjunto. Na Equação 13 quando consideramos os nós, a distância $\mathcal{D}(\bar{g}, \bar{s}_i)$ é a ND, Equação 11; quando as entidades são as camadas, $\mathcal{D}(\bar{g}, \bar{s}_i)$ é a LD, Equação 12.

A função de diversidade $U : \tilde{S} \rightarrow \mathbb{R}_+$, é definida recursivamente como $U(S) = \max_{\bar{s}_i \in S} \{U(S \setminus \bar{s}_i) + \mathcal{D}(\bar{s}_i, S \setminus \bar{s}_i)\}$ para todo $S \in \tilde{S}$ com $|S| \geq 2$, onde $|S|$ representa a cardinalidade do conjunto e $U(S) = 0$, para todo $S \in \tilde{S}$ tal que $|S| = 1$.

Usaremos U_i para nos referir à diversidade dos nós i nas diferentes camadas e U para nos referir à diversidade das camadas. Quando um elemento, nó ou camada, é removido, a diversidade do sistema diminui. Se $\bar{g}$ é removida de $S \cup \bar{g}$, a "perda" de diversidade é ao menos igual a $D(\bar{g}, S)$, $U(S \cup \bar{g}) \geq U(S) + D(\bar{g}, S)$.

Através de um método baseado em uma ordem lexicográfica de distância, um conjunto de ordem de diversidade por ser obtido $\mathcal{O}(S) = \{\bar{s}_1, \bar{s}_2, \dots, \bar{s}_{|S|}\}$, que indica os elementos na ordem de sua contribuição a diversidade do sistema.

Usamos $U_i(S)$ para nos referir à diversidade dos padrões de conexões que o nó i tem nas diferentes camadas e $U(S)$, para a diversidade do conjunto de camadas.

Segundo Bossert et al. (2001), no caso de todos os elementos terem o mesmo valor de diversidade (zero no nosso caso), é possível ter uma 'ordem de diversidade' através do cálculo de um método baseado em uma distância lexicográfica: $\mathcal{O}(S) = \{\bar{s}_1, \bar{s}_2, \dots, \bar{s}_{|S|}\}$, que indica os elementos na ordem de contribuição à diversidade ao conjunto. A Figura 41 exemplifica este procedimento.

Assim, foram calculadas as medidas propostas em Carpi et al. (2018). O resultado do cálculo da Dissimilaridade das Camadas é apresentado na Figura 42.

O Resultado da Diversidade de Nó pode ser visto na Figura 43, cujos resultados são listados no Apêndice L. O maior valor de Diversidade de Nó destaca a importância que o indivíduo tem para a estrutura de rede, identificando os líderes da rede *multiplex* de criminalidade.

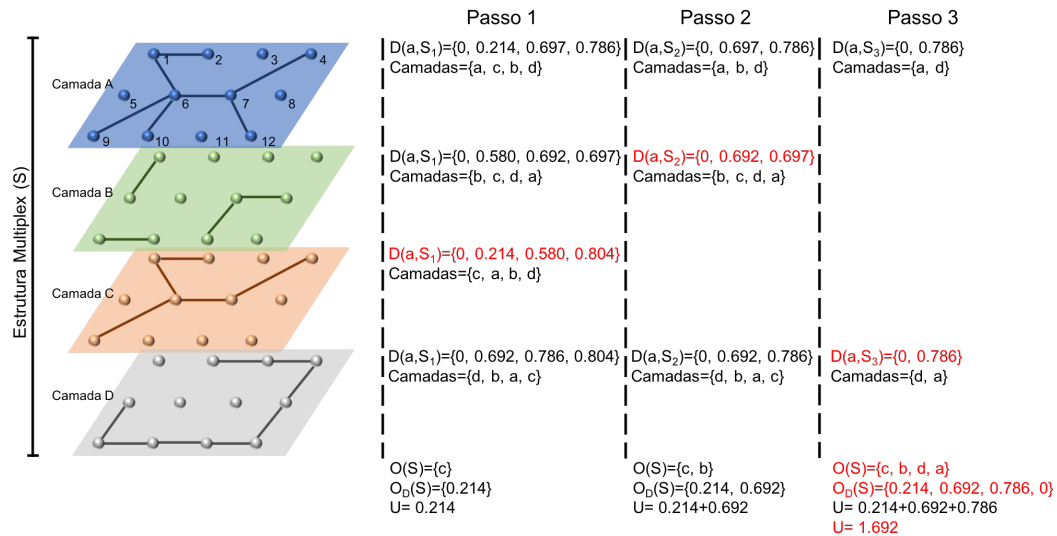


Figura 41 – Cálculo da diversidade de uma estrutura de 4 camadas. As camadas têm os seguintes valores LD : $D(a; b) = 0.697$, $D(a; c) = 0.214$, $D(a; d) = 0.786$, $D(b; c) = 0.580$, $D(b; d) = 0.692$ e $D(c; d) = 0.804$. Calculamos a diversidade do sistema aplicando a equação $U(S)$ recursivamente, com as camadas S_i ordenadas de acordo com a distância ao conjunto $S - S_i$. Etapa 1: em $S = a; b; c; d$, as camadas a e c apresentam o menor valor de LD , e c é a camada que menos contribui para a diversidade de S , já que está mais perto das camadas restantes. Então, o primeiro passo da recursão é $U(S) = U(S_1) + 0.214$ onde $S_1 = S - c$. Passo 2: Em $S_1 = a; b; d$, as camadas b e d apresentam o menor valor de LD , e b é a camada que menos contribui para a diversidade de S_2 . Portanto, $U(S_1) = U(S_2) + 0.692$ onde $S_2 = S_1 - b$. Etapa 3: O valor de LD do conjunto $S_2 = a; d$ é $D(a; d) = 0.786$. Assim, a diversidade de um sistema com cardinalidade 0 é 0, $U(S_2) = D(a; d)$ e $U(S) = 0.214 + 0.692 + 0.786 = 1.692$.

Fonte: adaptado de Carpi et al. (2018) [tradução do autor]

	1	2	3	4	5	6	7
1	0	0,5405	0,5495	0,5632	0,6362	0,6486	0,6224
2	0,5405	0	0,4162	0,3376	0,3910	0,4329	0,4172
3	0,5495	0,4162	0	0,3246	0,2797	0,2466	0,2505
4	0,5632	0,3376	0,3246	0	0,2523	0,2277	0,2475
5	0,6362	0,3910	0,2797	0,2523	0	0,0809	0,0723
6	0,6486	0,4329	0,2466	0,2277	0,0809	0	0,0484
7	0,6224	0,4172	0,2505	0,2475	0,0723	0,0484	0

Figura 42 – Resultados da Dissimilaridade das Camadas da rede *multiplex* de criminalidade, onde: [1] Tráfico de Drogas; [2] Roubo; [3] Homicídio; [4] Porte de Arma; [5] Sequestro; [6] Tráfico de Armas; [7] Falsidade Ideológica - um dos passos para calcular a Diversidade de Nó.

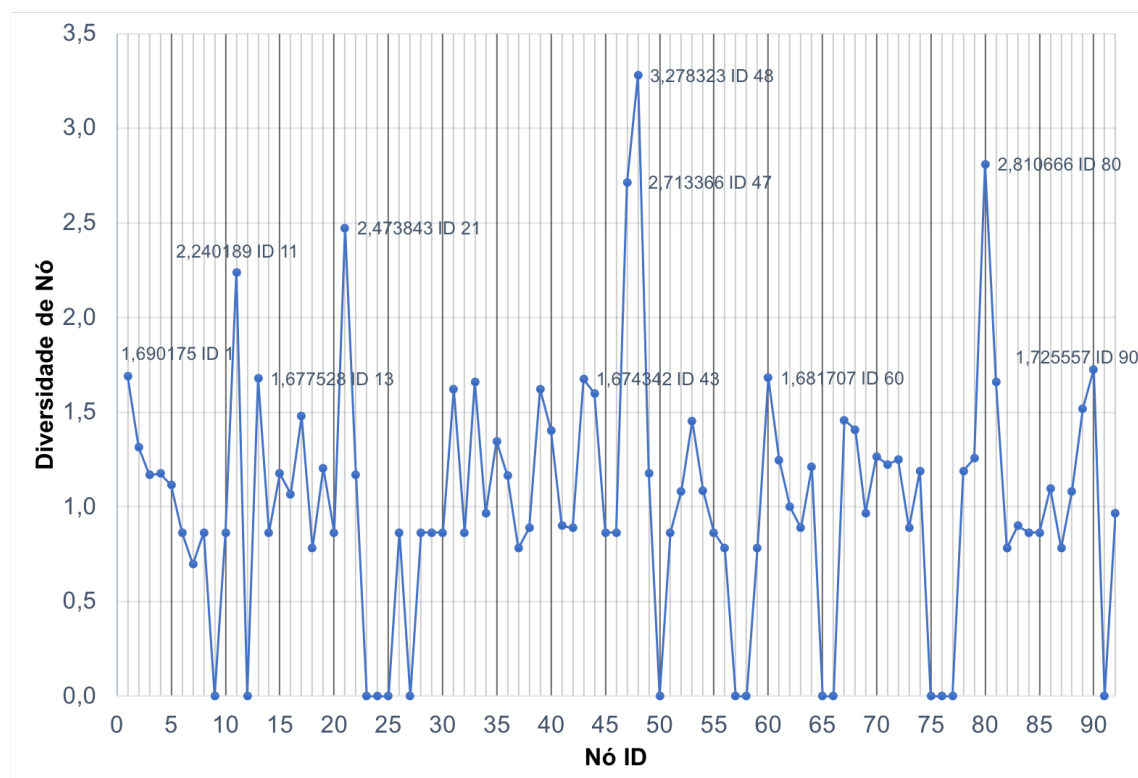


Figura 43 – Diversidade de Nó - Os maiores resultados identificam os líderes da rede *multiplex* de criminalidade. Por esta medida os 10 primeiros líderes são os indivíduos: 48, 80, 47, 21, 11, 90, 1, 60, 13, 43.

O indivíduo 48 destaca-se na rede já que possui o maior valor de Diversidade de Nó. É o indivíduo que mais cometeu crimes (Tráfico de Drogas, Roubo, Homicídio, Porte de Arma, Tráfico de Armas e Falsidade Ideológica) e tem alta redundância de conexões com o indivíduo 80, que possui maiores valores de centralidade na rede, consequentemente gerando alto grau de confiabilidade aos demais indivíduos da rede. Outro fato que destaca o indivíduo 48 é a prática do crime de Tráfico de Armas, indispensável para prática de outros crimes e auto-proteção no ambiente inóspito de criminalidade. O que se pode perceber é que o indivíduo 48 é fornecedor de armas para toda rede.

A redundância de crimes na rede *multiplex* implica em confiança, quanto maior a redundância, maior os laços de confiança entre seus indivíduos, ou seja, representam laços mais fortes. A Figura 44 mostra os 10 laços com maior repetição nas camadas. A redundância de laços reforça o resultado da Diversidade de Nó, identificando os indivíduos 48, 80, 47 e 21 como líderes da rede, cujos resultados são listados no Apêndice M.

No estudo *multiplex* o indivíduo 51 perde a importância como *hub*, elencada pelas medidas de centralidade, por ter cometido somente o crime de Tráfico de Drogas, portanto fazendo parte somente de uma camada *multiplex*. Já o indivíduo 21 vem a tona por estar presente em 4 camadas *multiplex* de criminalidade (Tráfico de Drogas, Roubo, Homicídio, Porte de Arma e Tráfico de Armas), sempre conectado ao indivíduo 80.

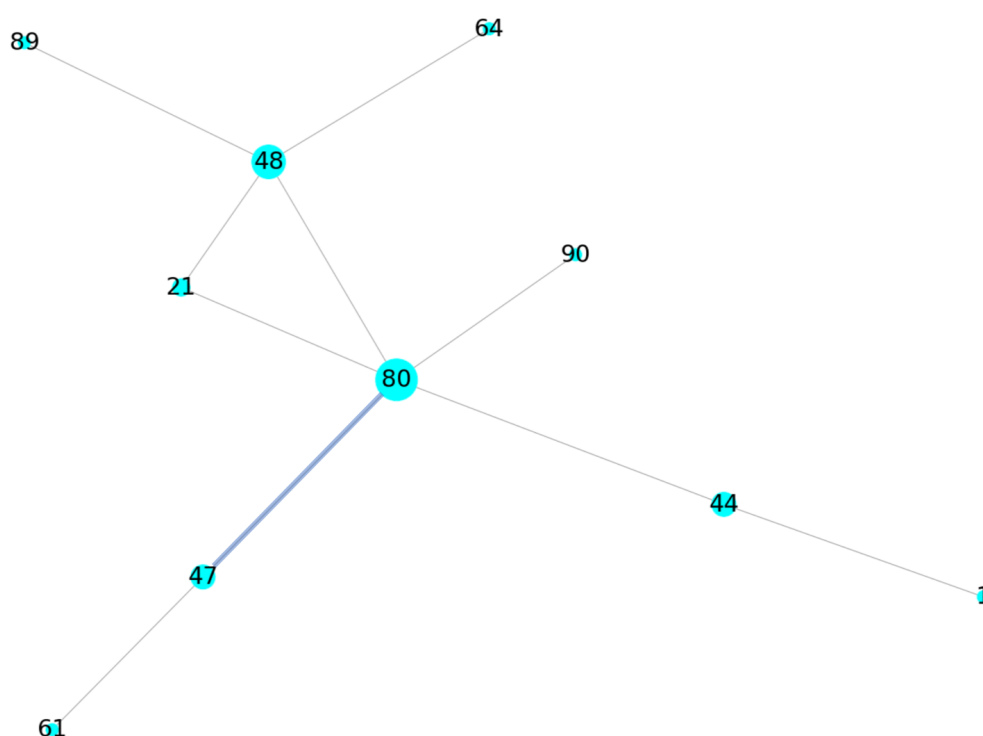


Figura 44 – Rede de maior quantidade de laços *multiplex* - o laço 80-47 têm 5 camadas de laços *multiplex*, enquanto os demais 4 laços.

A ordem de contribuição à diversidade global do sistema *multiplex* foi: [1] Tráfico de Drogas, [3] Homicídio, [2] Roubo, [4] Porte de Arma, [5] Sequestro, [6] Tráfico de Armas e [7] Falsidade Ideológica.

Esta ordem mostra que o crime que mais diversidade traz ao conjunto de crimes é o Tráfico de Drogas, seguido por Homicídio, Roubo, Porte de Arma, Sequestro, Tráfico de Armas e Falsidade Ideológica.

As medidas de centralidade foram capazes de identificar os indivíduos mais centrais da rede, os *hub*, do ponto de vista quantitativo e unidimensional. As funcionalidades *multiplex* abordam características multidimensionais e vão além da centralidade, permitindo identificar os líderes por suas características e valores sociais, ao analisar as camadas de criminalidade, a diversidade, a redundância, a resiliência e a confiança. O estudo *multiplex* destaca o indivíduo que mais influencia a rede de criminalidade, ou seja, o indivíduo cujas ações o tornam mais eficaz na prática de crimes, cujo papel na rede analisada cabe ao indivíduo 48. Enfim, *multiplex*, através de medidas quantitativas, traz a tona um resultado significativo na identificação de líderes de redes de criminalidade.

6 Conclusão

Organizações criminosas foram vistas como redes de indivíduos que buscam interagir entre si, de forma prolongada no tempo, aproveitando atividades criminosas para atrair vantagens, através de atuações em um mercado e em um território. A parceria busca atrair incentivos mútuos de forma a melhorar a produtividade de suas ações, através de uma infraestrutura previamente organizada (MORSELLI, 2009).

Tendo em vista os aspectos apresentados, pode-se caracterizar uma rede de criminalidade como uma rede social que compartilha conexões, informações, estilos e perfis em um sistema voltado à prática de ações criminosas. Estas redes de criminalidade aparecem casualmente entre pessoas que têm algum relacionamento ou atividade comum. Estes podem se caracterizar por amizades, relacionamentos amorosos, de trabalho, ou outras características afins, que levam pessoas a interagir, buscando um objetivo comum, no caso, o crime.

Através dos algoritmos e ferramentas desenvolvidas, foi possível identificar redes de criminalidade para análise; com o uso de medidas de centralidade, foi possível identificar o líder das redes, bem como os líderes das sub-comunidades em rede; como fruto das análises de centralidade, através de simulações, foi possível identificar a melhor forma de romper uma rede de criminalidade, analisando os passos desta ruptura, bem como da resiliência natural decorrente; como resultado de redes *Multiplex*, a rede de criminalidade foi decomposta em camadas por tipo de crimes, permitindo a identificação dos líderes, usando a inédita medida de diversidade no estudo de criminalidade.

6.1 Trabalhos Futuros

Em um mundo de explosão demográfica, crises globais, distúrbios étnicos e religiosos e aumento da criminalidade, a compreensão da estrutura e funcionamento da sociedade, bem como a natureza de suas alterações, é crucial para Segurança Pública.

A crescente integração da tecnologia com as pessoas criou volumes sem precedentes de dados sobre o comportamento cotidiano da sociedade. O uso destes dados abrem novas oportunidades para se trabalhar em direção a um entendimento quantitativo dos sistemas sociais complexos.

Neste contexto é urgente a necessidade de maior conhecimento da complexidade da criminalidade interconectada, bem como da capacidade de se aplicar tais conhecimentos às formulações de políticas de Segurança Pública.

A proposta é trabalhar técnicas computacionais que permitam buscar em redes sociais a

extensão de redes de criminalidade, identificando os elementos que expandem estas redes e seu papel nestas relações criminosas.

6.2 Considerações Finais

Os resultados deste trabalho foram apresentados no *V Complex Net - Workshop and School on Dynamics, Transport and Control in Complex Networks*, que ocorreu no Instituto Nacional de Pesquisas Espaciais (INPE), de 26 de agosto a 1 de setembro de 2018.

Este trabalho também foi submetido ao *Dynamics Days Latin America and the Caribbean*¹ e será apresentado entre os dias 26 e 30 de novembro de 2018, em Punta del Este, Uruguai.

Levando-se em consideração os resultados apresentados, entende-se que é possível modelar relacionamentos criminosos, a partir de um banco de dados real, criando-se algoritmos e ferramentas que identificam as redes, seus relacionamentos e seus líderes, sua evolução, além de decompor a rede em camadas *multiplex*, para também identificar relacionamentos e líderes.

Este trabalho é pioneiro, até onde sabemos, ao utilizar o conceito de redes *multiplex* para identificação e análise de redes de criminalidade.

¹ <https://ddayslac2018.org>

Referências

- ADAMATZKY, A. Identification of cellular automata. In: _____. **Computational Complexity: Theory, Techniques, and Applications**. New York, NY: Springer New York, 2012. p. 1564–1575. ISBN 978-1-4614-1800-9. Disponível em: <https://doi.org/10.1007/978-1-4614-1800-9_100>. Citado 2 vezes nas páginas 21 e 22.
- AGRESTE, S. et al. Network structure and resilience of mafia syndicates. **Information Sciences**, Elsevier, v. 351, p. 30–47, 2016. Citado na página 53.
- ALBERT, R.; JEONG, H.; BARABÁSI, A.-L. Error and attack tolerance of complex networks. **nature**, Nature Publishing Group, v. 406, n. 6794, p. 378, 2000. Citado na página 60.
- ARENAS, A. et al. Community analysis in social networks. **The European Physical Journal B**, Springer, v. 38, n. 2, p. 373–380, 2004. Citado na página 53.
- ARRUDA, G. F. de et al. Disease localization in multilayer networks. **Physical Review X**, APS, v. 7, n. 1, p. 011014, 2017. Citado na página 72.
- ATMAN, A. **Aspectos Fractais em Sistemas Complexos**. Tese (Doutorado) — Ph. D. Thesis, UFMG, Belo Horizonte, 2002. Citado na página 21.
- BAGGIO, J. A. et al. Multiplex social ecological network analysis reveals how social changes affect community robustness more than resource depletion. **Proceedings of the National Academy of Sciences**, National Acad Sciences, v. 113, n. 48, p. 13708–13713, 2016. Citado na página 20.
- BAR-YAM, Y. **Dynamics of complex systems**. [S.l.]: Addison-Wesley, 1997. v. 213. Citado na página 22.
- BARABÁSI, A.-L. **Linked: The new science of networks**. [S.l.]: AAPT, 2003. Citado 2 vezes nas páginas 14 e 19.
- BARABÁSI, A.-L. Network science. **Phil. Trans. R. Soc. A**, The Royal Society, v. 371, n. 1987, p. 20120375, 2013. Citado na página 19.
- BARABÁSI, A.-L.; ALBERT, R. Emergence of scaling in random networks. **science**, American Association for the Advancement of Science, v. 286, n. 5439, p. 509–512, 1999. Citado na página 19.
- BARGIGLI, L. et al. The multiplex structure of interbank networks. **Quantitative Finance**, Taylor & Francis, v. 15, n. 4, p. 673–691, 2015. Citado 2 vezes nas páginas 19 e 20.
- BARRAT, A.; BARTHELEMY, M.; VESPIGNANI, A. **Dynamical processes on complex networks**. [S.l.]: Cambridge university press, 2008. Citado na página 53.
- BASHAN, A. et al. The extreme vulnerability of interdependent spatially embedded networks. **Nature Physics**, Nature Research, v. 9, n. 10, p. 667–672, 2013. Citado na página 20.
- BATTISTON, S. et al. The price of complexity in financial networks. **Proceedings of the National Academy of Sciences**, National Acad Sciences, v. 113, n. 36, p. 10031–10036, 2016. Citado na página 20.

- BAYLEY, D. H. **Padrões de Policiamento: Uma Análise Internacional Comparativa Vol. 1**. [S.l.]: Edusp, 2001. Citado 3 vezes nas páginas 9, 10 e 24.
- BAYLEY, D. H.; SKOLNICK, J. H. **Nova Polícia: Inovações na Polícia de Seis Cidades Norte-Americanas Vol. 2Nova**. [S.l.]: Edusp, 2006. Citado 3 vezes nas páginas 7, 8 e 9.
- BIANCONI, G. Statistical mechanics of multiplex networks: Entropy and overlap. **Physical Review E**, APS, v. 87, n. 6, p. 062806, 2013. Citado na página 20.
- BLONDEL, V. D. et al. Fast unfolding of communities in large networks. **Journal of statistical mechanics: theory and experiment**, IOP Publishing, v. 2008, n. 10, p. P10008, 2008. Citado 2 vezes nas páginas 52 e 53.
- BOCCALETTI, S. et al. The structure and dynamics of multilayer networks. **Physics Reports**, Elsevier, v. 544, n. 1, p. 1–122, 2014. Citado na página 19.
- BOCCARA, N. **Modeling complex systems**. [S.l.]: Springer Science & Business Media, 2010. Citado 2 vezes nas páginas 3 e 24.
- BOSSERT, W. et al. **The measurement of diversity**. [S.l.]: Centre de recherche et développement en économique, Université de Montréal, 2001. Citado 3 vezes nas páginas 75, 76 e 77.
- BOUCHARD, M.; AMIRAUT, J. Advances in research on illicit networks. **Global crime**, Taylor & Francis, v. 14, n. 2-3, p. 119–122, 2013. Citado na página 1.
- BRIGHT, D. A. et al. The use of actor-level attributes and centrality measures to identify key actors: a case study of an Australian drug trafficking network. **Journal of Contemporary Criminal Justice**, SAGE Publications Sage CA: Los Angeles, CA, v. 31, n. 3, p. 262–278, 2015. Citado na página 53.
- BRUINSMA, G.; BERNASCO, W. Criminal groups and transnational illegal markets. **Crime, Law and Social Change**, Springer, v. 41, n. 1, p. 79–94, 2004. Citado na página 1.
- CALDERONI, F.; MORSELLI, C. Inside criminal networks. **European Journal on Criminal Policy and Research**, Springer Science & Business Media, v. 16, n. 1, p. 69, 2010. Citado na página 25.
- CAMPANA, P. Explaining criminal networks: Strategies and potential pitfalls. **Methodological Innovations**, SAGE Publications Sage UK: London, England, v. 9, p. 2059799115622748, 2016. Citado na página 2.
- CANTINI, L. et al. Detection of gene communities in multi-networks reveals cancer drivers. **Scientific reports**, Nature Publishing Group, v. 5, p. srep17386, 2015. Citado 2 vezes nas páginas 19 e 20.
- CARDILLO, A. et al. Modeling the multi-layer nature of the European air transport network: Resilience and passengers re-scheduling under random failures. **The European Physical Journal Special Topics**, Springer, v. 215, n. 1, p. 23–33, 2013. Citado na página 20.
- CARLEY, K. M.; LEE, J.-S.; KRACKHARDT, D. Destabilizing networks. **Connections**, v. 24, n. 3, p. 79–92, 2002. Citado na página 53.

- CARPI, L. C. et al. Assessing diversity in multiplex networks. **arXiv preprint arXiv:1805.12350**, 2018. Citado 4 vezes nas páginas 75, 76, 77 e 78.
- CLAUSET, A.; NEWMAN, M. E.; MOORE, C. Finding community structure in very large networks. **Physical review E**, APS, v. 70, n. 6, p. 066111, 2004. Citado 2 vezes nas páginas 50 e 51.
- ÇOLAK, S.; LIMA, A.; GONZÁLEZ, M. C. Understanding congested travel in urban areas. **Nature communications**, Nature Publishing Group, v. 7, 2016. Citado na página 20.
- CRUCITTI, P.; LATORA, V.; MARCHIORI, M. Model for cascading failures in complex networks. **Physical Review E**, APS, v. 69, n. 4, p. 045104, 2004. Citado na página 19.
- DOMENICO, M. D.; SASAI, S.; ARENAS, A. Mapping multiplex hubs in human functional brain networks. **Frontiers in neuroscience**, Frontiers Media SA, v. 10, 2016. Citado 2 vezes nas páginas 19 e 20.
- DOMENICO, M. D. et al. Mathematical formulation of multilayer networks. **Physical Review X**, APS, v. 3, n. 4, p. 041022, 2013. Citado na página 20.
- DOMENICO, M. D. et al. Mathematical formulation of multilayer networks. **Physical Review X**, APS, v. 3, n. 4, p. 041022, 2013. Citado na página 72.
- DONGES, J. F. et al. Investigating the topology of interacting networks-theory and application to coupled climate subnetworks. **arXiv preprint arXiv:1102.3067**, 2011. Citado 2 vezes nas páginas 19 e 20.
- DUIJN, P. A.; KASHIRIN, V.; SLOOT, P. M. The relative ineffectiveness of criminal network disruption. **Scientific reports**, Nature Publishing Group, v. 4, p. 4238, 2014. Citado 10 vezes nas páginas 1, 26, 29, 30, 58, 59, 60, 61, 62 e 75.
- DUIJN, P. A.; KLERKS, P. P. Social network analysis applied to criminal networks: Recent developments in dutch law enforcement. In: **Networks and network analysis for defence and security**. [S.l.]: Springer, 2014. p. 121–159. Citado na página 1.
- EASLEY, D.; KLEINBERG, J. **Networks, crowds, and markets: Reasoning about a highly connected world**. [S.l.]: Cambridge University Press, 2010. Citado 3 vezes nas páginas 11, 17 e 18.
- EMMERT-STREIB, F.; DEHMER, M. Exploring statistical and population aspects of network complexity. **PLoS One**, Public Library of Science, v. 7, n. 5, p. e34523, 2012. Citado na página 75.
- FEITOZA, D. Direito processual penal. **Rio de Janeiro: Impetus**, 2010. Citado na página 10.
- FILHO, C. C. B. et al. Conglomerados de homicídios e o tráfico de drogas em belo horizonte, minas gerais, brasil, de 1995 a 1999 homicide clusters and drug traffic in belo horizonte, minas gerais state, brazil. **Cad. Saúde Pública**, v. 17, n. 5, p. 1163–1171, 2001. Citado na página 8.
- FLAKE, G. W. et al. Self-organization and identification of web communities. **Computer**, IEEE, v. 35, n. 3, p. 66–70, 2002. Citado na página 53.

- FORTUNA, M. A.; BONACHELA, J. A.; LEVIN, S. A. Evolution of a modular software network. **Proceedings of the National Academy of Sciences**, National Acad Sciences, v. 108, n. 50, p. 19985–19989, 2011. Citado na página 53.
- FU, Y.-H.; HUANG, C.-Y.; SUN, C.-T. Using global diversity and local topology features to identify influential network spreaders. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 433, p. 344–355, 2015. Citado na página 75.
- GALLOTTI, R.; PORTER, M. A.; BARTHELEMY, M. Lost in transportation: Information measures and cognitive limits in multilayer navigation. **Science advances**, American Association for the Advancement of Science, v. 2, n. 2, p. e1500445, 2016. Citado 2 vezes nas páginas 19 e 20.
- GAMA, J. et al. **Extração de conhecimento de dados: data mining**. [S.l.]: Edições Silabo, 2015. Citado na página 26.
- GAO, J.; BARZEL, B.; BARABÁSI, A.-L. Universal resilience patterns in complex networks. **Nature**, Nature Publishing Group, v. 530, n. 7590, p. 307, 2016. Citado na página 75.
- GAO, J. et al. Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes. **Physical Review E**, APS, v. 85, n. 6, p. 066134, 2012. Citado na página 19.
- GIRVAN, M.; NEWMAN, M. E. Community structure in social and biological networks. **Proceedings of the national academy of sciences**, National Acad Sciences, v. 99, n. 12, p. 7821–7826, 2002. Citado na página 53.
- GUO, Q. et al. Levy random walks on multiplex networks. **Scientific reports**, Nature Publishing Group, v. 6, 2016. Citado na página 20.
- IACOVACCI, J.; BIANCONI, G. Extracting information from multiplex networks. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP Publishing, v. 26, n. 6, p. 065306, 2016. Citado na página 20.
- JANZEN, D.; SAIEDIAN, H. Test-driven development concepts, taxonomy, and future direction. **Computer**, IEEE, v. 38, n. 9, p. 43–50, 2005. Citado na página 28.
- JONSSON, P. F. et al. Cluster analysis of networks generated through homology: automatic identification of important protein communities involved in cancer metastasis. **BMC bioinformatics**, BioMed Central, v. 7, n. 1, p. 2, 2006. Citado na página 53.
- KIVELÄ, M. et al. Multilayer networks. **Journal of complex networks**, Oxford University Press, v. 2, n. 3, p. 203–271, 2014. Citado na página 19.
- KLEINEBERG, K.-K. et al. Hidden geometric correlations in real multiplex networks. **Nature Physics**, Nature Research, v. 12, n. 11, p. 1076–1081, 2016. Citado na página 20.
- KLOTZ, J. G. et al. Properties of boolean networks and methods for their tests. **EURASIP Journal on Bioinformatics and Systems Biology**, Springer, v. 2013, n. 1, p. 1, 2013. Citado na página 25.
- KOWALTOWSKI, T. Von neumann: suas contribuições à computação. **Estudos Avançados**, SciELO Brasil, v. 10, n. 26, p. 237–260, 1996. Citado na página 21.

- KRAUSE, A. E. et al. Compartments revealed in food-web structure. **Nature**, Nature Publishing Group, v. 426, n. 6964, p. 282, 2003. Citado na página 53.
- KREBS, V. E. Mapping networks of terrorist cells. **Connections**, v. 24, n. 3, p. 43–52, 2002. Citado na página 1.
- KURANT, M.; THIRAN, P. Layered complex networks. **Physical review letters**, APS, v. 96, n. 13, p. 138701, 2006. Citado na página 19.
- LANDHERR, A.; FRIEDL, B.; HEIDEMANN, J. A critical review of centrality measures in social networks. **Business & Information Systems Engineering**, Springer, v. 2, n. 6, p. 371–385, 2010. Citado na página 26.
- LAZEGA, E.; HIGGINS, S. S. **Redes sociais e estruturas relacionais**. [S.l.]: Fino Traço Editora, 2014. Citado 3 vezes nas páginas 24, 35 e 44.
- LEINFELT, F.; ROSTAMI, A. The stockholm gang model—panther stockholm. **Sweden: Erlander AB, Stockholm**, 2012. Citado na página 25.
- MALM, A.; BICHLER, G. Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. **Journal of Research in Crime and Delinquency**, Sage Publications Sage CA: Los Angeles, CA, v. 48, n. 2, p. 271–297, 2011. Citado na página 53.
- MASYS, A. J. **Networks and network analysis for defence and security**. [S.l.]: Springer Science & Business Media, 2014. Citado 2 vezes nas páginas 25 e 53.
- MEIRELLES, A. O tempo e a violência. **Contagem: Editora O Tempo**, 2007. Citado na página 8.
- MENEZES, N. N. C. **Introdução à programação com Python: algoritmos e lógica de programação para iniciantes**. [S.l.]: Novatec, 2010. Citado na página 27.
- MIN, Y. et al. Diversity of multilayer networks and its impact on collaborating epidemics. **Physical Review E**, APS, v. 90, n. 6, p. 062803, 2014. Citado na página 75.
- MONET, J.-C. **Polícias e Sociedades na Europa Vol. 3**. [S.l.]: Edusp, 2001. Citado na página 7.
- MORSELLI, C. **Inside criminal networks**. [S.l.]: Springer, 2009. v. 8. Citado 9 vezes nas páginas 1, 3, 10, 11, 12, 13, 14, 53 e 81.
- MORSELLI, C.; GIGUÈRE, C.; PETIT, K. The efficiency/security trade-off in criminal networks. **Social Networks**, Elsevier, v. 29, n. 1, p. 143–153, 2007. Citado na página 53.
- MORSELLI, C.; ROY, J. Brokerage qualifications in ringing operations. **Criminology**, Wiley Online Library, v. 46, n. 1, p. 71–98, 2008. Citado na página 53.
- MOUGI, A.; KONDOH, M. Diversity of interaction types and ecological community stability. **Science**, American Association for the Advancement of Science, v. 337, n. 6092, p. 349–351, 2012. Citado na página 75.
- MOURA, D. d. P. **Evolução da sociedade disciplinar para sociedade de controle: uma análise com enfoque na inteligência**. 2017. Citado na página 9.

MUCHA, P. J. et al. Community structure in time-dependent, multiscale, and multiplex networks. **science**, American Association for the Advancement of Science, v. 328, n. 5980, p. 876–878, 2010. Citado na página 20.

NATARAJAN, M. Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. **Journal of Quantitative Criminology**, Springer, v. 22, n. 2, p. 171–192, 2006. Citado na página 1.

NEWMAN, M. **Networks: an introduction**. [S.l.]: Oxford university press, 2010. Citado 2 vezes nas páginas 19 e 53.

OATLEY, G. et al. The gang gun-crime problem-solutions from social network theory, epidemiology, cellular automata, bayesian networks and spatial statistics. **Computational Forensics**, 2008. Citado 2 vezes nas páginas 22 e 23.

PAPACHRISTOS, A. V. The coming of a networked criminology. **Advances in criminological theory**, Transaction New Brunswick, NJ, v. 17, p. 101–140, 2011. Citado na página 1.

PICCARDI, C.; CALATRONI, L.; BERTONI, F. Communities in italian corporate networks. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 389, n. 22, p. 5247–5258, 2010. Citado na página 53.

PODOLNY, J. M.; PAGE, K. L. Network forms of organization. **Annual review of sociology**, Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, v. 24, n. 1, p. 57–76, 1998. Citado na página 2.

RAAB, J.; MILWARD, H. B. Dark networks as problems. **Journal of public administration research and theory**, Oxford University Press, v. 13, n. 4, p. 413–439, 2003. Citado na página 1.

RADICCHI, F.; ARENAS, A. Abrupt transition in the structural formation of interconnected networks. **Nature Physics**, Nature Research, v. 9, n. 11, p. 717–720, 2013. Citado na página 20.

RADUCHA, T.; GUBIEC, T. Predicting language diversity with complex networks. **PloS one**, Public Library of Science, v. 13, n. 4, p. e0196593, 2018. Citado na página 75.

REQUEJO, R. J.; DÍAZ-GUILERA, A. Replicator dynamics with diffusion on multiplex networks. **Physical Review E**, APS, v. 94, n. 2, p. 022301, 2016. Citado na página 20.

RESSLER, S. Social network analysis as an approach to combat terrorism: Past, present, and future research. **Homeland Security Affairs**, Naval Postgraduate School, Center for Homeland Defense and Security, v. 2, n. 2, 2006. Citado na página 25.

ROSTAMI, A.; MONDANI, H. The complexity of crime network data: A case study of its consequences for crime control and the study of networks. **PloS one**, Public Library of Science, v. 10, n. 3, p. e0119309, 2015. Citado 2 vezes nas páginas 25 e 29.

SANTO, L. E. E.; MEIRELLES, A. Entendendo a nossa insegurança. **Belo Horizonte: Instituto Brasileiro de Policiologia**, 2003. Citado 2 vezes nas páginas 8 e 24.

SAYAMA, H. **Introduction to the modeling and analysis of complex systems**. [S.l.]: Open SUNY Textbooks, 2015. Citado 7 vezes nas páginas 25, 42, 43, 45, 46, 47 e 52.

- SCHIEBER, T. A. et al. Quantification of network structural dissimilarities. **Nature communications**, Nature Publishing Group, v. 8, p. 13928, 2017. Citado na página 76.
- SCOTT, J. **Social network analysis**. [S.l.]: Sage, 2017. Citado 6 vezes nas páginas 25, 42, 43, 45, 46 e 47.
- SLOOT, P. M.; KAMPIS, G.; GULYÁS, L. **Advances in dynamic temporal networks: Understanding the temporal dynamics of complex adaptive networks**. [S.l.]: Springer, 2013. Citado na página 1.
- SMITH, C. M.; PAPACHRISTOS, A. V. Trust thy crooked neighbor: multiplexity in chicago organized crime networks. **American Sociological Review**, SAGE Publications Sage CA: Los Angeles, CA, v. 81, n. 4, p. 644–667, 2016. Citado 3 vezes nas páginas 26, 29 e 32.
- SPAPENS, T. Macro networks, collectives, and business processes: An integrated approach to organized crime. **Eur. J. Crime Crim. L. & Crim. Just.**, HeinOnline, v. 18, p. 185, 2010. Citado na página 1.
- SPAPENS, T. Interaction between criminal groups and law enforcement: the case of ecstasy in the netherlands. **Global crime**, Taylor & Francis, v. 12, n. 1, p. 19–40, 2011. Citado na página 1.
- SPARROW, M. K. The application of network analysis to criminal intelligence: An assessment of the prospects. **Social networks**, North-Holland, v. 13, n. 3, p. 251–274, 1991. Citado na página 1.
- STIRLING, A. A general framework for analysing diversity in science, technology and society. **Journal of the Royal Society Interface**, The Royal Society, v. 4, n. 15, p. 707–719, 2007. Citado na página 75.
- TICHY, N. M.; TUSHMAN, M. L.; FOMBRUN, C. Social network analysis for organizations. **Academy of management review**, Academy of Management, v. 4, n. 4, p. 507–519, 1979. Citado na página 25.
- VARESE, F. The structure of a criminal network examined: the russian mafia in rome. 2006. Citado na página 53.
- VARESE, F. The structure and the content of criminal connections: The russian mafia in italy. **European sociological review**, Oxford University Press, v. 29, n. 5, p. 899–909, 2012. Citado na página 1.
- WAL, A. L. T.; BOSCHMA, R. A. Applying social network analysis in economic geography: framing some key analytic issues. **The Annals of Regional Science**, Springer, v. 43, n. 3, p. 739–756, 2009. Citado na página 25.
- WANG, W. et al. Structural diversity effects of multilayer networks on the threshold of interacting epidemics. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 443, p. 254–262, 2016. Citado na página 75.
- WASSERMAN, S.; FAUST, K. **Social network analysis: Methods and applications**. [S.l.]: Cambridge university press, 1994. v. 8. Citado na página 25.
- WATTS, D. J.; STROGATZ, S. H. Collective dynamics of ‘small-world’ networks. **nature**, Nature Publishing Group, v. 393, n. 6684, p. 440–442, 1998. Citado na página 19.

WEITZMAN, M. L. The quarterly journal of economics. **On diversity**, v. 107, p. 363–405, 1992. Citado 2 vezes nas páginas 75 e 76.

ZIVIANI, N. **Projeto de algoritmos: com implementações em Java e C++**. [S.l.]: THOMSON PIONEIRA, 2007. ISBN 9788522105250. Citado 3 vezes nas páginas 14, 15 e 19.

Apêndices

APÊNDICE A – Medidas de Centralidade para Análise de Redes Sociais

Degree			Betweenness			Closeness			Eigenvector			PageRank		
Class	ID	Medida	Class	ID	Medida	Class	ID	Medida	Class	ID	Medida	Class	ID	Medida
1	80	0,296703	1	80	0,902686	1	80	0,517045	1	80	0,633999	1	80	0,100143
2	51	0,142857	2	51	0,352829	2	51	0,395652	2	48	0,216597	2	51	0,050605
3	48	0,120879	3	48	0,225397	3	48	0,374486	3	51	0,200602	3	48	0,039900
4	47	0,087912	4	11	0,201709	4	11	0,369919	4	2	0,164851	4	47	0,028761
5	19	0,065934	5	81	0,106716	5	2	0,359684	5	19	0,163590	5	81	0,021976
6	11	0,065934	6	44	0,095604	6	54	0,358268	6	11	0,160695	6	19	0,021053
7	2	0,054945	7	47	0,086447	7	25	0,356863	7	25	0,160416	7	11	0,020091
8	81	0,054945	8	19	0,085714	8	81	0,356863	8	81	0,148981	8	2	0,019307
9	33	0,054945	9	2	0,084982	9	44	0,355469	9	54	0,148907	9	46	0,017994
10	46	0,054945	10	90	0,064469	10	19	0,354086	10	21	0,145712	10	33	0,017820
11	25	0,043956	11	26	0,043712	11	90	0,350000	11	16	0,139628	11	44	0,016231
12	39	0,043956	12	21	0,043468	12	76	0,350000	12	76	0,137071	12	26	0,015699
13	13	0,043956	13	25	0,041514	13	16	0,348659	13	56	0,136498	13	21	0,015492
14	17	0,043956	14	67	0,032723	14	21	0,348659	14	44	0,126940	14	25	0,015174
15	21	0,043956	15	77	0,032275	15	56	0,346008	15	90	0,120676	15	13	0,014271
16	31	0,043956	16	53	0,028856	16	22	0,344697	16	22	0,118512	16	67	0,013766
17	44	0,043956	17	46	0,022222	17	3	0,342105	17	3	0,110990	17	39	0,013100
18	23	0,032967	18	23	0,021978	18	57	0,342105	18	57	0,110990	18	17	0,013100
19	4	0,032967	19	36	0,021978	19	62	0,342105	19	62	0,110990	19	31	0,013100
20	90	0,032967	20	28	0,021978	20	70	0,342105	20	70	0,110990	20	77	0,013003
21	77	0,032967	21	40	0,021978	21	74	0,342105	21	74	0,110990	21	23	0,012543
22	10	0,032967	22	60	0,021978	22	78	0,342105	22	78	0,110990	22	86	0,012543
23	12	0,032967	23	83	0,021978	23	7	0,342105	23	7	0,110990	23	53	0,012527
24	55	0,032967	24	86	0,021978	24	37	0,342105	24	37	0,110990	24	4	0,011668
25	26	0,032967	25	33	0,018315	25	52	0,342105	25	52	0,110990	25	49	0,011668
26	27	0,032967	26	4	0,010867	26	66	0,342105	26	66	0,110990	26	90	0,011395
27	35	0,032967	27	49	0,010867	27	87	0,342105	27	87	0,110990	27	43	0,011242
28	91	0,032967	28	73	0,010745	28	88	0,342105	28	88	0,110990	28	27	0,011114
29	67	0,032967	29	22	0,010379	29	33	0,289809	29	46	0,071872	29	68	0,011001
30	43	0,032967	30	13	0,007000	30	13	0,288889	30	47	0,069130	30	12	0,010846
31	53	0,032967	31	43	0,000651	31	77	0,287975	31	33	0,064185	31	55	0,010846
32	49	0,032967	32	1	0,000611	32	53	0,287975	32	39	0,061917	32	91	0,010645
33	68	0,032967	33	79	0,000366	33	68	0,287975	33	17	0,061917	33	10	0,010645
34	86	0,032967	34	27	0,000244	34	28	0,286164	34	31	0,061917	34	35	0,010645
35	36	0,021978	35	42	0,000244	35	40	0,286164	35	13	0,061480	35	28	0,009902
36	15	0,021978	36	3	0,000000	36	30	0,284375	36	12	0,061216	36	40	0,009902
37	16	0,021978	37	15	0,000000	37	32	0,284375	37	55	0,061216	37	36	0,009860
38	18	0,021978	38	5	0,000000	38	8	0,284375	38	27	0,058944	38	83	0,009549
39	72	0,021978	39	9	0,000000	39	84	0,284375	39	23	0,058742	39	42	0,009389
40	22	0,021978	40	10	0,000000	40	58	0,284375	40	86	0,058742	40	60	0,009178
41	1	0,021978	41	39	0,000000	41	47	0,280000	41	68	0,057120	41	73	0,009065
42	59	0,021978	42	12	0,000000	42	46	0,277439	42	59	0,048236	42	1	0,008678
43	28	0,021978	43	55	0,000000	43	39	0,276596	43	10	0,044067	43	72	0,008561
44	40	0,021978	44	16	0,000000	44	17	0,276596	44	35	0,044067	44	18	0,008561
45	42	0,021978	45	17	0,000000	45	31	0,276596	45	91	0,044067	45	76	0,008519
46	73	0,021978	46	18	0,000000	46	12	0,275758	46	1	0,042969	46	22	0,008473

Degree			Betweenness			Closeness			Eigenvector			PageRank		
Class	ID	Medida	Class	ID	Medida	Class	ID	Medida	Class	ID	Medida	Class	ID	Medida
47	54	0,021978	47	72	0,000000	47	55	0,275758	47	53	0,041516	47	79	0,008344
48	56	0,021978	48	20	0,000000	48	27	0,275758	48	77	0,039508	48	15	0,008242
49	60	0,021978	49	24	0,000000	49	83	0,274924	49	83	0,039116	49	56	0,008076
50	76	0,021978	50	14	0,000000	50	59	0,274096	50	64	0,037918	50	54	0,007867
51	79	0,021978	51	50	0,000000	51	64	0,273273	51	69	0,037918	51	59	0,007863
52	83	0,021978	52	59	0,000000	52	69	0,273273	52	89	0,037918	52	16	0,007766
53	3	0,010989	53	29	0,000000	53	89	0,273273	53	28	0,036229	53	14	0,006079
54	5	0,010989	54	30	0,000000	54	60	0,272455	54	40	0,036229	54	50	0,006079
55	9	0,010989	55	31	0,000000	55	23	0,267647	55	30	0,035119	55	29	0,005839
56	20	0,010989	56	32	0,000000	56	86	0,267647	56	32	0,035119	56	71	0,005839
57	24	0,010989	57	34	0,000000	57	36	0,266862	57	8	0,035119	57	38	0,005821
58	14	0,010989	58	35	0,000000	58	26	0,266862	58	84	0,035119	58	41	0,005689
59	50	0,010989	59	91	0,000000	59	67	0,266082	59	58	0,035119	59	63	0,005533
60	29	0,010989	60	38	0,000000	60	1	0,264535	60	72	0,030922	60	82	0,005531
61	30	0,010989	61	71	0,000000	61	73	0,264535	61	18	0,030922	61	34	0,005366
62	32	0,010989	62	45	0,000000	62	10	0,263768	62	36	0,029772	62	92	0,005366
63	34	0,010989	63	6	0,000000	63	34	0,263768	63	43	0,029269	63	9	0,005315
64	38	0,010989	64	54	0,000000	64	35	0,263768	64	60	0,029022	64	65	0,005185
65	71	0,010989	65	8	0,000000	65	91	0,263768	65	24	0,028638	65	75	0,005185
66	45	0,010989	66	84	0,000000	66	92	0,263768	66	26	0,027784	66	85	0,005180
67	6	0,010989	67	92	0,000000	67	4	0,262248	67	4	0,027664	67	30	0,004939
68	8	0,010989	68	85	0,000000	68	24	0,262248	68	49	0,027664	68	32	0,004939
69	84	0,010989	69	56	0,000000	69	49	0,262248	69	34	0,026081	69	8	0,004939
70	92	0,010989	70	57	0,000000	70	18	0,260000	70	92	0,026081	70	84	0,004939
71	85	0,010989	71	58	0,000000	71	72	0,260000	71	67	0,024447	71	58	0,004939
72	57	0,010989	72	82	0,000000	72	43	0,228070	72	73	0,023698	72	3	0,004783
73	58	0,010989	73	61	0,000000	73	79	0,227500	73	79	0,018154	73	57	0,004783
74	82	0,010989	74	62	0,000000	74	9	0,224138	74	6	0,012582	74	62	0,004783
75	61	0,010989	75	63	0,000000	75	85	0,224138	75	5	0,012103	75	70	0,004783
76	62	0,010989	76	64	0,000000	76	29	0,223039	76	20	0,012103	76	74	0,004783
77	63	0,010989	77	65	0,000000	77	71	0,223039	77	45	0,012103	77	78	0,004783
78	64	0,010989	78	68	0,000000	78	5	0,219277	78	61	0,012103	78	7	0,004783
79	65	0,010989	79	69	0,000000	79	20	0,219277	79	65	0,010284	79	37	0,004783
80	69	0,010989	80	70	0,000000	80	45	0,219277	80	75	0,010284	80	52	0,004783
81	70	0,010989	81	74	0,000000	81	61	0,219277	81	15	0,009686	81	66	0,004783
82	74	0,010989	82	76	0,000000	82	6	0,217703	82	42	0,008428	82	87	0,004783
83	78	0,010989	83	78	0,000000	83	41	0,216152	83	85	0,007268	83	88	0,004783
84	7	0,010989	84	7	0,000000	84	82	0,214623	84	9	0,006917	84	64	0,004714
85	37	0,010989	85	37	0,000000	85	42	0,211628	85	41	0,006848	85	69	0,004714
86	52	0,010989	86	52	0,000000	86	65	0,211628	86	29	0,006343	86	89	0,004714
87	66	0,010989	87	66	0,000000	87	75	0,211628	87	71	0,006343	87	6	0,004689
88	87	0,010989	88	87	0,000000	88	14	0,211137	88	38	0,005212	88	5	0,004686
89	88	0,010989	89	88	0,000000	89	50	0,211137	89	82	0,005081	89	20	0,004686
90	41	0,010989	90	41	0,000000	90	38	0,211137	90	14	0,004864	90	45	0,004686
91	75	0,010989	91	75	0,000000	91	63	0,210648	91	50	0,004864	91	61	0,004686
92	89	0,010989	92	89	0,000000	92	15	0,208716	92	63	0,004280	92	24	0,004613

APÊNDICE B – Medidas de Centralidade da Rede de Inteligência

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
1	80	0,296703	1	80	0,902686	1	80	0,100143	1	80	0,433177
2	51	0,142857	2	51	0,352829	2	51	0,050605	2	51	0,182097
3	48	0,120879	3	48	0,225397	3	48	0,039900	3	48	0,128725
4	47	0,087912	4	11	0,201709	4	47	0,028761	4	11	0,095912
5	11	0,065934	5	81	0,106716	5	81	0,021976	5	47	0,067707
6	19	0,065934	6	44	0,095604	6	19	0,021053	6	81	0,061212
7	2	0,054945	7	47	0,086447	7	11	0,020091	7	19	0,057567
8	33	0,054945	8	19	0,085714	8	2	0,019307	8	2	0,053078
9	46	0,054945	9	2	0,084982	9	46	0,017994	9	44	0,051931
10	81	0,054945	10	90	0,064469	10	33	0,017820	10	90	0,036277
11	13	0,043956	11	26	0,043712	11	44	0,016231	11	21	0,034305
12	17	0,043956	12	21	0,043468	12	26	0,015699	12	25	0,033548
13	21	0,043956	13	25	0,041514	13	21	0,015492	13	46	0,031721
14	25	0,043956	14	67	0,032723	14	25	0,015174	14	26	0,030793
15	31	0,043956	15	77	0,032275	15	13	0,014271	15	33	0,030360
16	39	0,043956	16	53	0,028856	16	67	0,013766	16	67	0,026485
17	44	0,043956	17	46	0,022222	17	17	0,013100	17	77	0,026082
18	4	0,032967	18	23	0,021978	18	31	0,013100	18	53	0,024783
19	10	0,032967	19	28	0,021978	19	39	0,013100	19	23	0,022496
20	12	0,032967	20	36	0,021978	20	77	0,013003	20	86	0,022496
21	23	0,032967	21	40	0,021978	21	23	0,012543	21	13	0,021742
22	26	0,032967	22	60	0,021978	22	86	0,012543	22	17	0,019019
23	27	0,032967	23	83	0,021978	23	53	0,012527	23	31	0,019019
24	35	0,032967	24	86	0,021978	24	4	0,011668	24	39	0,019019
25	43	0,032967	25	33	0,018315	25	49	0,011668	25	4	0,018501
26	49	0,032967	26	4	0,010867	26	90	0,011395	26	49	0,018501
27	53	0,032967	27	49	0,010867	27	43	0,011242	27	28	0,017953
28	55	0,032967	28	73	0,010745	28	27	0,011114	28	40	0,017953
29	67	0,032967	29	22	0,010379	29	68	0,011001	29	36	0,017939
30	68	0,032967	30	13	0,007000	30	12	0,010846	30	83	0,017835
31	77	0,032967	31	43	0,000651	31	55	0,010846	31	60	0,017711
32	86	0,032967	32	1	0,000611	32	10	0,010645	32	43	0,014953
33	90	0,032967	33	79	0,000366	33	35	0,010645	33	27	0,014775
34	91	0,032967	34	27	0,000244	34	91	0,010645	34	68	0,014656
35	1	0,021978	35	42	0,000244	35	28	0,009902	35	12	0,014604
36	15	0,021978	36	3	0,000000	36	40	0,009902	36	55	0,014604
37	16	0,021978	37	5	0,000000	37	36	0,009860	37	10	0,014537
38	18	0,021978	38	6	0,000000	38	83	0,009549	38	35	0,014537
39	22	0,021978	39	7	0,000000	39	42	0,009389	39	91	0,014537
40	28	0,021978	40	8	0,000000	40	60	0,009178	40	73	0,013929
41	36	0,021978	41	9	0,000000	41	73	0,009065	41	22	0,013610
42	40	0,021978	42	10	0,000000	42	1	0,008678	42	42	0,010537
43	42	0,021978	43	12	0,000000	43	72	0,008561	43	1	0,010422
44	54	0,021978	44	14	0,000000	44	18	0,008561	44	79	0,010229
45	56	0,021978	45	15	0,000000	45	76	0,008519	45	72	0,010180
46	59	0,021978	46	16	0,000000	46	22	0,008473	46	18	0,010180

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
47	60	0,021978	47	17	0,000000	47	79	0,008344	47	76	0,010166
48	72	0,021978	48	18	0,000000	48	15	0,008242	48	15	0,010073
49	73	0,021978	49	20	0,000000	49	56	0,008076	49	56	0,010018
50	76	0,021978	50	24	0,000000	50	54	0,007867	50	54	0,009948
51	79	0,021978	51	29	0,000000	51	59	0,007863	51	59	0,009947
52	83	0,021978	52	30	0,000000	52	16	0,007766	52	16	0,009915
53	3	0,010989	53	31	0,000000	53	14	0,006079	53	14	0,005689
54	5	0,010989	54	32	0,000000	54	50	0,006079	54	50	0,005689
55	6	0,010989	55	34	0,000000	55	29	0,005839	55	29	0,005609
56	7	0,010989	56	35	0,000000	56	71	0,005839	56	71	0,005609
57	8	0,010989	57	37	0,000000	57	38	0,005821	57	38	0,005603
58	9	0,010989	58	38	0,000000	58	41	0,005689	58	41	0,005559
59	14	0,010989	59	39	0,000000	59	63	0,005533	59	63	0,005507
60	20	0,010989	60	41	0,000000	60	82	0,005531	60	82	0,005507
61	24	0,010989	61	45	0,000000	61	34	0,005366	61	34	0,005452
62	29	0,010989	62	50	0,000000	62	92	0,005366	62	92	0,005452
63	30	0,010989	63	52	0,000000	63	9	0,005315	63	9	0,005435
64	32	0,010989	64	54	0,000000	64	65	0,005185	64	65	0,005391
65	34	0,010989	65	55	0,000000	65	75	0,005185	65	75	0,005391
66	37	0,010989	66	56	0,000000	66	85	0,005180	66	85	0,005390
67	38	0,010989	67	57	0,000000	67	8	0,004939	67	8	0,005309
68	41	0,010989	68	58	0,000000	68	30	0,004939	68	30	0,005309
69	45	0,010989	69	59	0,000000	69	32	0,004939	69	32	0,005309
70	50	0,010989	70	61	0,000000	70	58	0,004939	70	58	0,005309
71	52	0,010989	71	62	0,000000	71	84	0,004939	71	84	0,005309
72	57	0,010989	72	63	0,000000	72	3	0,004783	72	3	0,005257
73	58	0,010989	73	64	0,000000	73	7	0,004783	73	7	0,005257
74	61	0,010989	74	65	0,000000	74	37	0,004783	74	37	0,005257
75	62	0,010989	75	66	0,000000	75	52	0,004783	75	52	0,005257
76	63	0,010989	76	68	0,000000	76	57	0,004783	76	57	0,005257
77	64	0,010989	77	69	0,000000	77	62	0,004783	77	62	0,005257
78	65	0,010989	78	70	0,000000	78	66	0,004783	78	66	0,005257
79	66	0,010989	79	71	0,000000	79	70	0,004783	79	70	0,005257
80	69	0,010989	80	72	0,000000	80	74	0,004783	80	74	0,005257
81	70	0,010989	81	74	0,000000	81	78	0,004783	81	78	0,005257
82	71	0,010989	82	75	0,000000	82	87	0,004783	82	87	0,005257
83	74	0,010989	83	76	0,000000	83	88	0,004783	83	88	0,005257
84	75	0,010989	84	78	0,000000	84	64	0,004714	84	64	0,005234
85	78	0,010989	85	82	0,000000	85	69	0,004714	85	69	0,005234
86	82	0,010989	86	84	0,000000	86	89	0,004714	86	89	0,005234
87	84	0,010989	87	85	0,000000	87	6	0,004689	87	6	0,005226
88	85	0,010989	88	87	0,000000	88	5	0,004686	88	5	0,005225
89	87	0,010989	89	88	0,000000	89	20	0,004686	89	20	0,005225
90	88	0,010989	90	89	0,000000	90	45	0,004686	90	45	0,005225
91	89	0,010989	91	91	0,000000	91	61	0,004686	91	61	0,005225
92	92	0,010989	92	92	0,000000	92	24	0,004613	92	24	0,005201

APÊNDICE C – Medidas de Centralidade da sub-Rede de Autores

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
1	80	0,291139	1	80	0,898247	1	80	0,102509	1	80	0,430632
2	51	0,151899	2	51	0,360273	2	51	0,055153	2	51	0,189108
3	48	0,126582	3	48	0,236287	3	48	0,045715	3	48	0,136195
4	47	0,101266	4	11	0,229146	4	47	0,033226	4	11	0,109488
5	11	0,075949	5	44	0,109542	5	11	0,023367	5	47	0,077937
6	33	0,063291	6	47	0,099318	6	81	0,022438	6	44	0,059718
7	13	0,050633	7	81	0,098994	7	33	0,021535	7	81	0,057355
8	17	0,050633	8	2	0,098669	8	44	0,018977	8	2	0,051049
9	19	0,050633	9	90	0,074002	9	46	0,018284	9	90	0,041776
10	21	0,050633	10	19	0,049984	10	19	0,018206	10	19	0,039607
11	31	0,050633	11	21	0,049984	11	21	0,018206	11	21	0,039607
12	39	0,050633	12	67	0,037650	12	13	0,016899	12	33	0,039401
13	44	0,050633	13	33	0,033377	13	2	0,016503	13	46	0,031411
14	46	0,050633	14	53	0,033214	14	67	0,015966	14	67	0,030530
15	81	0,050633	15	25	0,025316	15	17	0,015157	15	53	0,028621
16	2	0,037975	16	26	0,025316	16	31	0,015157	16	13	0,025197
17	4	0,037975	17	28	0,025316	17	39	0,015157	17	17	0,021930
18	12	0,037975	18	36	0,025316	18	53	0,014673	18	31	0,021930
19	43	0,037975	19	40	0,025316	19	4	0,013564	19	39	0,021930
20	49	0,037975	20	46	0,025316	20	49	0,013564	20	4	0,021345
21	53	0,037975	21	60	0,025316	21	12	0,013460	21	49	0,021345
22	55	0,037975	22	83	0,025316	22	55	0,013460	22	26	0,021176
23	67	0,037975	23	4	0,012496	23	90	0,013350	23	25	0,021127
24	68	0,037975	24	49	0,012496	24	43	0,013285	24	36	0,021127
25	90	0,037975	25	73	0,012334	25	68	0,013034	25	28	0,020726
26	1	0,025316	26	22	0,011847	26	26	0,012894	26	40	0,020726
27	10	0,025316	27	13	0,008060	27	25	0,012749	27	83	0,020716
28	15	0,025316	28	43	0,000974	28	36	0,012749	28	60	0,020415
29	16	0,025316	29	1	0,000811	29	28	0,011546	29	43	0,017411
30	18	0,025316	30	42	0,000325	30	40	0,011546	30	12	0,017145
31	22	0,025316	31	3	0,000000	31	83	0,011514	31	55	0,017145
32	25	0,025316	32	5	0,000000	32	42	0,010876	32	68	0,017003
33	26	0,025316	33	6	0,000000	33	60	0,010613	33	73	0,016059
34	28	0,025316	34	7	0,000000	34	73	0,010527	34	22	0,015713
35	35	0,025316	35	8	0,000000	35	1	0,010146	35	42	0,012172
36	36	0,025316	36	10	0,000000	36	10	0,009989	36	1	0,012091
37	40	0,025316	37	12	0,000000	37	18	0,009989	37	10	0,011768
38	42	0,025316	38	14	0,000000	38	35	0,009989	38	18	0,011768
39	54	0,025316	39	15	0,000000	39	72	0,009989	39	35	0,011768
40	56	0,025316	40	16	0,000000	40	22	0,009977	40	72	0,011768

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
41	60	0,025316	41	17	0,000000	41	15	0,009562	41	15	0,011626
42	72	0,025316	42	18	0,000000	42	54	0,009549	42	54	0,011622
43	73	0,025316	43	20	0,000000	43	16	0,009532	43	16	0,011616
44	83	0,025316	44	29	0,000000	44	56	0,009532	44	56	0,011616
45	3	0,012658	45	30	0,000000	45	14	0,007356	45	14	0,006671
46	5	0,012658	46	31	0,000000	46	38	0,007295	46	38	0,006651
47	6	0,012658	47	32	0,000000	47	86	0,007295	47	86	0,006651
48	7	0,012658	48	34	0,000000	48	29	0,006782	48	29	0,006480
49	8	0,012658	49	35	0,000000	49	71	0,006782	49	71	0,006480
50	14	0,012658	50	37	0,000000	50	41	0,006768	50	41	0,006476
51	20	0,012658	51	38	0,000000	51	34	0,006642	51	34	0,006434
52	29	0,012658	52	39	0,000000	52	92	0,006642	52	92	0,006434
53	30	0,012658	53	41	0,000000	53	63	0,006400	53	63	0,006353
54	32	0,012658	54	45	0,000000	54	82	0,006386	54	82	0,006348
55	34	0,012658	55	52	0,000000	55	85	0,006032	55	85	0,006230
56	37	0,012658	56	54	0,000000	56	8	0,005782	56	8	0,006147
57	38	0,012658	57	55	0,000000	57	30	0,005782	57	30	0,006147
58	41	0,012658	58	56	0,000000	58	32	0,005782	58	32	0,006147
59	45	0,012658	59	58	0,000000	59	58	0,005782	59	58	0,006147
60	52	0,012658	60	59	0,000000	60	84	0,005782	60	84	0,006147
61	58	0,012658	61	61	0,000000	61	59	0,005761	61	59	0,006140
62	59	0,012658	62	62	0,000000	62	64	0,005761	62	64	0,006140
63	61	0,012658	63	63	0,000000	63	69	0,005761	63	69	0,006140
64	62	0,012658	64	64	0,000000	64	89	0,005761	64	89	0,006140
65	63	0,012658	65	68	0,000000	65	6	0,005760	65	6	0,006140
66	64	0,012658	66	69	0,000000	66	3	0,005664	66	3	0,006107
67	69	0,012658	67	70	0,000000	67	7	0,005664	67	7	0,006107
68	70	0,012658	68	71	0,000000	68	37	0,005664	68	37	0,006107
69	71	0,012658	69	72	0,000000	69	52	0,005664	69	52	0,006107
70	74	0,012658	70	74	0,000000	70	62	0,005664	70	62	0,006107
71	78	0,012658	71	78	0,000000	71	70	0,005664	71	70	0,006107
72	79	0,012658	72	79	0,000000	72	74	0,005664	72	74	0,006107
73	82	0,012658	73	82	0,000000	73	78	0,005664	73	78	0,006107
74	84	0,012658	74	84	0,000000	74	87	0,005664	74	87	0,006107
75	85	0,012658	75	85	0,000000	75	88	0,005664	75	88	0,006107
76	86	0,012658	76	86	0,000000	76	79	0,005536	76	79	0,006065
77	87	0,012658	77	87	0,000000	77	5	0,005405	77	5	0,006021
78	88	0,012658	78	88	0,000000	78	20	0,005405	78	20	0,006021
79	89	0,012658	79	89	0,000000	79	45	0,005405	79	45	0,006021
80	92	0,012658	80	92	0,000000	80	61	0,005405	80	61	0,006021

APÊNDICE D – Medidas de Centralidade da sub-Rede de Condenados

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
1	80	0,272727	1	80	0,759907	1	80	0,100094	1	80	0,377576
2	51	0,181818	2	51	0,393007	2	51	0,067509	2	51	0,214111
3	48	0,151515	3	48	0,260140	3	48	0,055209	3	48	0,155621
4	47	0,090909	4	11	0,206993	4	47	0,039644	4	11	0,097304
5	11	0,060606	5	47	0,110956	5	81	0,027201	5	47	0,080503
6	21	0,060606	6	81	0,110490	6	11	0,024312	6	81	0,066099
7	33	0,060606	7	21	0,055944	7	21	0,022224	7	21	0,046258
8	46	0,060606	8	90	0,055944	8	46	0,021977	8	90	0,039693
9	81	0,060606	9	77	0,041725	9	33	0,021232	9	46	0,037007
10	12	0,045455	10	19	0,028438	10	42	0,019377	10	77	0,035214
11	13	0,045455	11	25	0,028438	11	67	0,019377	11	33	0,032019
12	19	0,045455	12	26	0,028438	12	19	0,018519	12	19	0,030804
13	55	0,045455	13	28	0,028438	13	77	0,018462	13	26	0,024758
14	68	0,045455	14	40	0,028438	14	90	0,017681	14	60	0,024437
15	77	0,045455	15	46	0,028438	15	12	0,016188	15	28	0,024237
16	90	0,045455	16	53	0,028438	16	55	0,016188	16	40	0,024237
17	4	0,030303	17	60	0,028438	17	13	0,016092	17	53	0,024237
18	16	0,030303	18	83	0,028438	18	68	0,016092	18	25	0,024209
19	17	0,030303	19	33	0,014219	19	26	0,015532	19	83	0,024191
20	18	0,030303	20	42	0,000932	20	60	0,014571	20	12	0,020548
21	25	0,030303	21	67	0,000932	21	28	0,013971	21	55	0,020548
22	26	0,030303	22	79	0,000466	22	40	0,013971	22	13	0,020515
23	28	0,030303	23	3	0,000000	23	53	0,013971	23	68	0,020515
24	40	0,030303	24	4	0,000000	24	25	0,013885	24	42	0,016871
25	42	0,030303	25	5	0,000000	25	83	0,013831	25	67	0,016871
26	49	0,030303	26	6	0,000000	26	17	0,013022	26	17	0,014442
27	53	0,030303	27	7	0,000000	27	4	0,012606	27	4	0,014303
28	54	0,030303	28	8	0,000000	28	49	0,012606	28	49	0,014303
29	56	0,030303	29	9	0,000000	29	16	0,012213	29	79	0,014250
30	60	0,030303	30	12	0,000000	30	18	0,012107	30	16	0,014172
31	67	0,030303	31	13	0,000000	31	72	0,012107	31	18	0,014137
32	72	0,030303	32	14	0,000000	32	79	0,011981	32	72	0,014137
33	79	0,030303	33	16	0,000000	33	56	0,011688	33	56	0,013997
34	83	0,030303	34	17	0,000000	34	54	0,011659	34	54	0,013987

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
35	3	0,015152	35	18	0,000000	35	63	0,010474	35	63	0,008542
36	5	0,015152	36	20	0,000000	36	73	0,010474	36	73	0,008542
37	6	0,015152	37	29	0,000000	37	14	0,008841	37	14	0,007998
38	7	0,015152	38	30	0,000000	38	82	0,008433	38	82	0,007861
39	8	0,015152	39	32	0,000000	39	29	0,008176	39	29	0,007776
40	9	0,015152	40	34	0,000000	40	71	0,008176	40	71	0,007776
41	14	0,015152	41	35	0,000000	41	85	0,008176	41	85	0,007776
42	20	0,015152	42	37	0,000000	42	86	0,008139	42	86	0,007764
43	29	0,015152	43	41	0,000000	43	41	0,008117	43	41	0,007756
44	30	0,015152	44	45	0,000000	44	34	0,008018	44	34	0,007723
45	32	0,015152	45	49	0,000000	45	92	0,008018	45	92	0,007723
46	34	0,015152	46	52	0,000000	46	5	0,007857	46	5	0,007669
47	35	0,015152	47	54	0,000000	47	20	0,007857	47	20	0,007669
48	37	0,015152	48	55	0,000000	48	45	0,007857	48	45	0,007669
49	41	0,015152	49	56	0,000000	49	61	0,007857	49	61	0,007669
50	45	0,015152	50	58	0,000000	50	35	0,007486	50	35	0,007546
51	52	0,015152	51	59	0,000000	51	9	0,007470	51	9	0,007540
52	58	0,015152	52	61	0,000000	52	8	0,007021	52	8	0,007391
53	59	0,015152	53	63	0,000000	53	30	0,007021	53	30	0,007391
54	61	0,015152	54	64	0,000000	54	32	0,007021	54	32	0,007391
55	63	0,015152	55	68	0,000000	55	58	0,007021	55	58	0,007391
56	64	0,015152	56	69	0,000000	56	3	0,006966	56	3	0,007372
57	69	0,015152	57	71	0,000000	57	7	0,006966	57	7	0,007372
58	71	0,015152	58	72	0,000000	58	37	0,006966	58	37	0,007372
59	73	0,015152	59	73	0,000000	59	52	0,006966	59	52	0,007372
60	74	0,015152	60	74	0,000000	60	74	0,006966	60	74	0,007372
61	82	0,015152	61	82	0,000000	61	87	0,006966	61	87	0,007372
62	85	0,015152	62	85	0,000000	62	88	0,006966	62	88	0,007372
63	86	0,015152	63	86	0,000000	63	59	0,006932	63	59	0,007361
64	87	0,015152	64	87	0,000000	64	64	0,006932	64	64	0,007361
65	88	0,015152	65	88	0,000000	65	69	0,006932	65	69	0,007361
66	89	0,015152	66	89	0,000000	66	89	0,006932	66	89	0,007361
67	92	0,015152	67	92	0,000000	67	6	0,006909	67	6	0,007353

APÊNDICE E – Medidas de Centralidade da Rede de Gangues

Degree			Betweenness			PageRank			D+B+PR		
Class	ID	Medida	Class	ID	Medida	Class	Id	Medida	Class	Id	Medida
35	3	0,015152	35	18	0,000000	35	63	0,010474	35	63	0,008542
36	5	0,015152	36	20	0,000000	36	73	0,010474	36	73	0,008542
37	6	0,015152	37	29	0,000000	37	14	0,008841	37	14	0,007998
38	7	0,015152	38	30	0,000000	38	82	0,008433	38	82	0,007861
39	8	0,015152	39	32	0,000000	39	29	0,008176	39	29	0,007776
40	9	0,015152	40	34	0,000000	40	71	0,008176	40	71	0,007776
41	14	0,015152	41	35	0,000000	41	85	0,008176	41	85	0,007776
42	20	0,015152	42	37	0,000000	42	86	0,008139	42	86	0,007764
43	29	0,015152	43	41	0,000000	43	41	0,008117	43	41	0,007756
44	30	0,015152	44	45	0,000000	44	34	0,008018	44	34	0,007723
45	32	0,015152	45	49	0,000000	45	92	0,008018	45	92	0,007723
46	34	0,015152	46	52	0,000000	46	5	0,007857	46	5	0,007669
47	35	0,015152	47	54	0,000000	47	20	0,007857	47	20	0,007669
48	37	0,015152	48	55	0,000000	48	45	0,007857	48	45	0,007669
49	41	0,015152	49	56	0,000000	49	61	0,007857	49	61	0,007669
50	45	0,015152	50	58	0,000000	50	35	0,007486	50	35	0,007546
51	52	0,015152	51	59	0,000000	51	9	0,007470	51	9	0,007540
52	58	0,015152	52	61	0,000000	52	8	0,007021	52	8	0,007391
53	59	0,015152	53	63	0,000000	53	30	0,007021	53	30	0,007391
54	61	0,015152	54	64	0,000000	54	32	0,007021	54	32	0,007391
55	63	0,015152	55	68	0,000000	55	58	0,007021	55	58	0,007391
56	64	0,015152	56	69	0,000000	56	3	0,006966	56	3	0,007372
57	69	0,015152	57	71	0,000000	57	7	0,006966	57	7	0,007372
58	71	0,015152	58	72	0,000000	58	37	0,006966	58	37	0,007372
59	73	0,015152	59	73	0,000000	59	52	0,006966	59	52	0,007372
60	74	0,015152	60	74	0,000000	60	74	0,006966	60	74	0,007372
61	82	0,015152	61	82	0,000000	61	87	0,006966	61	87	0,007372
62	85	0,015152	62	85	0,000000	62	88	0,006966	62	88	0,007372
63	86	0,015152	63	86	0,000000	63	59	0,006932	63	59	0,007361
64	87	0,015152	64	87	0,000000	64	64	0,006932	64	64	0,007361
65	88	0,015152	65	88	0,000000	65	69	0,006932	65	69	0,007361
66	89	0,015152	66	89	0,000000	66	89	0,006932	66	89	0,007361
67	92	0,015152	67	92	0,000000	67	6	0,006909	67	6	0,007353

APÊNDICE F – Identificação de Comunidades da Rede de Inteligência

Id	Comunidade	Id	Comunidade
2	0	32	4
23	0	33	4
25	0	40	4
36	0	43	4
38	0	51	4
65	0	53	4
75	0	58	4
86	0	68	4
3	1	71	4
7	1	77	4
18	1	79	4
21	1	84	4
37	1	85	4
52	1	10	5
56	1	16	5
57	1	19	5
62	1	24	5
66	1	35	5
70	1	91	5
72	1	6	6
74	1	12	6
78	1	27	6
80	1	41	6
87	1	46	6
88	1	48	6
4	2	54	6
15	2	55	6
49	2	59	6
90	2	64	6
5	3	69	6
11	3	83	6
17	3	89	6
20	3	1	7
31	3	22	7
39	3	42	7
45	3	44	7
47	3	63	7
60	3	67	7
61	3	73	7
82	3	14	8
8	4	26	8
9	4	34	8
13	4	50	8
28	4	76	8
29	4	81	8
30	4	92	8

APÊNDICE G – Medidas de Eficiência de Resiliência

Passos	Nodes Removidos	Grau Eficiência Degree	Grau Eficiência Betweenness	Grau Eficiência PageRank	Grau Eficiência Média Centralidade
1	0	0,318	0,318	0,318	0,318
2	1	0,344	0,344	0,344	0,344
3	2	0,365	0,365	0,365	0,365
4	3	0,390	0,383	0,390	0,383
5	4	0,393	0,393	0,400	0,393
6	5	0,403	0,404	0,410	0,403
7	6	0,415	0,414	0,414	0,414
8	7	0,423	0,425	0,427	0,427
9	8	0,425	0,439	0,429	0,439
10	9	0,437	0,447	0,434	0,447
11	10	0,436	0,453	0,447	0,453
12	11	0,435	0,460	0,453	0,452
13	12	0,441	0,459	0,460	0,455
14	13	0,440	0,466	0,459	0,461
15	14	0,440	0,473	0,458	0,468
16	15	0,439	0,480	0,465	0,475
17	16	0,453	0,483	0,464	0,479
18	17	0,466	0,487	0,464	0,482
19	18	0,465	0,491	0,464	0,486
20	19	0,465	0,495	0,467	0,490
21	20	0,464	0,500	0,471	0,490
22	21	0,472	0,504	0,475	0,490
23	22	0,472	0,509	0,478	0,489
24	23	0,471	0,514	0,494	0,489
25	24	0,470	0,513	0,493	0,493
26	25	0,470	0,518	0,493	0,493
27	26	0,474	0,518	0,493	0,498
28	27	0,473	0,518	0,493	0,503
29	28	0,482	0,518	0,493	0,508
30	29	0,482	0,518	0,492	0,513
31	30	0,486	0,519	0,492	0,518
32	31	0,491	0,519	0,492	0,519
33	32	0,491	0,519	0,491	0,519
34	33	0,491	0,519	0,491	0,519
35	34	0,491	0,520	0,496	0,519
36	35	0,490	0,520	0,502	0,519
37	36	0,490	0,520	0,507	0,519
38	37	0,490	0,521	0,513	0,519
39	38	0,490	0,521	0,513	0,520
40	39	0,495	0,522	0,520	0,520
41	40	0,501	0,522	0,520	0,520
42	41	0,508	0,522	0,520	0,520
43	42	0,507	0,522	0,520	0,520
44	43	0,507	0,523		0,520
45	44	0,508	0,523		0,520
46	45	0,508	0,524		
47	46	0,515	0,523		
48	47	0,515	0,523		
49	48	0,516	0,524		
50	49	0,516	0,524		
51	50	0,516	0,525		
52	51	0,524	0,526		
53	52		0,526		
54	53		0,526		
55	54		0,527		
56	55		0,527		

APÊNDICE H – Medidas de Segurança de Resiliência

Passos	Nodes Removidos	Grau Segurança Degree	Grau Segurança Betweenness	Grau Segurança PageRank	Grau Segurança Média Centralidade
1	0	0,0294	0,0294	0,0294	0,0294
2	1	0,0298	0,0298	0,0298	0,0298
3	2	0,0300	0,0300	0,0300	0,0300
4	3	0,0304	0,0306	0,0304	0,0304
5	4	0,0303	0,0308	0,0308	0,0300
6	5	0,0305	0,0313	0,0310	0,0302
7	6	0,0306	0,0309	0,0306	0,0304
8	7	0,0305	0,0311	0,0308	0,0305
9	8	0,0301	0,0313	0,0304	0,0310
10	9	0,0303	0,0317	0,0303	0,0314
11	10	0,0301	0,0322	0,0307	0,0319
12	11	0,0299	0,0324	0,0312	0,0318
13	12	0,0301	0,0323	0,0313	0,0313
14	13	0,0299	0,0328	0,0312	0,0318
15	14	0,0300	0,0333	0,0310	0,0316
16	15	0,0304	0,0338	0,0314	0,0321
17	16	0,0309	0,0333	0,0312	0,0323
18	17	0,0314	0,0339	0,0314	0,0324
19	18	0,0311	0,0344	0,0318	0,0330
20	19	0,0312	0,0350	0,0320	0,0335
21	20	0,0317	0,0356	0,0325	0,0333
22	21	0,0322	0,0362	0,0330	0,0330
23	22	0,0323	0,0369	0,0331	0,0331
24	23	0,0324	0,0375	0,0337	0,0337
25	24	0,0325	0,0364	0,0334	0,0338
26	25	0,0321	0,0366	0,0339	0,0339
27	26	0,0326	0,0368	0,0345	0,0345
28	27	0,0332	0,0370	0,0346	0,0351
29	28	0,0337	0,0372	0,0352	0,0357
30	29	0,0343	0,0369	0,0353	0,0364
31	30	0,0344	0,0375	0,0360	0,0370
32	31	0,0350	0,0383	0,0355	0,0377
33	32	0,0356	0,0390	0,0356	0,0379
34	33	0,0362	0,0392	0,0362	0,0386
35	34	0,0363	0,0399	0,0369	0,0387
36	35	0,0370	0,0407	0,0376	0,0395
37	36	0,0377	0,0416	0,0383	0,0390
38	37	0,0377	0,0424	0,0391	0,0391
39	38	0,0384	0,0433	0,0391	0,0398
40	39	0,0392	0,0443	0,0399	0,0399
41	40	0,0400	0,0452	0,0407	0,0400
42	41	0,0408	0,0447	0,0408	0,0408
43	42	0,0408	0,0449	0,0408	0,0416
44	43	0,0417	0,0459		0,0425
45	44	0,0426	0,0470		0,0426
46	45	0,0435	0,0481		
47	46	0,0444	0,0473		
48	47	0,0455	0,0475		
49	48	0,0465	0,0486		
50	49	0,0476	0,0498		
51	50	0,0488	0,0511		
52	51	0,0500	0,0524		
53	52		0,0526		
54	53		0,0540		
55	54		0,0555		
56	55		0,0556		

APÊNDICE I – Medidas de Eficiência de Ruptura

Simulação	Nodes Removidos	Grau de Eficiência
1	13	0,0734
2	19	0,0620
3	24	0,0561
4	25	0,0519
5	30	0,0522
6	34	0,0536
7	37	0,0545
8	38	0,0502
9	39	0,0468
10	40	0,0467

APÊNDICE J – Identificação de Crimes praticados pelos Infratores

Id	Homicídio	Roubo	Sequestro/ Extorção Mediante Sequestro	Estupro	Tráfico de Droga	Tráfico de Arma	Porte de Arma	Falsidade Ideológica	Estelionato
1	1	1			a		1		
2	1				1				
3		1			1		1	1	
4		1			1		1	1	
5		1			1			1	
6	1	1			1			1	
7	1							1	
8					1				
10		1			1				
11		1	1		1			1	
12		1							
13	1	1	1		1			1	
14		1			1		1		1
15		1			1		1		
16					1		1		
17		1	1				1		
18		1							
19					1		1		
20					1				
21	1	1			1	1	1		
22		1			1		1		
26					1				
28	1				1				
29		1			1				
30					1		1		
31		1	1		1				
32					1				
33	1	1			1				
34		1			1			1	
35					1		1		
36	1						1		
37		1							
38	1						1		
39		1	1		1				
40					1		1		
41	1	1			1		1		
42	1	1			1		1		
43	1	1			1		1		
44	1	1			1				
45					1				
46					1				
47	1	1	1		1		1		
48	1	1		1	1	1	1	1	1
49		1			1		1	1	
51					1				
52	1				1				
53	1				1				
54	1				1				
55					1				
56		1							
58	1								
59		1							
60	1	1			1		1	1	
61	1	1			1		1	1	
62		1	1						
63	1	1			1		1		
64	1	1	1		1		1		
65	1				1				
67		1			1	1	1		
68	1				1		1		
69		1			1		1		
70	1					1			
71		1			1		1		
72		1			1				
73		1	1				1		
74	1	1			1			1	
78	1	1			1			1	
79	1	1			1		1	1	
80	1	1	1		1		1		
81		1			1		1		
82		1					1		
83	1	1					1		
84	1	1			1				
85					1				
86	1	1	1		1		1		
87		1							
88	1				1				
89	1	1			1				
90	1	1			1		1		
92		1			1				
Total	37	53	11	1	63	4	37	15	2

APÊNDICE K – Medidas *Multiplex*

Multiplexity					
Class	Id	Medida	Class	Id	Medida
1	48	0,8571429	47	70	0,2857143
2	21	0,7142857	48	71	0,2857143
3	47	0,7142857	49	72	0,2857143
4	80	0,7142857	50	73	0,2857143
5	1	0,5714286	51	83	0,2857143
6	11	0,5714286	52	86	0,2857143
7	44	0,5714286	53	88	0,2857143
8	61	0,5714286	54	92	0,2857143
9	64	0,5714286	55	6	0,1428571
10	89	0,5714286	56	7	0,1428571
11	90	0,5714286	57	8	0,1428571
12	3	0,4285714	58	10	0,1428571
13	4	0,4285714	59	14	0,1428571
14	13	0,4285714	60	18	0,1428571
15	15	0,4285714	61	20	0,1428571
16	17	0,4285714	62	26	0,1428571
17	22	0,4285714	63	28	0,1428571
18	31	0,4285714	64	29	0,1428571
19	33	0,4285714	65	30	0,1428571
20	39	0,4285714	66	32	0,1428571
21	43	0,4285714	67	37	0,1428571
22	49	0,4285714	68	45	0,1428571
23	60	0,4285714	69	46	0,1428571
24	67	0,4285714	70	51	0,1428571
25	74	0,4285714	71	55	0,1428571
26	78	0,4285714	72	56	0,1428571
27	79	0,4285714	73	59	0,1428571
28	81	0,4285714	74	82	0,1428571
29	2	0,2857143	75	84	0,1428571
30	5	0,2857143	76	85	0,1428571
31	16	0,2857143	77	87	0,1428571
32	19	0,2857143	78	9	0
33	34	0,2857143	79	12	0
34	35	0,2857143	80	23	0
35	36	0,2857143	81	24	0
36	38	0,2857143	82	25	0
37	40	0,2857143	83	27	0
38	41	0,2857143	84	50	0
39	42	0,2857143	85	57	0
40	52	0,2857143	86	58	0
41	53	0,2857143	87	65	0
42	54	0,2857143	88	66	0
43	62	0,2857143	89	75	0
44	63	0,2857143	90	76	0
45	68	0,2857143	91	77	0
46	69	0,2857143	92	91	0

APÊNDICE L – Medidas de Diversidade de Nó

Class	ID	Medida	Class	ID	Medida
1	48	3,278323	47	34	0,966231
2	80	2,810666	48	92	0,966231
3	47	2,713366	49	41	0,900258
4	21	2,473843	50	83	0,900258
5	11	2,240189	51	42	0,890331
6	90	1,725557	52	38	0,889485
7	1	1,690175	53	63	0,889223
8	60	1,681707	54	73	0,889178
9	13	1,677528	55	6	0,864248
10	43	1,674342	56	8	0,864248
11	33	1,661463	57	10	0,864248
12	81	1,660981	58	14	0,864248
13	31	1,623755	59	20	0,864248
14	39	1,623755	60	26	0,864248
15	44	1,599427	61	28	0,864248
16	89	1,520120	62	29	0,864248
17	17	1,478308	63	30	0,864248
18	67	1,458600	64	32	0,864248
19	53	1,454237	65	45	0,864248
20	68	1,407708	66	46	0,864248
21	40	1,404117	67	51	0,864248
22	35	1,347016	68	55	0,864248
23	2	1,316481	69	84	0,864248
24	70	1,266582	70	85	0,864248
25	79	1,257082	71	18	0,781209
26	72	1,249718	72	37	0,781209
27	61	1,248201	73	56	0,781209
28	71	1,224877	74	59	0,781209
29	64	1,211208	75	82	0,781209
30	19	1,204705	76	87	0,781209
31	74	1,189971	77	7	0,697205
32	78	1,189971	78	9	0,000000
33	4	1,175713	79	12	0,000000
34	15	1,175713	80	23	0,000000
35	49	1,175713	81	24	0,000000
36	22	1,170652	82	25	0,000000
37	3	1,168331	83	27	0,000000
38	36	1,165315	84	50	0,000000
39	5	1,115240	85	57	0,000000
40	86	1,098373	86	58	0,000000
41	54	1,085730	87	65	0,000000
42	52	1,082204	88	66	0,000000
43	88	1,082204	89	75	0,000000
44	16	1,067827	90	76	0,000000
45	62	0,999871	91	77	0,000000
46	69	0,967211	92	91	0,000000

APÊNDICE M – Quantidade de Laços

Multiplex

Class	Node1	Node2	Quant.
1	80	47	5
2	21	48	4
3	44	1	4
4	44	80	4
5	47	61	4
6	64	48	4
7	80	21	4
8	80	48	4
9	80	90	4
10	89	48	4
11	3	80	3
12	4	15	3
13	4	90	3
14	11	39	3
15	11	47	3
16	17	47	3
17	21	81	3
18	22	1	3
19	22	80	3
20	31	11	3
21	31	39	3
22	33	13	3
23	43	13	3
24	43	33	3
25	47	31	3
26	47	39	3
27	48	67	3
28	49	4	3
29	49	15	3
30	49	90	3
31	60	11	3
32	74	80	3
33	78	80	3
34	79	33	3
35	80	3	3
36	80	11	3
37	80	81	3
38	2	80	2
39	16	19	2
40	16	80	2
41	17	11	2
42	17	39	2
43	19	48	2
44	19	80	2
45	19	81	2
46	31	17	2
47	34	81	2

Class	Node1	Node2	Quant.
48	35	19	2
49	38	36	2
50	40	71	2
51	42	67	2
52	42	73	2
53	43	53	2
54	44	67	2
55	44	73	2
56	47	5	2
57	47	67	2
58	48	54	2
59	62	80	2
60	63	67	2
61	68	13	2
62	68	33	2
63	69	48	2
64	72	21	2
65	80	16	2
66	80	19	2
67	80	52	2
68	80	54	2
69	80	88	2
70	83	41	2
71	83	48	2
72	86	2	2
73	92	81	2
74	2	36	1
75	5	47	1
76	10	19	1
77	13	51	1
78	18	21	1
79	18	72	1
80	20	47	1
81	26	14	1
82	26	81	1
83	28	51	1
84	29	28	1
85	30	51	1
86	32	51	1
87	33	51	1
88	35	10	1
89	45	47	1
90	46	6	1
91	46	48	1
92	46	55	1
93	47	20	1
94	48	51	1

Class	Node1	Node2	Quant.
95	48	55	1
96	48	59	1
97	51	8	1
98	51	40	1
99	51	84	1
100	53	51	1
101	53	85	1
102	56	21	1
103	56	80	1
104	60	82	1
105	67	70	1
106	68	51	1
107	80	7	1
108	80	37	1
109	80	51	1
110	80	70	1
111	80	87	1

Anexos

ANEXO A – Memorando PMMG

**POLÍCIA
MILITAR**
DE MINAS GERAIS
ESTADO-MAIOR

Memorando nº 10. 034 .1/17-EMPM

Belo Horizonte, 13 de janeiro de 2017.

Ao : Coronel PM Diretor de Inteligência
Assunto : Autorização de Pesquisa

Deu entrada nesta Chefia do Estado-Maior a solicitação do nº 095.606-0, Cel QOR Alex Sander de Oliveira Toledo, CPF 777.493.756-00, CI M-5.054.896, pertencente ao Centro Administração de Pessoal (CAP), para acessar os dados contidos no "Cadastro de Vínculo de Ocorrências" da Polícia Militar de Minas Gerais.

O Oficial encontra-se devidamente matriculado no Centro Federal de Educação Tecnológica de Minas Gerais e está realizando a pesquisa intitulada "Modelagem para Identificação de Redes Humanas de Criminalidade",

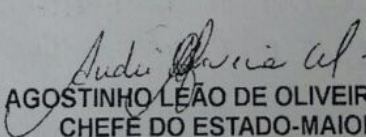
O objetivo do acesso do "Cadastro de Vínculo de Ocorrências" é a pesquisa e o estudo visando transformar o banco de dados em um grafo dinâmico, que permita estudar interações na rede. O caráter ético desta pesquisa deverá assegurar a preservação da identidade das pessoas contidas no referido banco de dados.

Diante do exposto, RESOLVE:

1. autorizar o nº 095.606-0, Cel QOR Alex Sander de Oliveira Toledo, a utilizar os dados contidos no "Cadastro de Vínculo de Ocorrências" da Polícia Militar de Minas Gerais, para fins de estudos;

2. Deverão ser realizados contatos bilaterais entre a DINT e o Oficial solicitante, para a adoção das medidas pertinentes, conforme a legislação em vigor.

EMPM em Belo Horizonte, 13 de janeiro de 2017.


ANDRÉ AGOSTINHO LEÃO DE OLIVEIRA, CORONEL PM
CHEFE DO ESTADO-MAIOR