



Universidade de Brasília – UnB
Programa de Pós-Graduação em Administração – PPGA
Mestrado Profissional em Administração Pública – MPA

**REDES CRIMINOSAS EM INVESTIGAÇÕES
PREVIDENCIÁRIAS NA POLÍCIA FEDERAL**

Nelson Levy Kneip de Freitas Macêdo

Brasília – DF

2020



Universidade de Brasília – UnB
Programa de Pós-Graduação em Administração – PPGA
Mestrado Profissional em Administração Pública – MPA

**REDES CRIMINOSAS EM INVESTIGAÇÕES
PREVIDENCIÁRIAS NA POLÍCIA FEDERAL**

Nelson Levy Kneip de Freitas Macêdo

Dissertação apresentada à banca examinadora do Programa de Pós-graduação em Administração – PPGA/UnB, como requisito parcial para a obtenção do título de Mestre em Administração Pública.

Orientador: Professor Doutor Adalmir de Oliveira Gomes.

Brasília – DF

2020

Espaço para a ficha catalográfica

NELSON LEVY KNEIP DE FREITAS MACEDO

**REDES CRIMINOSAS EM INVESTIGAÇÕES
PREVIDENCIÁRIAS NA POLÍCIA FEDERAL**

PARECER DA COMISSÃO EXAMINADORA:

A Comissão examinadora composta pelos professores abaixo, sob a presidência do primeiro, considera o candidato Macêdo NELSON LEVY KNEIP DE FREITAS MACÊDO aprovado.

Brasília-DF, 20 de fevereiro de 2020.

Prof. Dr. Adalmir de Oliveira Gomes (UnB)
(orientador)

Prof. Dr. Daniel Pires Vieira (UnB)
(membro interno)

Prof. Dr. Mario Procopiuck (PUC/PR)
(membro externo)

Profª Dra. Maria Figueiredo Moreira (UnB)
(membro suplente)

Às mulheres da minha vida: Efigênia, D'júlia,
D'jennifer, Mariana e Maria Erotides, pelo exemplo de
força e suavidade que somente o poder feminino pode
fazer unir.

RESUMO

As fraudes contra o sistema previdenciário brasileiro causam prejuízo bilionário anualmente aos cofres públicos e o presente trabalho busca formas de auxiliar à Polícia Federal no combate a este tipo de fraude. Para tanto foram estudados, com o método da Análise de Redes Sociais, alguns casos já concluídos de operações de combate a grupos criminosos atuantes naquela área, delineando uma rede básica de composição de grupos criminosos e propondo algoritmo de detecção ou predição destes grupos. O algoritmo foi testado em investigações em andamento em quatro unidades da federação, identificando a existência de 37 prováveis grupos criminosos organizados envolvidos em fraudes apuradas em diversas investigações feitas de maneira isolada. O algoritmo proposto pode auxiliar não só na identificação ou predição de grupos criminosos, mas também ajudar na definição, mediante critérios objetivos e com base em método científico, da aplicação dos recursos disponíveis de forma a maximizar os resultados no combate à atuação de grupos criminosos organizados.

Palavras-Chave: Polícia Federal – Análise de Redes Sociais – Organizações Criminosas – Crimes previdenciários – Predição – Detecção.

ABSTRACT

Frauds against the Brazilian social security system cause billionaire losses annually to public coffers and the present work seeks ways to assist the Federal Police in combating this type of fraud. For this purpose, some cases already concluded of operations to combat criminal groups operating in that area were studied, using the Social Network Analysis method, outlining a basic network of composition of criminal groups and proposing an algorithm for detecting or predicting these groups. The algorithm was tested in ongoing investigations in four units of the federation, identifying the existence of 37 probable organized criminal groups involved in fraud investigated in several investigations carried out in isolation. The proposed algorithm can assist not only in the identification or prediction of criminal groups, but also in the definition, using objective criteria and based on a scientific method, of the application of available resources in order to maximize the results in combating the activities of organized criminal groups.

Keywords: Federal Police - Social Network Analysis - Criminal Organizations - Social Security Crimes - Prediction - Detection.

Impunitas, peccandi illecebra

(A impunidade incentiva o crime)

Fedro (Livro II, Fábula III. Séc. I d.C.)

LISTA DE FIGURAS

Figura 1. Fluxo da pesquisa	52
Figura 2. Modelo de redes observado nas operações analisadas	63
Figura 3. Rede da Operação Fim de Linha	65
Figura 4. Rede da Operação Casa Cheia	67
Figura 5. Rede da Operação Casa Cheia II	69
Figura 6: Rede da Operação Intervenção	71
Figura 7: Rede da Operação Intervenção II	72
Figura 8. Rede da Operação Aquestos	74
Figura 9. Rede da Operação Duo Fratres II	78
Figura 10. Estrutura de rede básica	79
Figura 13. Rede dos inquéritos em andamento na UF1	85
Figura 14. Rede de grupos criminosos detectados da UF1	87
Figura 15. Rede dos inquéritos em andamento na UF2	88
Figura 16. Rede de grupos criminosos detectados da UF2	89
Figura 17. Rede dos inquéritos em andamento na UF3	91
Figura 18: Rede de grupos criminosos detectados UF3	92
Figura 19. Rede dos inquéritos em andamento na UF4	93
Figura 20. Rede de grupos criminosos detectados UF4	94
Figura 21. Rede simplificada do subgrupo do IPL1059	141
Figura 22. Rede formada a partir do IPL889	157
Figura 23. Rede formada a partir do IPL939	158
Figura 24. Rede formada a partir do IPL864	159
Figura 25. Rede da rede do subgrupo do IPL720	172

LISTA DE TABELAS

Tabela 1 Distinções entre associação criminosa e organização criminosa	31
Tabela 2 Comparativo entre as regras da Lei 9.034/05 e Lei 12.850/13	32
Tabela 3 Meios utilizados para fraudes nas operações	53
Tabela 4 Centralidade dos atores da rede da Operação Fim de Linha	65
Tabela 5 Atores da Rede da Operação Casa Cheia	67
Tabela 6 Atores da Rede da Operação Casa Cheia II	69
Tabela 7 Atores da Rede da Operação Intervenção	71
Tabela 8 Atores da Rede da Operação Intervenção II	73
Tabela 9 Atores da Rede da Operação Aquestos	75
Tabela 10 Atores da Rede da Operação Duo Fratres II	78
Tabela 11 Análise de aplicação do modelo-base a operações já concluídas	82
Tabela 12 Algoritmo de detecção/predição de grupos criminosos em fraudes previdenciárias	83
Tabela 13 Endereços duplicados em benefícios de inquiridos da UF4	95
Tabela 14 Operações deflagradas, objeto, processos fraudados e prejuízo	97
Tabela 15 Percentual de IPLs identificáveis pelo modelo proposto	98
Tabela 16 Quantitativos de grupos identificados pelo algoritmo	99
Tabela 45 Dados gerais e estatísticas de regressão das Operações	104
Tabela 17 Servidores com maior grau de centralidade na rede da UF1	114
Tabela 18 APS com maior grau de centralidade na UF1	115
Tabela 19 Dados das redes do subgrupo formadas com atores de maior grau de centralidade	115
Tabela 20 Redes de subgrupos formadas a partir dos Servidores da UF1	116
Tabela 21 Redes de subgrupos formados a partir das APSs da UF1	121
Tabela 22 Medições dos principais atores da rede da UF1	125
Tabela 23 Matriz de Correlação da rede da UF1	127
Tabela 24 Servidores com maior grau de centralidade na rede da UF1	128
Tabela 25 APS com maior grau de centralidade na rede da UF1	129
Tabela 26 Dados das redes do subgrupo formadas com atores de maior grau de centralidade	129
Tabela 27 Redes de subgrupos formados a partir dos servidores da UF1	131
Tabela 28 Redes de subgrupos formados a partir das APSs da UF2	134

Tabela 29 Medições dos principais atores da rede da UF2	139
Tabela 30 Matriz de Correlação da UF2	142
Tabela 31 Servidores com maior grau de centralidade na rede da UF1	143
Tabela 32 APS com maior grau de centralidade na rede da UF1	143
Tabela 33 Dados das redes do subgrupo formadas com atores de maior grau de centralidade	144
Tabela 34 Redes de subgrupos formados a partir dos servidores da UF3	145
Tabela 35 Redes de subgrupos formados a partir das APSs da UF2	150
Tabela 36 Medições dos principais atores da rede da UF2	155
Tabela 37 Matriz de Correlação da UF3	159
Tabela 38 Servidores com maior grau de centralidade na rede da UF1	161
Tabela 39 APS com maior grau de centralidade na rede da UF1	161
Tabela 40 Dados das redes do subgrupo formadas com atores de maior grau de centralidade	162
Tabela 41 Redes de subgrupos formados a partir dos servidores da UF4	163
Tabela 42 Redes de subgrupos formados a partir das APSs da UF4	166
Tabela 43 Medições dos principais atores da rede da UF4	170
Tabela 44 Matriz de correlação da UF4	172

SUMÁRIO

1. INTRODUÇÃO	12
2. VISÃO GERAL SOBRE A SEGURIDADE SOCIAL NO BRASIL	16
2.1. Crimes contra a seguridade social	17
2.2. Estrutura institucional para investigação dos crimes contra a previdência	19
2.3. Conexão e continência	23
3. REFERENCIAL TEÓRICO	26
3.1. Origem das Organizações Criminosas	26
3.2. Conceito legal das organizações criminosas	27
3.3. Características	32
3.4. As redes e a investigação policial	35
3.5. Redes de organizações criminosas	38
3.6. Detecção e predição de organizações criminosas	42
4. MÉTODO	47
4.1. Desenho da pesquisa	52
4.2. Seleção das operações concluídas	52
4.3. Análise de Redes Sociais	54
4.3.1 Conceitos	55
4.3.2 Tipos de redes	58
4.3.3. Variáveis	59
4.4. Limitações dos dados e das análises	61
5. RESULTADOS	63
5.1. Etapa 1: mapeamento de operações já concluídas	63
5.1.1. Rede 1: Operação Fim de Linha	64
5.1.2. Rede 2: Operação Casa Cheia	66
5.1.3 Rede 3: Operação Casa Cheia II	68
5.1.4. Rede 4: Operação Intervenção	70
5.1.5. Rede 5: Operação Intervenção II	72

5.1.6. Rede 6: Operação Aquestos	74
5.1.7. Rede 7: Operação Duo Fratres II	76
5.2. Etapa 2: Pontos comuns e delineamento de uma rede básica	79
5.3. Etapa 3: Teste do algoritmo em redes de investigações em andamento	84
5.3.1. Rede 8: Unidade da Federação 1 - UF1	84
5.3.2. Rede 9: Unidade da Federação 2 - UF2	87
5.3.3. Rede 10: Unidade da Federação 3 - UF3	90
5.3.4. Rede 11: Unidade da Federação 4 - UF4	93
5.3.5 Síntese dos resultados	97
6. DISCUSSÃO E IMPLICAÇÕES DOS RESULTADOS	99
7. CONSIDERAÇÕES FINAIS	105
REFERÊNCIAS	108
Apêndice I - Individualização das redes dos subgrupos da UF1	114
Apêndice II - Individualização das redes de subgrupos da UF2	128
Apêndice III - Individualização das redes de subgrupos da UF3	143
Apêndice IV - Individualização das redes de subgrupos da UF4	161
Apêndice V – Memória de cálculo	174

1. INTRODUÇÃO

No ordenamento jurídico pátrio, a investigação e combate a crimes contra a Previdência Social são atribuições da Polícia Federal - PF, que realiza, todo ano, diversas operações policiais e outras ações nesse sentido. Tais crimes geram prejuízos enormes para o país e a sociedade, tendo o Tribunal de Contas da União - TCU (2018) estimado a perda de no mínimo 63 bilhões de reais apenas com fraudes e erros em benefícios previdenciários.

Um dos maiores problemas relacionados com esse tipo de crime é a constituição de redes em forma de associações ou organizações criminosas que, explorando fragilidades do sistema e não raras vezes contando com a participação de servidores do próprio Instituto Nacional de Seguridade Social - INSS, fraudam o sistema de previdência e causam prejuízos de maneira muito mais severa do que ações individuais e descoordenadas.

O combate a esse tipo de crime, e o combate a essas redes, é um grande desafio porque o sistema de Previdência Social no Brasil apresenta grande capilaridade e precisa atender uma parcela muito frágil da população, de forma que no binômio ‘facilidade de acesso’ *versus* ‘segurança do sistema’ a decisão político-gerencial favorece a proteção dos cidadãos e facilita o acesso aos benefícios, o que conseqüentemente cria brechas que são exploradas por pessoas mal-intencionadas.

Existe pouca literatura a respeito de fraudes previdenciárias, bem como pouca inovação em termos de modelos de investigação, principalmente nos estratos superiores de publicação científica, sendo observável que o trabalho investigativo-policial se desenvolve de maneira muito mais empírica (aqui no sentido de métodos de investigação transmitidos pelos policiais mais experientes aos mais jovens) do que embasado em modelos teórico-científicos.

O presente estudo buscou suprir parte dessa lacuna ao investigar redes de organizações criminosas que atuam para lesar o sistema previdenciário. O estudo inova ao utilizar a Análise de Redes Sociais – ARS como método de pesquisa para buscar delinear uma rede básica de atuação de grupos criminosos fraudadores de benefícios da Previdência Social. Além disso, o estudo buscou ainda identificar esse padrão de redes de organizações criminosas em investigações em andamento na PF, testando a busca pela rede básica apresentada. Em outras palavras, o presente estudo descreve redes de grupos criminosos observadas em operações passadas de combate a crimes previdenciários para, com isso, propor modelagem (em forma de algoritmo) que ajude a predizer ou detectar redes atuais e futuras do mesmo tipo.

Assim, o estudo busca responder a seguinte pergunta: é possível identificar vínculos ou conexões (rede social) existente em investigações policiais em andamento e que tenham a mesma estrutura observada em casos anteriores de fraudes previdenciárias cometidas por grupos criminosos? Ao responder essa pergunta, acredita-se que o estudo poderá gerar modelos de detecção ou preditivos úteis tanto no combate a organizações criminosas atuais que lesam o sistema previdenciários, quanto na prevenção da formação de novas organizações criminosas.

Desta forma, o objetivo geral da pesquisa passa por descrever a estrutura de relacionamentos de redes de grupos criminosos em investigações anteriores (operações) da Polícia Federal sobre crimes previdenciários a fim de propor um modelo de detecção/predição de redes de grupos criminosos em investigações atuais e futuras.

Os objetivos específicos são os seguintes:

- a) Identificar e selecionar operações anteriores a 2019 da PF de combate a fraudes previdenciárias para análise de suas redes;
- b) Identificar uma rede básica que se aplique aos grupos criminosos já detectados anteriormente e que atuavam em crimes previdenciários, delineando algoritmo de detecção ou predição de grupos criminosos; e
- c) Testar o algoritmo delineado em redes de investigações atuais da PF em quatro diferentes unidades da Federação.

O estudo é relevante por diversos motivos. Em termos gerenciais e técnicos, o estudo se justifica porquanto pode auxiliar na identificação de investigações conexas (ou mesmo em duplicidade), cujo modelo pode inclusive ser adaptado para implementação em outras áreas de investigação. Isso porque, embora exista rotina de busca por investigações conexas no cotidiano das unidades, é bastante factível que a suspeita e/ou descoberta de atos de uma organização criminosa (determinadas fraudes, por exemplo) ocorra de maneira isolada, especialmente levando em conta o grande número de investigações em andamento e a larga distribuição geográfica de atuação dos grupos criminosos. A atuação de maneira isolada no combate às fraudes faria com que fossem abertas diferentes investigações para cada fraude descoberta. Caso a conexão entre estas não seja detectada, ou seja, caso não haja a identificação do grupo que age de maneira subliminar, acarretaria que fossem responsabilizados apenas os fraudadores que aparecem fisicamente (os “peixes pequenos”), e nunca os destinatários finais ou reais líderes das organizações criminosas.

Ainda em termos gerenciais, o processamento de grande volume de informações gerados com as diferentes investigações demanda a criação de rotinas que possam auxiliar no trabalho investigativo. A definição de uma rede básica pode ajudar a entender conexões

existentes entre investigações diferentes. A aplicação prática do conhecimento teórico sobre a Análise de Redes Sociais possibilita a identificação de conexões que seriam invisíveis pelos métodos tradicionais, seja pela limitação humana em processar tamanho volume de informações, seja porque as investigações correm sob responsabilidade de pessoas diferentes e em locais diferentes.

Em termos econômicos, a responsabilização dos líderes dos grupos criminosos poderia gerar um efeito pedagógico de desestimular outras pessoas dispostas ao cometimento de fraudes contra a Previdência Social. Como as fraudes e erros em processos de benefício representam valores consideráveis, afetando em torno de 11% dos benefícios, o incremento das ações que evitem tais fraudes pode gerar uma enorme economia financeira ao erário. Tal economia também traria benefícios em termos sociais, posto que os recursos, que hoje se esvaem nas fraudes, poderiam ser utilizados na efetivação de políticas públicas em benefício de toda a população. Além disso, em última análise, a melhoria do sistema de fiscalização ajuda a preservar a integridade do próprio sistema de Previdência Social, de amplo alcance e interesse coletivo.

Em termos institucionais, considerando a instituição PF, o estudo aponta caminhos que podem auxiliar no aprimoramento dos mecanismos de combate à criminalidade atuante em matéria de crimes previdenciários, contribuindo para o alcance de um objetivo institucional de combate à criminalidade, previsto no Planejamento Estratégico do órgão. A identificação e o combate às organizações criminosas podem trazer ganhos de qualidade ao trabalho produzido, auxiliando no alcance da missão institucional da PF.

Por fim, em termos teóricos, o estudo é importante por gerar conhecimentos a respeito das redes de organizações criminosas, tema esse relativamente pouco desenvolvido na literatura internacional, como mostram os resultados da revisão realizada. Os resultados do estudo podem contribuir para a consolidação de uma teoria específica para o funcionamento de redes de organizações criminosas no âmbito previdenciário.

O presente estudo está dividido da seguinte forma: a) inicialmente é feita uma contextualização a respeito do sistema de Seguridade Social no Brasil, abordando as principais modalidades de fraudes cometidas, a estrutura atualmente disponível para combate a tais fraudes e as regras existentes para reunião de investigações correlatas; b) em seguida é apresentado o referencial teórico a respeito das organizações criminosas, trazendo: b.1) seu conceito legal e características, b.2.) as redes e a investigação policial; b.3) redes de organizações criminosas, e b.4) a detecção e predição de organizações criminosas; c) apresentação dos aspectos metodológicos, detalhando as etapas da pesquisa, variáveis, desenho

da pesquisa e limitações; d) apresentação dos resultados, com d.1) o mapeamento de redes em operações já concluídas, d.2) o delineamento de uma rede básica e de algoritmo de detecção ou predição, d.3) o mapeamento de investigações em andamento e teste do algoritmo; e) a discussão dos resultados e f) as considerações finais.

2. VISÃO GERAL SOBRE A SEGURIDADE SOCIAL NO BRASIL

Nesta seção serão apresentadas algumas características gerais do sistema de Previdência Social vigente no Brasil. Serão vistos ainda os principais tipos de crimes e fraudes cometidos contra o sistema de previdência. Após, será apresentada a forma como está estruturada a Polícia Federal para atuação na repressão e investigação de crimes contra a Previdência Social, apresentando ainda elementos que ajudem a entender como funcionam as investigações sobre fatos conexos.

Conforme histórico do INSS (2017), desde a época do Império já havia no Brasil certas formas de previdência. Em 1923 com o Decreto Legislativo nº 4.682 (Lei Eloy Chaves) foi marcado o primeiro marco jurídico-normativo, tendo sido criadas as Caixas de Aposentadorias e Pensões para as empresas ferroviárias para apoiar os trabalhadores em suas inatividades. Em 1930, com a ampliação da atuação dos sindicatos, o Estado assumiu a previdência e surgiram os Institutos de Aposentadorias e Pensões - IAPs. Em 1960, a Lei nº 3.807 criou a Lei Orgânica de Previdência Social e depois, em 1966, o Decreto-Lei nº 72 unificou os IAPs então existentes, sendo criado o Instituto Nacional de Previdência Social – INPS. Em 1977 foi criado o Sistema Nacional de Previdência e Assistência Social – SINPAS. Com a Constituição de 1988, foi criado o conceito de Seguridade Social composto pelas áreas da Saúde, Assistência e Previdência Social (INSS, 2017).

Em 1990 foi criado o Instituto Nacional do Seguro Social - INSS, com a fusão do INPS com o Instituto de Administração Financeira da Previdência e Assistência Social – IAPAS. Atualmente, o INSS é responsável pelos segurados vinculados ao Regime Geral de Previdência Social, previsto no art. 201 da Constituição Federal. O Regime Geral tem caráter contributivo e de filiação obrigatória, ou seja, todos os trabalhadores devem contribuir para o financiamento da previdência.

No ano de 2019 foi aprovada a Emenda à Constituição nº 103 que estabeleceu a denominada Reforma da Previdência, visando economia de recursos mediante o estabelecimento de condições mais rígidas em relação às condições até então vigentes, como o aumento da idade mínima para aposentadoria, aumento do tempo de contribuição e alíquota de contribuição dos servidores públicos, dentre outras medidas. Na exposição de motivos para a Proposta de Emenda à Constituição – PEC 06/2019 (Brasil, 2019), que originou na EC nº 103, argumentou-se que o déficit do Regime Geral de Previdência Social foi de R\$195,2 bilhões em 2018, anotando-se ainda que “da mesma forma que o combate às fraudes, a cobrança das dívidas

é muito relevante, mas não constitui medida suficiente para trazer equilíbrio à Previdência Social” (item 16).

A exposição de motivos da PEC argumenta ainda que o primeiro pilar da reforma da previdência seria o combate às fraudes, e que, nessa área, foi editada a Medida Provisória 871/2019, com a finalidade de “estabelecer instrumentos para eliminar a possibilidade de recebimento indevido de benefícios previdenciários, por meio de ajuste de dispositivos legais e instituição de programas especiais de combate às irregularidades” (item 14). De fato, o Tribunal de Contas da União (TCU, 2018) apontou estimativa que a Previdência Social tem prejuízo anual em torno de 63 bilhões de reais por ano apenas com fraudes e erros. Tendo em vista o alto volume de recursos e o prejuízo direto aos cofres públicos, torna-se prioridade buscar meios para otimizar o combate às fraudes e, com isso, tentar minimizar os prejuízos.

2.1. Crimes contra a seguridade social

Analisando os principais crimes cometidos contra a Previdência Social, é possível separar as fraudes em dois grandes grupos: fraudes em custeio e fraudes em benefícios. As fraudes em custeio ocorrem quando o objeto fraudado é o financiamento da Previdência Social, por exemplo, quando o patrão recolhe do trabalhador a contribuição previdenciária, mas não repassa os valores para o INSS. De outro lado estão as fraudes cujo objeto visado é o benefício, podendo esta modalidade ser cometida em dois momentos: na concessão do benefício, por exemplo, com a falsificação de documentos que comprovem condição que daria direito a um benefício; ou na manutenção de um benefício, por exemplo, quando uma pessoa que recebia regularmente um benefício falece e, após seu falecimento, os familiares continuam sacando o benefício sem comunicar ao INSS o óbito.

Os principais crimes no custeio são a apropriação indébita previdenciária e a sonegação de contribuição previdenciária. O crime de apropriação indébita previdenciária é descrito no art. 168-A do Código Penal – CP (Brasil, 1940).

Art. 168-A. Deixar de repassar à Previdência Social as contribuições recolhidas dos contribuintes, no prazo e forma legal ou convencional:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 1º Nas mesmas penas incorre quem deixar de:

I – recolher, no prazo legal, contribuição ou outra importância destinada à Previdência Social que tenha sido descontada de pagamento efetuado a segurados, a terceiros ou arrecadada do público;

II – recolher contribuições devidas à Previdência Social que tenham integrado despesas contábeis ou custos relativos à venda de produtos ou à prestação de serviços;

III – pagar benefício devido a segurado, quando as respectivas cotas ou valores já tiverem sido reembolsados à empresa pela Previdência Social.

Já o crime de sonegação de contribuição previdenciária é previsto no art. 337-A do CP (Brasil, 1940).

Art. 337-A. Suprimir ou reduzir contribuição social previdenciária e qualquer acessório, mediante as seguintes condutas:

I – omitir de folha de pagamento da empresa ou de documento de informações previsto pela legislação previdenciária segurados empregado, empresário, trabalhador avulso ou trabalhador autônomo ou a este equiparado que lhe prestem serviços;

II – deixar de lançar mensalmente nos títulos próprios da contabilidade da empresa as quantias descontadas dos segurados ou as devidas pelo empregador ou pelo tomador de serviços;

III – omitir, total ou parcialmente, receitas ou lucros auferidos, remunerações pagas ou creditadas e demais fatos geradores de contribuições sociais previdenciárias:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

A sonegação da contribuição previdenciária prevê ainda algumas condutas diferentes, como a omissão dos dados na folha de pagamento ou nos lançamentos contábeis da empresa. De qualquer sorte, o legislador considerou as condutas com reprovabilidade semelhante, tendo sido prevista para ambos os crimes a pena de 2 a 5 anos de reclusão.

Dentre as fraudes em benefícios, o estelionato foi o crime com maior incidência (em número de inquéritos policiais) observado nas unidades analisadas. A conduta criminosa é descrita da seguinte forma: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento” (art. 171 do CP, Brasil, 1940). A expressão ‘majorado’ é utilizada no parágrafo terceiro (§3º) do mesmo artigo e prevê o aumento de pena em um terço “se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência” (art. 171 §3º do CP, Brasil, 1940). Desta forma, quando um estelionato é praticado contra o INSS, deve incidir também a causa de aumento prevista no §3º posto que a Previdência Social está ali contemplada.

O crime de estelionato possui dois elementos principais que são: a obtenção da vantagem ilícita, e o emprego de artifício, ardil ou outro meio fraudulento para manter outra pessoa em erro. No caso das fraudes previdenciárias, os dois elementos são claros. Imagine-se um caso onde são falsificados documentos de uma pessoa para justificar a concessão de um benefício previdenciário. A fraude reside na falsificação do documento, e a obtenção da vantagem ilícita decorre do pagamento do benefício.

As falsidades foram aqui inseridas de maneira genérica pois englobam os crimes do art. 297 até o crime do art. 304 do CP. Neste grupo estão a falsificação de documento público (art. 297 do CP), a falsificação de documentos para fins previdenciários (art. 297 §3º e §4º do CP), a falsidade ideológica (art. 299 do CP) e o uso de documento falso (art. 304 do CP). No caso da falsidade ideológica, um exemplo é quando o criminoso obtém um papel original em

branco para emissão de RG (Registro Geral) e o preenche com dados falsos. Assim, o papel onde está o documento é verdadeiro, mas os dados ali contidos são falsos. Enquanto os demais artigos preveem a falsificação em si, o art. 304 prevê como crime o uso de documentos falsos, prevendo para esse caso a mesma punição de quem falsificou.

Entende-se ainda necessário abordar o crime de inserção de dados falsos em sistemas de informação, previsto no art. 313-A do CP (Brasil, 1940).

Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

O crime de inserção de dados falsos possui uma característica diferente dos demais, pois é um tipo de crime que somente pode ser cometido por um tipo específico de pessoa, no caso, um funcionário público autorizado. É a figura que os autores jurídicos chamam de crime próprio. Esse crime possui punição mais grave que os outros crimes mencionados e pode ser configurado quando, por exemplo, um servidor do INSS faz parte de uma associação criminosas e utiliza sua condição de servidor do INSS para fazer o lançamento de informações inexistentes que embasarão a concessão de determinado benefício de maneira fraudulenta. Assim, além do crime de participação em associação criminosa (ou em organização criminosa, dependendo do caso), o servidor poderá ser responsabilizado também pela inserção de dados falsos no sistema do INSS, e/ou pelo estelionato majorado, dependendo do caso, eis que ao fazer isso gerou a obtenção de vantagem ilícita mediante fraude.

2.2. Estrutura institucional para investigação dos crimes contra a previdência

A investigação de crimes contra a Previdência Social é atribuição exclusiva da Polícia Federal por determinação constitucional. A Polícia Federal está subordinada ao Ministério da Justiça e Segurança Pública, componente do Poder Executivo Federal. Dentro da estrutura da Polícia Federal, a atividade principal do órgão – que são as investigações de crimes praticados contra bens ou interesses da União (ou seja, interesse federal) – fica a cargo da Diretoria de Investigação e Combate ao Crime Organizado – DICOR. Compete à DICOR “dirigir, planejar, coordenar, controlar e avaliar a atividade de investigação criminal relativa a infrações penais de atribuição da Polícia Federal” (art. 16 do Regimento Interno da PF – MJSP, 2017). Na DICOR, as atividades são divididas em Coordenações-Gerais, dentre as quais está a

Coordenação-Geral de Polícia Fazendária – CGPFAZ. Na estrutura da CGPFAZ existe a Divisão de Repressão a Crimes Previdenciários – DPREV, divisão responsável nacionalmente pela coordenação técnica das unidades regionais e locais. Todos os órgãos/setores aqui mencionados ficam fisicamente sediados em Brasília-DF.

Em todas as unidades da Federação a Polícia Federal possui uma Superintendência Regional, normalmente localizada na capital do Estado, e cuja estrutura possui relativa simetria com a organização nacional. Nas superintendências existe a Delegacia Regional de Investigação e Combate ao Crime Organizado – DRCOR, na qual estão subordinadas as delegacias responsáveis pelas investigações propriamente ditas. Dentre as delegacias subordinadas à DRCOR, está a DELEPREV – Delegacia de Prevenção e Repressão a Crimes Previdenciários. Em regra, todos os inquéritos policiais que investigam crimes praticados contra a Previdência Social em andamento nas superintendências regionais tramitam na DELEPREV.

Alguns estados possuem ainda delegacias descentralizadas localizadas em municípios do interior. Essas delegacias descentralizadas normalmente possuem estrutura mais simples, não havendo especialização de setores ou servidores com relação à matéria previdenciária. Assim, nessas unidades, um mesmo delegado pode ser responsável por conduzir investigações de diversas naturezas (ambiental, previdenciário, fazendário, entorpecentes, etc.).

Existem ainda as forças-tarefa previdenciárias, compostas originalmente pela Polícia Federal, Ministério Público Federal e INSS, sendo esse último atualmente representado pela COINP – Coordenação de Inteligência Previdenciária, do Ministério da Economia. As forças-tarefas atuavam de maneira informal, sendo que em 2003 o TCU, por meio do Acórdão 314/2003 (TCU, 2003) recomendou a formalização de instrumento que permitisse legalmente a atuação conjunta dos órgãos.

Recomendar ao Ministério Público Federal, ao INSS e à Polícia Federal que envidem esforços para oficializar a atuação conjunta dos três órgãos por meio da Força Tarefa para combate de crimes previdenciários, mediante convênio ou portaria conjunta, contendo definição de regulamento próprio e destinação de recursos humanos, materiais e financeiros específicos, inclusive para estender os trabalhos aos demais estados além do Rio de Janeiro e São Paulo (item 9.3).

Os acordos para formalização das forças-tarefa foram assinados entre os órgãos mencionados e, atualmente, estão presentes em quase todas as Superintendências da Polícia Federal nos estados. Internamente, a atuação das forças-tarefa previdenciária – FTPrev está disciplinada pela Instrução Normativa 28/2010-DG/PF, que prevê que suas ações devem focar no combate à atuação de quadrilhas, associações e organizações criminosas que atuam em crimes previdenciários, especialmente aqueles com maior poder de lesividade, atuando com

seletividade e priorização, visando maior eficiência da colheita, qualidade e produção da prova (art. 3º).

Uma forma padrão de estrutura em uma Superintendência Regional da Polícia Federal contempla uma DELEPREV, onde tramitam vários inquéritos policiais de baixa ou média complexidade, e uma Força-Tarefa Previdenciária, onde tramitam as investigações de maior complexidade, tendo sido observados também casos onde um mesmo delegado atua nas duas áreas. Algumas investigações exigem um esforço investigativo maior, tanto pela complexidade da atuação dos criminosos, quanto pela necessidade de medidas judiciais invasivas, como afastamentos de sigilo (bancário, fiscal, telefônico, etc.), prisões ou medidas de busca e apreensão. Tais casos, atendidos alguns critérios internos da Polícia Federal, passam a receber a nomenclatura de ‘operações’. Assim, conceitualmente as operações são investigações feitas em inquéritos policiais que preenchem alguns critérios internos e, regra geral, englobam o cumprimento de medidas judiciais, como prisões e cumprimentos de mandados de busca e apreensão.

Por serem casos de grande complexidade e repercussão, é comum o cumprimento das medidas judiciais decretados no âmbito de operações policiais gerar interesse da mídia na cobertura dos casos. A esse respeito, Almeida (2019) avaliou a eficiência dos trabalhos investigativos realizados neste modelo, concluindo que as operações foram eficazes com relação à descoberta das autorias e comprovação dos crimes. Por outro lado, as investigações foram apenas relativamente eficazes em relação às condenações judiciais, especialmente em razão do extenso tempo de duração das investigações e das ações penais. As investigações analisadas por Almeida (2019) serão objeto de análise detalhada mais adiante neste trabalho, na busca para definição de uma rede básica de atuação das organizações criminosas investigadas.

Ainda em termos de estrutura disponível na PF, seu efetivo em 2018 era de 13.655 servidores, dos quais 2.676 nas carreiras administrativas e 10.979 policiais (Libório & Menezes, 2018). Do efetivo de policiais, vários ainda acabam sendo empregados em tarefas de polícia administrativa, como controle migratório, controle de armas e segurança privada, dentre outros, o que faz com que o efetivo empenhado na atividade-fim do órgão, a polícia judiciária (investigação e combate a crimes), seja ainda menor. Sob outro aspecto, em 2019 o Brasil passou a ser presidido por Jair Bolsonaro, que implementou mudanças que apontam para uma linha economicamente liberal a qual busca, de maneira geral, diminuir o aparato estatal e, conseqüentemente, o número de servidores públicos e, dentre estes, o número de policiais federais. Assim, caso se confirme a diminuição do efetivo, parece inafastável que haja impacto

negativo para o bom andamento dos trabalhos da PF, seja no combate a organizações criminosas ou nas demais atividades.

As atribuições da PF são bem amplas, abrangendo: tráfico ilícito de entorpecentes, contrabando/descaminho, polícia marítima, aeroportuária e de fronteiras, além dos crimes contra bens, serviços e interesses da União (art. 144 §1º da Constituição Federal do Brasil, 1988). O principal mecanismo para as investigações policiais, tanto em matéria previdenciária quanto nas demais, é o Inquérito Policial, disciplinado pelo Código de Processo Penal (Brasil, 1941). Diniz (2008) define o Inquérito Policial como sendo o “conjunto de diligências efetuadas pela autoridade policial, imprescindíveis para descobrir a verdade sobre um fato criminoso, suas circunstâncias e seu autor, e para apurar a responsabilidade do indiciado”, acrescentando que “é no inquérito policial que se podem colher dados que seriam difíceis de obter na instrução judiciária” (p. 925).

O Código de Processo Penal (CPP) determina que “todas as peças do inquérito policial serão, num só processado, reduzidas a escrito ou datilografadas e, neste caso, rubricadas pela autoridade” (art. 9º do CPP, Brasil, 1941). A respeito do procedimento, Tourinho Filho (2009) anota que, na entrada em vigor do Código, “praticamente não havia máquinas de escrever nas delegacias. Então, cabia ao escrivão ou à autoridade, de próprio punho, reduzir a escrito tudo quanto nele se fizesse. Hoje, entretanto, as peças do inquérito são datilografadas ou digitadas nas delegacias equipadas com computadores” (p. 73).

Anota Nucci (2008) que o inquérito policial é “procedimento formal, completamente burocratizado, pois exige peças escritas ou datilografadas, todas rubricadas pela autoridade competente” (p. 97). A regra do procedimento, ou seja, o Código de Processo Penal - CPP, foi criada em tempo que não havia sequer máquinas de datilografia nas delegacias. Assim, a modernização dos processos investigativos por meio do uso de novas tecnologias, como o uso de computadores, redes *on line*, uso de *big data*, ou mesmo a utilização de recursos da Análise de Redes Sociais - ARS via *software*, conforme abordada neste trabalho, deve se adequar às regras existentes. Mudanças legislativas tentando alterar o CPP tramitam há vários anos no Congresso Nacional, havendo atualmente mais de 250 propostas legislativas nesse sentido (Brasil, 2010). Ainda que as regras atuais não sejam consideradas adequadas, é preciso buscar formas de alcançar eficácia e efetividade nos procedimentos realizados pela PF, tarefa essa que motiva a realização deste trabalho.

2.3. Conexão e continência

Juridicamente existiu a preocupação de que evitar que dois processos que tivessem uma relação muito próxima fossem analisados de maneira separada, posto que tal situação poderia, dentre outras coisas, dar origem a decisões conflitantes. Imagine-se, por exemplo, a hipótese absurda de uma pessoa ser condenada como mandante de um crime e, em outro processo, decidir-se que o crime sequer existiu. Para tanto, foram criadas as figuras jurídicas da ‘conexão’ e da ‘continência’. O art. 76 do Código de Processo Penal – CPP (Brasil, 1941) define quando a competência será determinada pela conexão.

Art. 76. A competência será determinada pela conexão:

- I - se, ocorrendo duas ou mais infrações, houverem sido praticadas, ao mesmo tempo, por várias pessoas reunidas, ou por várias pessoas em concurso, embora diverso o tempo e o lugar, ou por várias pessoas, umas contra as outras;
- II - se, no mesmo caso, houverem sido umas praticadas para facilitar ou ocultar as outras, ou para conseguir impunidade ou vantagem em relação a qualquer delas;
- III - quando a prova de uma infração ou de qualquer de suas circunstâncias elementares influir na prova de outra infração.

Assim, a conexão visa unificar em um mesmo processo a análise de fatos cometidos por várias pessoas reunidas ou quando houver concurso de pessoas. Um dos exemplos disso seria uma organização criminosa cujos membros praticam várias fraudes em benefícios. Os atos, mesmo sendo diversos, são considerados como em concurso e devem ser analisados de maneira conjunta. Dessa forma, no caso concreto será possível avaliar se houve concurso formal, material ou crime continuado. Para a presente análise, importante apenas pontuar que os fatos conexos devem ser analisados de maneira conjunta.

Já o art. 77 do Código de Processo Penal – CPP (Brasil, 1941) define quando a competência será determinada pela continência.

Art. 77. A competência será determinada pela continência quando:

- I - duas ou mais pessoas forem acusadas pela mesma infração;
- II - no caso de infração cometida nas condições previstas nos arts. 51, § 1o, 53, segunda parte, e 54 do Código Penal.

Assim, a continência também serve para determinar se os membros devem ser investigados e julgados de maneira conjunta quando um mesmo crime é praticado por várias pessoas de uma organização criminosa.

Na Polícia Federal, quando o cometimento de um possível crime é noticiado, antes de ser determinada a abertura de inquérito policial ou outra providência, é realizada uma pesquisa nos sistemas internos a fim de verificar se os fatos ali narrados já estão sendo investigados em

algum inquérito policial ou se já foram objeto de algum inquérito policial já concluído. Não sendo identificada investigação em andamento ou já concluída, e feitas algumas outras análises, um inquérito policial é aberto para a investigação dos fatos.

Em regra, durante o andamento das investigações, não é feita uma nova pesquisa em busca de outros fatos conexos, o que pode acabar levando à ocorrência de investigações cuja conexão somente será identificada posteriormente. Imagine-se a seguinte hipótese: a) chegou a notícia que um indivíduo A possui um benefício previdenciário concedido mediante apresentação de documentos falsos. Não tendo sido identificada investigação em andamento, determinou-se a instauração do inquérito policial nº 1; b) no dia seguinte, chegou a notícia que um indivíduo B também possui um benefício previdenciário concedido mediante a apresentação de documentos falsos. Não tendo sido identificada investigação em andamento a respeito de B, determinou-se a instauração do inquérito policial nº 2; c) com o desenrolar das investigações, detectou-se que o benefício de A foi concedido pelo servidor C do INSS, na unidade APS nº 100, sem conferência dos documentos, e tendo A sido procurado pelo despachante D, que foi quem forneceu os documentos falsos; d) por outro lado, identificou-se que o benefício de B também foi concedido por C, na mesma APS nº 100, e também sem conferência dos documentos. Da mesma forma, B relata que quem forneceu os documentos foi D.

No caso ilustrativo parece haver elementos indicativos que, na verdade, existe uma mesma associação de pessoas (ou organização criminosa) responsável pelo cometimento das fraudes, tanto em relação ao benefício obtido por A, quanto no obtido por B. E que existem outras pessoas envolvidas, possivelmente o despachante D, e mesmo o servidor C, do INSS.

Ao imaginar-se uma delegacia pequena, onde há poucas investigações em andamento sob a responsabilidade de um mesmo delegado, parece crível que o responsável pelas investigações em algum momento consiga (por experiência profissional, boa memória, ou outra qualidade investigativa) fazer a conexão entre os fatos investigados. Ocorre que quando o volume de investigações aumenta, fazer tal análise mentalmente passa a ser improvável. Em uma das unidades da Federação onde foi feita a pesquisa de campo, denominada de UF2 (ver seção 4), existem cerca de 200 inquéritos em andamento a respeito de crimes previdenciários; na UF1 são cerca de 400; na UF4 são cerca de 600; e na UF3 são cerca de 1000. Isso significa que provavelmente na UF3 há vários delegados diferentes responsáveis por investigações previdenciárias. Além disso, existe a possibilidade de que as fraudes possam ter sido cometidas em cidades ou estados diferentes, o que faria com que uma unidade talvez sequer tivesse conhecimento da existência da investigação da outra.

Diante disso, parece essencial o aprimoramento da utilização de ferramentas informáticas para auxiliar na detecção de tais conexões. Com isso, poderia ser atendida a determinação jurídica-processual no sentido da reunião das investigações, e também aumentariam as chances de que todos os verdadeiros envolvidos nas fraudes fossem investigados. Voltando ao exemplo citado, caso os fatos fossem vistos de maneira isolada, provavelmente apenas os beneficiários A e B seriam responsabilizados. Com a verificação da conexão, seria possível também a responsabilização do despachante D e do servidor C, inclusive caracterizando associação criminosa (ou organização criminosa).

Sob o ponto de vista da administração pública, é possível falar em otimização de processos, e conseqüentemente em otimização de recursos, pessoas e tempo. Ora, se os fatos podem ser investigados por uma mesma equipe em apenas um processo, a existência de outra(s) equipe(s) investigando os mesmos fatos a partir de outro ponto de origem é desperdício de recursos por duplicidade. Um dos focos do presente trabalho é justamente identificar pontos de conexão em inquéritos policiais que permitam a identificação de investigações conexas para reunião e otimização dos esforços.

3. REFERENCIAL TEÓRICO

Esta seção apresenta aspectos gerais a respeito do conceito de organizações criminosas, trazendo elementos sobre origens, conceito legal e características. A revisão de literatura buscou identificar o conhecimento teórico existente a respeito da detecção ou predição de organizações criminosas por meio da Análise de Redes Sociais - ARS. O objetivo da revisão foi identificar a produção científica existente a respeito do tema a fim de servir de lastro teórico em três momentos: na compreensão das redes de operações já concluídas, na adequação do método para estudo das redes em investigações atuais e nas possibilidades/modelos de predição ou detecção de redes de grupos criminosos, atuais e futuras.

Assim sendo, foi feita pesquisa na base Scopus¹, buscando pelas expressões [(“*criminal organizations*” ou “*organized crime*”) E (“*prediction*” ou “*detection*”)], com filtro entre os anos 2000 e 2020, obtendo 265 resultados. Foi feita busca na base Google Scholar pelas expressões [“organizações criminosas” e “detecção” e “Análise de Redes Sociais”] e [“organizações criminosas” e “predição”], com filtro entre os anos 2000 e 2020, obtendo respectivamente 139 resultados. Foi feita ainda busca na base Google Scholar pelas expressões “Análise de Redes Sociais” (“*Social Network Analysis*”) e “polícia” (“*police*”), com filtros de publicações entre 2008 e 2018, em revistas de estrato A1 a B2, obtendo desta busca 31 artigos. Organizados os resultados foi feita análise preliminar sobre pertinência, tendo sido selecionados 95 dos resultados para leitura dirigida.

Desta forma, segue este referencial apresentado dados mais gerais sobre as organizações criminosas, como origem, conceito legal e características, seguidos da análise dos textos, que são divididos nas seguintes categorias: a) as redes e a investigação policial; b) redes em organizações criminosas; c) detecção e predição de organizações criminosas.

3.1. Origem das Organizações Criminosas

A expressão ‘*organized crime*’ foi inicialmente utilizada nos Estados Unidos em 1919 para caracterizar um conjunto um pouco indefinido de crimes que eram praticados no mercado ilícito que surgiu com a denominada Lei Seca (Gomes & Silva, 2015). Lima (2017) anota que as organizações criminosas representam uma ameaça séria à existência da própria sociedade e

¹ com utilização do software Publish or Perish versão 7.12

do estado democrático de direito, tanto pela gravidade dos crimes que cometem quanto pelo poder de influência que acabam exercendo dentro do próprio Estado.

Quando se aborda a ideia de organizações criminosas é difícil não lembrar da Máfia Italiana. A organização dessa Máfia começou tendo por base a estrutura familiar de seus membros, ganhando notoriedade algumas máfias como a *Cosa Nostra*, formada na região da Sicília, a *Camorra*, de Nápoles, e a *N'drangheta*, da Calábria, cuja forma de atuação começou restrita a crimes como contrabando e extorsão, passando depois a atuar no tráfico de entorpecentes e na lavagem de dinheiro e, por fim, passando a atuar na política “comprando votos e financiando campanhas eleitorais” (Lima, 2017:661). Outras organizações criminosas muito conhecidas são a japonesa *Yakusa* cuja atuação engloba o tráfico de drogas, exploração de prostituição, pornografia, jogos de azar, extorsão e tráfico de pessoas, composta exclusivamente por homens e com um código interno bastante rigoroso e a Tríade chinesa, fundada em 1911, também com estrutura hierárquica rígida e atuante no tráfico de drogas, exploração de prostituição e extorsão (Lima, 2017).

No Brasil, o primeiro grupo criminoso organizado apontado pela doutrina diz respeito aos cangaceiros de Virgulino Ferreira da Silva, conhecido como ‘Lampião’. Atualmente há outras organizações criminosas com atuação mais ampla e que foram formados dentro de presídios brasileiros como o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV). Em todas estas hipóteses parece haver elementos no sentido de que as organizações criminosas, em sua essência, guardam características semelhantes às organizações estudadas na administração, com a nada insignificante diferença que o objeto de atuação é contrário à lei.

Pontua-se ainda que as organizações criminosas afetam o seu habitat não apenas diretamente, cometendo crimes, mas também indiretamente, controlando negócios legais e ilegais, além de criar normas e desejos que guiam atitudes individuais em direção ao crime, conforme anota Marselli e Vannini (1997). Até mesmo o nível médio de educação dos políticos locais é elevando quando são implementadas estruturas legais-institucionais mais rígidas de combate às organizações criminosas, especialmente entre prefeitos e vereadores, que são aqueles que têm maior poder em nível local (Daniele & Geys, 2015).

3.2. Conceito legal das organizações criminosas

O sistema jurídico brasileiro adota em matéria criminal o sistema denominado positivismo onde, em síntese, as regras que serão utilizadas para punir uma determinada

conduta como crime devem estar expressamente previstas em lei. O sistema diverge, por exemplo, de países de origem anglo-saxônica onde é adotado o *common law*, em que as regras de conduta não estão expressas em lei, mas sim baseadas nos costumes. Por consequência disso, vigora no Brasil o chamado Princípio da reserva legal que resume claramente que não há crime nem pode haver punição se não houver previsão expressa em lei.

Seguindo tal raciocínio, tem-se que no Brasil era possível que pessoas membros de uma organização criminosa respondessem por um determinado crime da mesma forma como uma pessoa não ligada a qualquer organização criminosa. Um exemplo disso seria o de um criminoso, membro de organização criminosa, que comete um homicídio por determinação do comando da organização. Havia anteriormente previsão legal para punição pelo homicídio no Brasil, mas não havia previsão expressa para a composição de organização criminosa como um crime em si. E não havendo a definição jurídica do que é organização criminosa e a previsão de tal conduta como crime, não era possível a punição dos demais envolvidos.

A literatura internacional não possui um conceito claro e uniforme sobre o que é considerada uma organização criminosa (Crocker, 2019; Tayebi & Glasser, 2012), de forma que no presente trabalho adotaremos o conceito legal do termo no Brasil.

Até 1995 a expressão organização criminosa não possuía qualquer definição legal no Brasil. Começando a suprir a lacuna, foi editada a Lei nº 9.034/95 que, embora “definisse e regulasse meios de prova e procedimentos investigatórios referentes a ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo”, não previa expressamente o que caracterizava (ou diferenciava) cada uma das espécies citadas. Com vigência nessa época, o art. 288 do Código Penal (Brasil, 1940) previa expressamente o que era a “quadrilha ou bando” e havia previsão específica para “associações criminosas” atuantes no tráfico de entorpecentes na Lei 11.343/2006 (Brasil, 2006), mas não havia definição clara do que eram as organizações criminosas, de forma que não era possível o enquadramento (e conseqüentemente punição em termos penais) para a participação em organizações criminosas.

Faz-se apenas uma anotação neste ponto pois o Código Penal anteriormente previa o crime de “formação de quadrilha ou bando” caracterizada a conduta de “associarem-se mais de três pessoas, em quadrilha ou bando, para o fim de cometer crimes”. A Lei 12850/2013 posteriormente modificou ligeiramente a definição, e o crime passou a ser chamado de “associação criminosa”, definindo-se a ação do crime como sendo a de “associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes” (Brasil, 1940, art. 288).

Seguindo o raciocínio sobre as organizações criminosas, alguns anos depois a Convenção das Nações Unidas contra o Crime Organizado Transnacional (conhecida como Convenção de Palermo) abordou mais diretamente o tema. O conteúdo da Convenção foi internalizado no direito brasileiro por meio do Decreto 5015/2004 (Brasil, 2004) e dispõe no art. 2º que “grupo criminoso organizado” é:

Grupo estruturado de três ou mais pessoas, existente há algum tempo e atuando concertadamente com o propósito de cometer uma ou mais infrações graves enunciadas na presente Convenção, com a intenção de obter, direta ou indiretamente, um benefício econômico ou outro benefício material. (Brasil, 2004).

Com isso o Brasil avançou mais um pouco no combate às organizações criminosas. O Conselho Nacional de Justiça (CNJ) propôs a adoção do conceito ali estabelecido (Recomendação nº 3/2006 – CNJ, 2006), embora a utilização da previsão da Convenção de Palermo não fosse unanimemente aceita (nesse sentido, Lima, 2017, anota que ao admitir que um acordo internacional previsse um crime no Brasil seria entendimento contrário à garantia de que os crimes sejam apontados pelos representantes da população brasileira, o Congresso Nacional). Também no sentido de não ser possível a utilização da previsão contida na Convenção de Palermo, Gomes (2015) anota que “definições dadas pelas ou tratados internacionais jamais valem para reger nossas relações com o Direito penal interno em razão da exigência do princípio da democracia (ou garantia da *lex Populi*)” (p. 37).

Ante a relevância do tema, o Congresso Nacional passou a dar maior atenção às previsões legais a respeito de organizações criminosas, surgindo a Lei 12.694/2012 (Brasil, 2012). No dispositivo legal havia a previsão de formação de um júízo colegiado para o julgamento de crimes cometidos por organizações criminosas e também trouxe no art. 2º a previsão expressa do que era considerada uma organização criminosa:

Para os efeitos desta lei, consideração organização criminosa a associação de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com o objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de crimes cuja pena máxima seja igual ou superior a 4 (quatro) anos ou que sejam de caráter transnacional. (Brasil, 2012)

Embora a definição ali apresentada fosse expressamente caracterizada com a expressão “para os efeitos desta lei”, começava a ser incorporada no direito penal nacional um conceito mais preciso do que passaria a ser considerado como organização criminosa. Contudo, começou a haver divergência entre pesquisadores da área se o conceito de organização criminosa trazido pela lei 12.694/2012 poderia ser utilizado para os fins da Lei 9.034/95 anteriormente citada. De um lado, autores entendiam que deveria ser obedecido o que estava expressamente previsto na

Lei 12.694/2012 quando fala que a definição de organizações criminosas era para os efeitos daquela Lei (Nucci, 2013). De outro lado, havia autores defendendo que não fazia sentido uma lei (no caso, a Lei 12.694/2012) trazer um conceito de organizações criminosas que poderia ser utilizado para ocasionar um julgamento colegiado, mas que não poderia ser utilizado para a aplicação de medidas investigativas para combate às mesmas (medidas previstas na Lei 9.34/95). Nesse sentido estão, por exemplo, Lima (2017) e Pacelli (2013), que anota que “o conceito trazido no citado art. 2º da Lei 12.694/2012 fortalece e consolida a estrutura da organização criminosa apontada no art. 1º da lei 9.034/05” (p. 835).

A discussão acabou tendo curta duração posto que pouco tempo depois foi editada a Lei 12.850/2013, chamada pelos autores de nova Lei das Organizações Criminosas. A Lei nº 12.850/2013 trouxe em seu art. 1º §1º a previsão expressa do que passa a considerar como organização criminosa, fazendo-o nos seguintes termos:

Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional. (Brasil, 2013)

Comparando a previsão contida na Lei 12.694/2012 com a da Lei 12.850/2013, são observáveis algumas diferenças: a) passam a ser necessárias quatro ou mais pessoas (sendo que anteriormente eram três ou mais); b) o cometimento é de infrações penais (termo mais amplo que o anteriormente utilizado “crimes”, pois pode abranger, por exemplo, crimes de competência federal, estadual, militar, eleitoral, etc) com penas superior a quatro anos (antes eram aceitos crimes com penas iguais a quatro anos); c) a participação em organização criminosa passou a ser considerada um crime autônomo (o simples fato de pertencer a uma organização criminosa já passou a ser considerado crime).

Com relação à previsão de cometimento de crimes com penas superiores a quatro anos, Lima (2017) anota que, apesar de não ser uma regra escrita, a legislação criminal brasileira prevê alguns benefícios para quem comete crimes cujas penas não ultrapassem tal marco: podem cumprir a pena em regime aberto, ter a pena privativa de liberdade substituída por pena privativa de direito e prazo prescricional de oito anos (se a pena exceder a quatro anos, a prescrição ocorrerá em 12 anos). Dessa forma, os crimes com penas superiores a quatro anos são, de uma maneira sistêmica, considerados como de um grupo de crimes mais graves.

De fato, com a Lei 12.850/2013 (vigente no momento da elaboração deste trabalho), a participação em organização criminosa é prevista como um crime por si mesma. Assim, além

dos crimes cometidos pela organização criminosa, haverá para seus membros o cometimento de mais um crime. A previsão do art. 2º é a seguinte:

Art. 2º Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa:
Pena - reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas.

Assim sendo, no ordenamento jurídico vigente no Brasil (no momento da elaboração deste trabalho), está previsto expressamente em lei o conceito de organizações criminosas (art. 1º da Lei 12.850/2013) bem como da associação criminosa (art. 288 do Código Penal), sendo que a participação de pessoas na composição de organizações criminosas já é prevista como crime (art. 2º da Lei 12850/2013). Habib (2018) apresenta um quadro-resumo com as principais diferenças entre os dois crimes, como pode ser visto na Tabela 1.

Tabela 1

Distinções entre associação criminosa e organização criminosa

Associação criminosa	Organização criminosa
Exige-se o mínimo de 3 pessoas	Exige-se a reunião de, no mínimo, 4 pessoas
Destina-se à prática de crimes, independentemente da pena cominada	Destina-se à prática de infrações penais cujas penas máximas sejam superiores a 4 anos ou que sejam de caráter transnacional
Não se exige a divisão de tarefas entre os agentes para sua configuração	Exige-se que a organização criminosa seja estruturalmente ordenada e seja também caracterizada pela divisão de tarefas
Exige-se o especial fim de agir de cometer crimes	Exige-se como especial fim de agir o objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza

Fonte: Habib, 2018, p. 851.

A Lei 12850/2013 apresenta ainda várias outras características que, embora não sejam objeto da presente pesquisa, serão elencadas como simples complementação à abordagem: a) quem dificulta ou atrapalha a investigação de organizações criminosas recebe a mesma pena de quem participa diretamente da organização criminosa; b) a pena de quem comanda a organização é maior que a dos demais membros; c) as penas também são maiores em algumas condições como quando há emprego de arma de fogo, participação de criança/adolescente, se os crimes são transnacionais ou se há participação de funcionário público valendo-se desta condição para cometer o crime.

Trazendo um pouco das organizações criminosas para o contexto dos crimes contra a segurança social, tem-se que várias das investigações que resultaram em operações de combate a tais crimes tiveram como característica a participação de funcionários públicos no exercício da função como participantes do esquema criminoso. Algumas destas operações serão detalhadas adiante.

3.3. Características

Conforme visto, o conceito jurídico de organização criminosa é previsto na Lei 12.850/2013, compreendendo evoluções desde a previsão inicial contida na Lei 9.034/95. Com as definições de ambas, é possível traçar o seguinte quadro-resumo da Tabela 2.

Tabela 2

Comparativo entre as regras da Lei 9.034/05 e Lei 12.850/13.

Lei 9.034/95	Lei 12.850/13
a) 3 ou mais pessoas; b) existência há algum tempo; c) propósito de cometer crimes graves ou enunciados na Convenção de Palermo; d) intenção de obter direta ou indiretamente benefício econômico ou outro benefício material.	a) Associação de 4 ou mais pessoas; b) estruturalmente ordenada e caracterizada pela divisão de tarefas; c) objetivo de obter vantagem de qualquer natureza; d) prática de infrações cujas penas sejam superiores a 4 anos ou que sejam transnacionais

Fonte: compilação de dados das leis citadas.

Mais do que uma simples organização administrativa que atua com foco em um objeto ilícito, as definições administrativas de organizações podem ajudar a entender o conceito cunhado no mundo jurídico, onde a organização criminosa é formada por: a) quatro ou mais pessoas; b) estruturalmente ordenada; c) com divisão de tarefas, ainda que informalmente, d) com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza; e) mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

Com relação “às quatro ou mais pessoas” necessárias à caracterização da organização criminosa, Masson e Marçal (2018) anotam que é necessária não só a presença dessa quantidade de pessoas mas que essa reunião deve ser perene, estável, o que faz diferenciar o concurso de pessoas (a participação de mais de uma pessoa no cometimento de um crime, nos termos do art. 29 do Código Penal), sendo que a estabilidade e a permanência passaram a ser também

elementos necessários para caracterizar a ocorrência do crime de participação em organização criminosa.

Lima (2017) diferencia o que chama de crime organizado por natureza que são as punições dos crimes envolvendo a participação criminosa em unidades organizadas (seja pelo crime de participar de organizações criminosas, previsto na Lei 12850/2013 ou nos delitos de associação criminosa, previstos no art. 288 do Código Penal ou no art. 35 da Lei 11.343/2006, que prevê a associação criminosa para o cometimento de tráfico de entorpecentes) do crime organizado por extensão, que são os crimes praticados pelos membros das organizações criminosas. Assim, a participação na organização criminosa caracterizaria o crime organizado por natureza enquanto o tráfico de entorpecentes ou homicídios praticados pelos membros da organização criminosa são caracterizados como crime organizado por extensão. Quanto à “estrutura ordenada caracterizada pela divisão de tarefas”, Lima (2017) apresenta as principais características das organizações criminosas e anota que as:

Organizações criminosas geralmente se “caracterizam pela hierarquia estrutural, planejamento empresarial, uso de meios tecnológicos avançados, recrutamento de pessoas, divisão funcional das atividades, conexão estrutural ou funcional com o poder público, oferta de prestações sociais, divisão territorial das atividades ilícitas, alto poder de intimidação, alta capacitação para a prática de fraude e conexão local, regional, nacional ou internacional com outras organizações. Essa compartimentalização das atividades, expressada na elementar “divisão de tarefas”, reforça o sentido de estruturação empresarial que norteia o crime organizado. A divisão direcionada de tarefas costuma ser estabelecida pela gerência segundo as especialidades de cada um dos integrantes do grupo, a exemplo do que ocorre com o roubo de veículos, em que um agente fica responsável pela subtração, e outros por “legalizar o veículo” ou desmanche, falsificação de documentos ou revenda (p. 671).

O conceito jurídico das organizações criminosas parece convergir com a visão da administração sobre as organizações. A finalidade claramente definida² parece se alinhar à tipologia de Morgan (1996:24), segundo o qual “as organizações são entidades criadas para atingirem determinadas finalidades ou objetivos”. Além disso, a ideia de Morgan a respeito da organização como máquina, com a ênfase ao sistema mecanicista, parece ser perfeitamente correlacionável ao elemento de que a organização criminosa deve ser “estruturalmente ordenada e caracterizada pela divisão de tarefas”. No mesmo sentido, a visão de Etzioni sobre organizações abrange: a) unidades sociais (ou agrupamentos humanos); b) intencionalmente construídas e reconstruídas a fim de atingir objetivos específicos, posto que tais elementos estão presentes na concepção jurídica das organizações criminosas quando incluem a previsão de reunião de 4 ou mais pessoas assim como o objetivo específico de obter vantagem mediante o

² no caso das organizações criminosas de “obter vantagem de qualquer natureza”

cometimento de crimes. Desta forma, vislumbra-se o alinhamento do conceito jurídico das organizações criminosas com a visão da administração sobre as organizações.

Como forma de atacar as organizações criminosas, o HMIC³ (2005) sugeriu que em vez de utilizar técnicas caras como a vigilância, deveriam ser consideradas outras opções para atingir o cerne das organizações criminosas, mirando em ações proativas para processar os membros por crimes menos graves como fraudes em benefícios e comportamento antissocial. Abordando o texto do HMIC, Gilmour (2008) aponta que a criminalidade organizada pode ser dividida em três níveis⁴: Nível 1: interesse local, com criminalidade básica e comportamento antissocial, comandada por uma unidade básica de comando (UBC); Nível 2: interesses transnacionais, com ações de criminalidade organizada, grandes incidentes e eventos que afetam mais de uma UBC; Nível 3: envolvendo crimes graves e organizados, terrorismo ou outras atividades extremistas, operando em nível nacional ou internacional, podendo envolver casos graves com forte repercussão na mídia. No Brasil o conceito foi expandido falando-se atualmente no nível de “criminalidade organizada institucionalizada”, que é aquela praticada com o envolvimento de agentes públicos dos três Poderes, que atuam tanto na execução dos crimes, quanto com influência na criação de leis que protejam o esquema ou mesmo na interferência em julgamentos perante o Poder Judiciário (Pontes & Anselmo, 2019).

Embora seja clara a necessidade de combate ao mal produzido pelas organizações criminosas, a forma de executar tal atividade não é tão clara assim (Gilmour, 2008). A criminalidade organizada é tão gravosa que pode até mesmo afetar a estabilidade dos países, havendo lacunas de análises científicas acerca do problema e de ideias claras para estratégia e ideologia de combate às organizações criminosas em níveis legal, criminológico, forense e conceitos para identificação, detecção, investigação e prevenção à criminalidade organizada (Tokubayev, 2015).

Sob outro prisma, ao contrário das organizações criminosas, os pressupostos que norteiam a gestão nas organizações públicas, dentre elas as polícias, majoritariamente ainda se fundamentam numa visão estática de organização, com estruturas hierárquicas rígidas que dificultam o desenvolvimento de um pensamento “em rede”, dinâmico, capaz de se adaptar e readaptar a cada novo desafio. Esse descasamento de métodos de atuação entre as organizações criminosas e organizações públicas responsáveis pelas investigações torna mais difícil a ação do Estado na prevenção e repressão à atuação criminosa. (Augustinis, 2011)

³ Her Majesty's Inspectorate of Constabulary, que exerce uma espécie de controle externo das forças policiais na Inglaterra e País de Gales.

⁴ Classificação adotada pela SOCA – Serious Organized Crime Agency,

3.4. As redes e a investigação policial

Compreendido o conceito legal e características da atuação organizada de grupos criminosos, passou a revisão da literatura a observar como as redes formadas por tais grupos são percebidas sob o ponto de vista da investigação policial, eis que a análise de estruturas de grupos criminais organizados pode nos permitir obter informações valiosas sobre como esses grupos são organizadas, tais como seu tamanho, alcance e centralização (Sarvari et al, 2014), servindo até mesmo para a análise da implementação de políticas públicas (no presente caso, a política criminal e combate a fraudes), em interação com a gestão do conhecimento e a teoria da complexidade (Mischen & Jackson, 2008). Essa literatura servirá de lastro para o delineamento da rede básica de atuação de grupos criminosos que será feita adiante.

A literatura revisada aponta (Bright et al, 2015) que a Análise de Redes Sociais - ARS pode se prestar a auxiliar no mapeamento das redes criminosas e, identificando sua modelagem/padrão, permite melhor intervenção para dismantelar tais redes. E é nesse sentido que se pretende aplicar a ARS na compreensão dos casos estudados.

Formulando hipótese para dar apoio à investigação criminal, Petersen (2013) apresentam possibilidades para auxiliar na definição do foco de pesquisa para a criação de melhores processos, técnicas e ferramentas para auxiliar o trabalho policial na análise e tratamento do volume cada vez maior de informações que precisam ser processadas e analisadas. No trabalho, os autores exploram os desafios a serem enfrentados para que a informática possa ser melhor utilizada para apoio à investigação policial e, para tanto, apresentam um modelo de processo centrado no alvo (“*target-centric process model*”), cuja primeira prioridade é direcionar os problemas de uma maneira linear e introduzindo compartimentalização, ou seja, tentar fazer com que o processo investigativo obedeça a um processo de forma a evitar perdas de dados à medida que as fases vão avançando.

Analisando o modelo desenvolvido pelo Departamento de Polícia de Vancouver, Chang (2015) analisou o nível de maturidade de seus processos, avaliando os modelos analíticos utilizados por aquela força policial. Em linha similar, Chen et al (2018) analisam algoritmo de *machine learning* e métodos para detecção de operações suspeitas de envolvimento na lavagem de dinheiro baseada nas análises de vínculos, de modelagem de comportamento, de risco, detecção de anomalias e cruzamento de informações geográficas.

Analisando modelos de raciocínio sobre evidências legais (provas), Nissan (2012) pesquisou mecanismos de mineração de dados utilizados para produção de prova em casos de fraudes bem como para produção de informações de inteligência criminal ou para investigação. No artigo analisa uma ferramenta denominada “COPLINK”, desenvolvida pela Universidade do Arizona (EUA) e que se presta a identificar ligações entre atores de uma rede sob investigação. Segundo o autor, a ferramenta se mostrou como eficiente na identificação de ligações entre pessoas, embora o faça a partir de dados estruturados (ou seja, as informações tabeladas e já classificadas identificando previamente os dados dos atores. A observação é feita posto que há ferramentas que buscam a construção das redes a partir de dados não estruturados, por exemplo, notícias em jornais, conteúdos de depoimentos, periódicos, etc).

À medida que a organização e complexidade da atuação dos grupos criminosos aumenta, torna-se inevitável a utilização de ferramentas informáticas em apoio ao trabalho policial e, como anotam Chen et al (2004), “à medida que a complexidade dos crimes aumenta, ocorrem erros humanos, o tempo de análise aumenta e os criminosos têm mais tempo para destruir provas e escapar da prisão” (em livre tradução, p. 55).

Utilizando a teoria da estratégia e da influência para identificar elementos-chave em situações de combate, Pickett e Lingenfelter (2011) utilizam níveis de análise de redes para levantar hipóteses na busca de maior efetividade estratégica, testando como estas poderiam ter influenciado em situações reais de guerra, como as duas guerras mundiais e a guerra fria.

Sob outro ponto de vista, tem-se que as punições severas às organizações criminosas podem até fazer com que estas diminuam de tamanho, mas por outro lado fazem aumentar a efetividade de seus membros. Com a diminuição do tamanho das organizações, isso as torna mais simples e mais difíceis de detectar. Com isso, até mesmo uma punição menos severa pode ser um caminho a ser considerado para otimizar os resultados gerais no combate às organizações criminosas (Garoupa, 2007).

A ARS possui diversas aplicações, podendo ser utilizada para compreensão de redes de pesquisadores, para melhorar ambientes de trabalho ou para análise de grupos criminosos, conforme Zhao (2011). E esta última dimensão se pretende abordar no presente trabalho, eis que a ARS pode ser utilizada para a melhoria do trabalho de inteligência no auxílio ao trabalho policial (Duvenage, 2010). O grande desafio consiste em analisar o volume cada vez maior de informações a fim de extrair conteúdo útil (Sudhahar et al, 2015; Rasheed; Wiil & Niazi, 2015), sendo que uma das formas de realizar tal processamento é transformar as informações em uma rede onde é possível identificar os principais atores e objetos, verificando a relação entre estes.

Concentrando ainda mais o foco nas investigações policiais, Alzaidy (2010) aponta a necessidade de ferramentas que façam a mineração e classificação automatizadas de elementos de inteligência sobre redes criminosas para alimentar os bancos de dados da polícia e possibilitar o posterior cruzamentos destes, propondo metodologia que vise suprir tal lacuna. Exemplo de aplicação foi trazido por Cocx; Köster e Laros (2008), que estudaram um método de análise automatizada de carreira de criminosos, propondo a existência de um alinhamento da evolução das carreiras, de forma que é possível serem agrupados em plano bidimensional, permitindo visualização para análise dos desdobramentos possíveis.

Outro exemplo, apresentado por Tsetini (2015), verifica a utilização de perícia computacional para análise de crimes financeiros no caso concreto da empresa Enron (segundo a autora, um dos crimes financeiros mais complexos dentre as fraudes corporativas já observadas), verificando a rede de vínculos no sistema de e-mails daquela corporação.

Junto com outras providências, a ARS tem auxiliado no controle da criminalidade, conforme Martin e Rice (2011), abordando inclusive as limitações daquela para a compreensão de padrões criminosos. Contudo, além da produção, conforme Hollywood et al (2015) é necessário aprimorar a forma de compartilhamento de informações na aplicação da lei por várias agências e órgãos.

Outro exemplo de aplicação da ARS para análises criminais pode ser encontrado em Sarvari et al (2014), que mapearam uma rede com 43 mil endereços de e-mail de criminosos vazados na internet e, analisando a rede, mostrou que os criminosos são organizados em grupos fortemente conectados entre aqueles que aplicam golpes (*scammers*), podendo ser identificados os principais membros desses grupos, que contam com altas medidas de centralidade, de forma que ficam na posição central do gráfico e conectados a outros membros bem conectados na rede.

A compreensão das redes formadas por grupos criminosos apresenta dificuldades em relação às tradicionais análises de redes sociais, posto que os vínculos muitas vezes se apresentam de forma incompleta, incorreta ou inconsistente. Incompleta porque é usual nesse tipo de relação que os envolvidos operem de maneira secreta ou velada, incorreta porque muitas vezes a própria fonte de dados pode apresentar adulterações (como um criminoso que mente seu nome ou endereço quando abordado pela polícia) e inconsistente quando um criminoso é objeto de atenção de múltiplas forças policia, apresentando diversos registros e anotações que não necessariamente são consistentes entre si (Xu & Chen, 2005)

3.5. Redes de organizações criminosas

Feitas anotações a respeito da relevância da ARS para compreensão da forma de atuação de grupos criminosos, foram identificados trabalhos onde foi realizado o mapeamento de grupos criminosos complexos, como os observados nas máfias italianas. A compreensão da forma como foi feito o mapeamento daqueles grupos criminosos, em conjunto com a visão das redes no contexto policial, foram utilizados como base para o mapeamento das redes observadas nas operações já concluídas (que será apresentada adiante).

O ganho de eficiência interna (cooperação para sustentação da rede) de uma organização criminosa foi analisado por Baccara e Bar-Isaac (2008). A premissa-base é a de que o aumento do fluxo da informação interna em uma organização criminosa aumenta sua força, mas também aumenta o risco de comprometimento de um ou mais membros. Assim, as investigações sobre as redes de organizações criminosas podem ser divididas em dois grupos principais: a) detecção baseada em agentes, onde a probabilidade de detectar cada membro é independente de seu nível de cooperação e b) detecção baseada em cooperação, onde um agente nunca é detectado diretamente quando não está cooperando. Além disso, a estrutura das organizações criminosas como a Máfia ou organizações terroristas não dependem de interações com a estrutura de produção. Por fim as autoridades públicas, que normalmente miram em minimizar a extensão da cooperação, deveriam procurar maximizar a probabilidade de identificação de membros das organizações ou maximizar o número de membros detectados, anotando mecanismos que podem auxiliar em tal processo, a exemplo da clemência ou recompensas pela delação. (Baccara & Bar-Isaac, 2008).

Em contraponto, há quem defenda que mecanismos como a clemência e o *plea-bargain*⁵ não são efetivos em deter a atividade dos líderes das organizações criminosas (Garoupa, 2007), além do risco de que a delação leve a erros judiciais, como na experiência italiana que ficou conhecida como “caso Enzo Tortoza”, ocorrido na década de 1980, onde a delação por parte de membros da Nuova Camorra Organizzata levou à condenação injusta de inocente, conforme anotam Masson e Marçal (2018). Analisando a detecção de crimes do colarinho branco, Gottschalk e Smith (2016) apontam que estes são de difícil detecção. No caso das compras públicas, por exemplo, apesar de existirem mecanismos projetados para controlar e tornar transparente o processo de compras, a corrupção parece ser inerente às compras

⁵ Espécie de acordo onde, já no início do processo, o criminoso confessa a culpa em troca de diminuição da pena ou outro tipo de benefício, tornando o julgamento bem mais célere.

públicas desde que os governos começaram a comprar bens e serviços (p. 1), tendo analisado 390 criminosos de colarinho branco condenados na Noruega de 2009 a 2014 e apontando a importância dos denunciadores na identificação das fraudes/fraudadores, apesar de não haver qualquer tipo de recompensa para os denunciadores pelas leis da Noruega.

Dentre as famosas organizações criminosas citadas, a estrutura da rede formada pela máfia italiana *Cosa Nostra*, formada na região da Sicília, foi analisada por Musotto (2016), que utilizou o método de análise de redes para análise criminal, procurando identificar pessoas com maior poder de liderança naquela máfia italiana e com enfoque na distribuição geográfica dos componentes da rede, com mapas de calor indicativos para maior concentração de membros. Aquele trabalho mostra a importância da análise geográfica da distribuição dos membros de um grupo criminoso para perfeita compreensão de seu funcionamento e aplica um modelo (chamado '*Probit*') para analisar a probabilidade de que um membro tenha papel de liderança na rede.

Analisando também a rede criminosa da *Cosa Nostra*, Mastrobuoni e Patacchini (2012) utilizaram a análise de redes sociais para estudar as conexões entre os perfis criminais de cerca de 800 membros identificados daquela Organização entre as décadas de 1950 e 1960, mostrando por meio de medidas de centralidade conclusões que eram apenas conjecturas sobre o funcionamento da Máfia, apontando as características daqueles membros que possuem poder de liderança e como as relações familiares eram utilizadas para ganhar prestígio internamente (com casamentos internos e utilizando a mulher para ganhar centralidade, por exemplo).

Em outro caso, a empresa *Lockheed* foi acusada de fazer diversos pagamentos a oficiais estrangeiros para assegurar suas vendas mundo afora. A conduta de corrupção de servidores públicos para garantia das atividades foi comparada a uma ação de grupos organizados criminosos. Avaliando os pontos comuns entre os discursos de A. Carl Kotchian, presidente da *Lockheed*, e de Joseph Valachi, alto membro da *Cosa Nostra*, Albanese (1982) comparou pontos dos dois casos e apontou que ambos casos resultaram na mudança legislativa, mas que as novas leis ignoraram aspectos importantes do comportamento organizacional o que prejudicou seriamente sua aplicabilidade, sendo que a teoria geral das organizações era útil para explicar a má conduta das organizações em ambos os casos, sugerindo modelo para ajudar na predição de condições de mercado que predispõem as empresas a terem comportamentos ilícitos. Além disso, ambos os casos tratam de contextos em organizações, que praticam atividades ilícitas em um processo organizacional, com bases econômicas (uma para garantir vendas e outra para se proteger de inimigos em operações ilegais) situações estas que, aliadas a variáveis situacionais, ajudam a explicar o comportamento ilícito organizado.

Ainda sobre a *Cosa Nostra*, Moro (2016) aponta a alta relevância que os depoimentos de membros da organização tiveram para a compreensão do sistema como um todo. Tommaso Buscetta foi preso por tráfico de entorpecentes, Sammy “Bull” Gravano por homicídio e Mario Chiesa, político, por um esquema de corrupção e as colaborações destes foram de fundamental importância para a formação dos casos que resultaram no julgamento da organização criminosa (ainda que a colaboração tenha sido decorrente de estratégia da defesa). Aponta ainda Moro (2016) que o caso guarda semelhanças com o observado na denominada Operação Lava Jato, onde teria sido identificado quadro de corrupção sistêmica no Brasil e onde “o pagamento de propina tornou-se regra na relação entre o público e o privado”(p.1) e as ferramentas legais, como a colaboração premiada, foram fundamentais na descoberta do esquema criminoso.

Outra conhecida organização criminosa italiana é a *N'drangheta*, formada na região da Calábria, e cuja estrutura de rede foi analisada por Calderoni (2014) a partir de dados obtidos em operação policial com foco naquela organização denominada Operação Infinito. Anota Calderoni (2014) que as organizações criminosas tendem a ter estruturas mais agrupadas para reduzir os riscos de detecção e vazamento de informações, focando a análise daquele trabalho na co-participação dos membros nas reuniões (como *proxy* para descrever a rede de relações), concluindo que a rede ali observada é significativamente agrupada e que as comunidades estão parcialmente associadas à organização interna dos *N'drangheta* em diferentes localidades (fazendo tal associação quando um membro era identificado como parte de um ‘*locale*’, um grupo celular local, com hierarquia e organização). O tema da rede formada pela máfia *N'drangheta* foi revisitado por Calderoni (2017), que buscou a identificação de possíveis líderes locais (os *capobastone* ou *capolocali*), concluindo que os grupos locais não apresentam coesão estatisticamente significativa, o que é coerente com o observado na realidade, posto que se tratam de grupos abertos e com interação frequente entre seus membros, que se encontram para discutir atividades criminosas, problemas internos ou ainda para participarem de eventos sociais (como casamentos, jantares e celebrações). Assim, os trabalhos reforçam a importância dos diferentes grupos locais, mesmo todos fazendo parte de uma grande organização criminosa, além de mostrar como a ARS pode ser útil para a identificação dos líderes dos grupos criminosos.

Outro trabalho utilizando a ARS para estudar a rede formada pela *N'drangheta* foi realizado por Berlusconi (2016), que utilizou dados da Operação *Oversize*, que foi realizada entre os anos 2000 e 2006 e na qual foram alvo mais de 50 suspeitos de estarem envolvidos em crimes como tráfico internacional, homicídios e assaltos, sendo a maioria dos envolvidos identificados como sendo membros da *N'drangheta*, concluindo que a ARS pode auxiliar no

trabalho de inteligência policial e análise para investigações em andamento, identificando vínculos ocultos entre suspeitos.

No Brasil, o caso com maior repercussão onde identificou-se a utilização da análise de redes sociais foi o referente a operação de combate ao terrorismo denominada Operação Hashtag, conduzido pela Polícia Federal e deflagrada às vésperas dos Jogos Olímpicos de 2016 no Rio de Janeiro visando combater uma célula ligada ao grupo conhecido como Estado Islâmico. Nas investigações, foi identificada a utilização da comunicação por meio de redes sociais (Facebook) para divulgação de material terrorista e incentivo à filiação ao grupo Estado Islâmico, tendo sido feita a identificação dos vínculos entre os membros da célula atuante no país e resultando na “primeira sentença proferida na América Latina para punir o terrorismo islâmico”.(Chuy, 2018, p. 23).

Analisando as redes formadas por organizações criminosas em presídios brasileiros, Brandão (2015) analisou o caso do presídio de Alcaçuz, no Rio Grande do Norte, apontou a importância das redes formadas entre os que ali estão encarcerados citando, por exemplo, que presos supostamente ligados ao Primeiro Comando da Capital – PCC, utilizam da força para extorquir outros presos que ali estão. A organização criminosa PCC é citada também em outros trabalhos como sendo a responsável por resolver conflitos entre membros da própria organização e entre residentes das favelas (Cruz, 2013), promovendo ataques a policiais e guardas civis municipais (Cordeiro, Curado & Pedrosa, 2014), havendo casos onde “ações de controle do crime são negociadas em acordos mais ou menos velados, em que as atividades criminais geram insumos para as ações dos operadores do controle do crime” (Azevedo & Sinhoretto, 2017:197). Nas pesquisas a respeito do tema foram encontradas inclusive referências à ligação entre o PCC e a máfia italiana *N'drangheta* (Anesi, Rubino & Adorno, 2018; Fossati, 2020).

De outra banda, também foi observada presença de obras abrangendo a organização criminosa nacional denominada Comando Vermelho – CV, que seria responsável pelo controle do tráfico de entorpecentes em comunidades cariocas, realizando ataques a civis e possivelmente agindo em conjunto com o PCC (Toledo, 2011), agindo como se fosse o próprio Estado naquelas favelas como se tivesse legítimo monopólio do uso da força, além da cobrança por serviços como TV a cabo e internet (Soares, 2015). Anota-se que foi identificado pouca produção abordando de maneira científica organizações criminosas como o PCC e o CV, especialmente com relação às redes sociais nela observadas.

3.6. Detecção e predição de organizações criminosas

Na revisão foram buscados trabalhos que abordem a detecção e predição de atuação de grupos criminosos organizados. Essa parte da revisão de literatura serve como embasamento tanto para a detecção de redes em investigações em andamento, que será apresentada em seção própria adiante, quanto para a proposição de modelo de processo para predição de atuação de tais grupos.

Com as mudanças que ocorrem naturalmente nas sociedades, as organizações criminosas vão se adaptando às novas realidades e, com o dinamismo inerente às organizações informais, é necessário um sistema que seja capaz de se adaptar a elas (Gadekar, 2017). Assim sendo, necessário que se desenvolvam mecanismos que auxiliem na predição e detecção de organizações criminosas.

Em um dos estudos revisados, Van Vlasselaer et al (2013) utilizou a metodologia para investigação de fraudes contra o sistema previdenciário da Bélgica, inicialmente com o modelo denominado “*spider construction*”, que buscava a detecção de fraudes por empresas que intencionalmente deixavam de recolher as contribuições previdenciárias devidas. Nesse caso, a referência à teia de aranha ocorre porque as empresas envolvidas transferem recursos entre si, sendo que existem empresas “satélites” que declaram falência para não recolher as contribuições previdenciárias dos empregados, mas, na verdade, existe uma outra empresa-chave que é quem organiza toda a fraude. Analisando referido estudo, Gadekar (2017:452) viu como vantagem que “a enorme medição de dados adicionais pode melhorar os cálculos de aprendizagem padrão, sendo a parte mais difícil extrair dados relacionais de informações organizadas”. Por outro lado, o autor analisa vários métodos de possível detecção de fraude e aponta que “os métodos com melhor performance têm baixa precisão” e que “os métodos com melhor precisão sofrem com falta de robustez e eficiência no reconhecimento”⁶.

Um outro modelo de detecção, denominado ‘*Afraid*’, foi testado para verificação de fraudes, novamente contra o sistema de seguridade social da Bélgica (Van Vlasselaer et al, 2015). De acordo com a pesquisa, o novo algoritmo teria produzido melhoria de 15% em relação a modelos que fazem manualmente a análise para detecção de fraudes, o que aponta para o bom uso da tecnologia em favor do processo investigativo em combate a fraudes.

Em outra abordagem, Van Vlasselaer et al (2017) utilizou outro algoritmo denominado ‘*Gotcha!*’, também para análise de fraudes contra o sistema de seguridade social da Bélgica.

⁶ Livre tradução

De acordo com a nova pesquisa, o uso do novo algoritmo teria ampliado para 55% a detecção de fraudes, aplicando-se tanto a fraudes pretéritas quanto à predição de futuras fraudes por empresas (no mesmo sentido está a obra de Baesens, Vlasselaer & Verbeke, 2015). O modelo abordado no estudo apresenta avanço no sentido de mostrar que, na verdade, as fraudes costumam ser organizadas por uma outra empresa cujos vínculos com as empresas que praticam a fraude diretamente não é explícito. O modelo ‘*Gotcha!*’ foi analisado também por Mathimagal (2018), que procurou se aprofundar em questões como a dispersão da informação de vínculos em redes heterogêneas, algoritmos de paralelismo e otimização da análise de redes.

Observando conexões entre as premissas e resultados dos modelos descritos, é possível perceber que a concretização das fraudes passa por dois grupos de vinculação: um grupo com a vinculação explícita e outro com a vinculação oculta. Nos contextos descritos, havia a vinculação entre empresas que praticavam diretamente as fraudes (no caso, com a declaração de falência) mas havia também a figura de uma empresa-chave, que era a destinatária dos recursos e cuja vinculação com as demais era oculta. Trazendo a mesma lógica para as fraudes em benefícios, existem os beneficiários diretamente envolvidos, que são as pessoas que comparecem à Agência da Previdência Social para fazer o processo fraudulento mas devem existir outras pessoas chave, que são os destinatários reais dos recursos e que organizam toda a fraude (e, com isso, ficaria caracterizada a atuação organizada de pessoas para o cometimento de crimes, seja sob a forma de associação criminosa, seja sob a forma de organização).

Essa lógica se adequa ao encontrado na literatura no sentido de que os criminosos de baixo nível, ou seja, aqueles que fazem o “trabalho braçal”, têm probabilidade muito maior de serem presos e identificados, enquanto os de maior nível tendem a chamar menos a atenção. Contudo, o combate efetivo às organizações criminosas somente ocorre quando são identificados os membros mais influentes e de alto nível (Taha, 2019).

Na área dos crimes previdenciários, conforme será demonstrado, vários crimes são cometidos por meio da fraude de dados (como em inserções de vínculos inexistentes de emprego, contribuições, etc). Trazendo uma visão sobre a detecção de fraudes de dados, Lenz (2015) anota que tais fraudes ocorrem principalmente em quatro modalidades, que chamou de: espionagem, plágio, manipulação e fabricação de dados. Nesse tema, a internet abriu uma série de brechas que são aproveitadas pelos criminosos, de forma que não existe um detector de fraude de dados abrangente, e supostamente nunca haverá, devido à heterogeneidade das formas de se praticar fraudes, segundo Lenz (2015). Ainda sobre as novas possibilidades de fraudes eletrônicas, Leighton-Daly (2018) anota que o ambiente moderno que vivemos, com vários processos on-line e habilitado para tecnologia, facilita aos fraudadores não apenas roubando

informações, mas usando essas informações para obter uma vantagem financeira de outras pessoas, de maneiras que antes não eram possíveis.

A identificação de organizações criminosas por meio da Análise de Redes Sociais guarda viabilidade também pela análise das ocorrências policiais. Nessa linha, Tayebi e Glasser (2011; 2012) analisaram redes de coautoria⁷ (*co-offending networks*) e, partindo da análise computacional de dados do registro de ocorrências da polícia canadense, utilizaram como método a ARS aliada a técnicas de mineração de dados, para propor modelo computacional de análise de redes de coautoria, argumentando que seria virtualmente impossível obter tais informações utilizando os métodos tradicionais de análise. No artigo de Tayebi e Glasser (2012), o método foi dividido em quatro blocos: 1) modelagem dos dados de crimes e extração de rede coautoria (indicando lacuna conceitual entre o nível de dados e o nível de mineração); 2) um método de detecção de grupo, uma extensão do método de percolação de clique, para identificar a atividade do grupo ofensor; 3) um método de avaliação do crime para caracterizar o grupo como estrutura organizado (nos moldes da literatura criminológica); 4) um modelo de evolução de grupo para analisar o comportamento do grupo ofensor ao longo do ciclo de vida observável de um grupo. O presente trabalho utiliza metodologia similar baseada nos trabalhos de Tayebi e Glasser (2012; 2016), com algumas adaptações em razão do objetivo deste trabalho, conforme será descrito mais detalhadamente na seção de método. Aplicando a metodologia nos dados de ocorrências policiais da Província da Columbia Britânica, no Canadá, Tayebi e Glasser (2012) apontam terem sido identificados 35 grupos, tendo concluído pela probabilidade de 65% de que esses sejam grupos criminosos organizados.

Avançando no campo da predição de grupos criminosos, os mesmos autores Tayebi e Glasser (2016) abordaram a Análise de Redes Sociais como ferramenta de apoio ao policiamento preditivo. Anotam que a natureza dos grupos criminosos organizados é diferente de outros tipos de grupos como a amizade ou grupos de coautoria, sendo que as organizações criminosas geralmente têm um grupo bem estabelecido, explicitamente definido e estrito. Diferente dos grupos de amizade e de coautoria, os grupos criminosos também têm uma relação mais sistemática e organizada para atingir os objetivos de cometimento de crimes. Assim, a detecção de grupos criminosos organizados exige uma definição mais rigorosa da comunidade, sendo proposto algoritmo que será abordado na seção de método adiante. (Tayebi & Glasser, 2016).

⁷ Compreendidas como sendo formadas por pessoas que cometeram crimes conjuntamente.

Também na linha do policiamento preditivo, Borowik, Wawrzyniak e Cichosz (2018) mostram a utilidade dos algoritmos analíticos na previsão de crimes, que podem ser utilizados também em outras aplicações como análises criminais, criar perfis criminais e detectar tendências criminais, ajudando a, com base em observações do passado, otimizar o trabalho policial na prevenção de novas ocorrências. De outro lado, esse tipo de predição baseada em observações passadas traz consigo alguns riscos, como algoritmos enviesados, que podem perpetuar discriminações (Agarwal, 2018).

A fim de detectar e interromper a atividade de organizações criminosas transnacionais, Bahulkar et al (2018) utilizaram análises descritivas, preditivas e prescritivas a respeito da atuação em redes interdependentes de contrabando e de lavagem de dinheiro. Um ponto crítico apontado naquele estudo é que, embora sejam conhecidas informações parciais sobre as redes das organizações criminosas transnacionais, é provável haver conexões importantes e intencionalmente ocultas entre os criminosos, diante do que sugerem algoritmo para identificação das conexões faltantes, caracterização dos grupos criminosos e forma de abordagem para aplicação da lei. Aquele estudo concluiu que a análise preditiva pode ajudar a obter informações ausentes nos dados de redes sociais sobre as organizações criminosas, de forma que a combinação dos dados da comunidade com os das investigações policiais ajudará a entender as operações detalhadas das organizações criminosas.

Buscando uma forma de prever regiões com alta probabilidade de ocorrência de crimes e visualizar áreas propensas a crimes, Devan e Gangadharan (2014) abordam a análise e prevenção aos crimes de maneira geral, verificando formas de analisar os dados criminais por meio de sistemas computadorizados (com técnicas de mineração em dados não estruturados) para acelerar processos que ajudem a polícia na resolução de crimes.

Outra linha de abordagem para identificação ou detecção de redes de organizações criminosas por meio da análise de dados de telefones móveis ou de redes sociais abertas. Nessa linha, Ferrara et al (2014) apresentaram uma estrutura teórica para ajudar na caracterização de organizações criminosas reconstruídas a partir de metadados de registros telefônicos bem como para desvendar a estrutura subjacente das redes criminosas ocultas nos dados de comunicação. Assim, por meio da ARS aplicada às redes criminosas obtidas por meio da telefonia móvel seria possível identificar o fluxo de informações e os indivíduos que exercem os papéis-chave na rede criminosa ressaltando, contudo, que a caracterização das organizações não deve se limitar à análise dos dados telefônicos, devendo abranger também outras fontes tais como a verificação de encontros físicos entre os membros e transações financeiras.

Falando sobre formas como os governos e polícias podem melhorar sua eficácia na detecção precoce de ações de grupos criminosos organizados, Williams e Godson (2002) diferenciam a antecipação da predição, essa última considerada mais difícil. A antecipação, segundo os autores mencionados, é definida como uma preconcepção intuitiva, um conhecimento anterior, um pressentimento, ou seja, identificar elementos que indiquem aos governos e agências para estarem preparados para novas direções da criminalidade organizada. Com isso, governos e agências poderiam aprimorar suas capacidades e criar medidas preventivas ou repressivas (p. 314), propondo métodos e modelos para tal tarefa que levam em conta o tipo de ambiente em que o crime organizado floresce ou modelos sobre as maneiras pelas quais o crime organizado se comporta.

A identificação do comportamento anômalo, os estatisticamente chamados *outliers*, ganha contornos diferentes quando o objeto analisado são as organizações criminosas. Isso porque, em termos estatísticos, os *outliers* são normalmente tidos como ruídos e seria feita uma tentativa de eliminação de seus efeitos, ao passo que na atividade de investigação criminal o comportamento anômalo se torna relevante, posto que nesta se pretende associar incidentes criminais causados pelo mesmo grupo de pessoas e detectar comportamentos discrepantes (Lin e Brown, 2002).

Por todo o exposto neste referencial teórico, foi possível compreender como os textos científicos têm abordado as redes formadas por grupos criminosos organizados bem como compreender a forma como as pesquisas têm buscado modelos de detecção ou predição de tais grupos. A produção científica a respeito de grupos criminosos atuantes na área de fraudes ao sistema de seguridade social é escassa, especialmente quando se trata da análise de redes sociais formadas em grupos que fraudam benefícios sociais. Compreendidos os aspectos teóricos a respeito do tema, a próxima seção apresenta os aspectos metodológicos do presente trabalho, com as etapas em que a pesquisa será desenvolvida bem como os aspectos principais da ARS.

4. MÉTODO

O presente estudo visa descrever a estrutura de relacionamentos de redes de grupos criminosos em investigações anteriores (operações) da Polícia Federal sobre crimes previdenciários e propor um modelo de detecção/predição de redes de grupos criminosos em investigações atuais e futuras. Para atingir tal objetivo o método se baseou na Análise de Redes Sociais – ARS, utilizada inicialmente para descrever as redes de grupos criminosos organizados em sete operações de combate a fraudes previdenciária e que, no momento da pesquisa, já tinham a fase policial concluídas. Embora a ARS possa ser utilizada também como embasamento teórico, no presente trabalho optou-se por sua utilização como método em apoio ao referencial teórico baseado na predição ou detecção de organizações criminosas. Conforme visto no referencial teórico, o estudo das organizações criminosas sob a forma de redes é viável, sendo possível a identificação do tipo de relacionamento entre os membros das organizações criminosas e até mesmo a identificação de seus líderes ou membros mais relevantes, etapa de alta relevância na desarticulação e combate a tais grupos.

Com a análise das redes, buscou-se a identificação de uma rede básica que se aplicava a tais grupos criminosos, sendo delineado um algoritmo de detecção ou predição de tais grupos criminosos. Em seguida o algoritmo delineado foi testado em investigações em andamento e, para tanto, foram mapeadas as redes formadas em investigações em andamento em quatro diferentes unidades da Federação. Com os resultados dos testes, ao fim do trabalho é proposto algoritmo para a detecção ou predição de redes de grupos criminosos organizados em crimes previdenciários para ser utilizado em investigações atuais e futuras da PF.

Esta seção de método está dividida da seguinte forma: a) apresentação das Etapas da pesquisa; b) desenho da pesquisa; c) critério e seleção das operações já concluídas que foram analisadas; d) aspectos da ARS, subdivididos em conceitos, tipos de redes e variáveis; e por fim e) limitações dos dados e das análises.

A operacionalização da pesquisa empírica foi dividida em três etapas. A **Etapa 1** visou o levantamento e análise dos dados de operações de combate a crimes previdenciários já concluídas. A **Etapa 2** consistiu na verificação de elementos comuns entre as redes mapeadas na Etapa 1, delineando uma rede básica para as investigações já concluídas e proposta de algoritmo de detecção/predição de atuação de grupos criminosos. E a **Etapa 3** consistiu no teste do algoritmo proposto em investigações em andamento a respeito de crimes contra a Previdência Social, mapeadas em algumas unidades da Federação.

Na **Etapa 1** foi feito o mapeamento de operações de combate a crimes contra a Previdência Social já concluídas. Nesse ponto, anota-se que as investigações policiais visam, essencialmente, comprovar a efetiva existência de um crime e indicar quem é(são) seu(s) autor(es). A investigação pode ser concluída, regra geral, de duas formas: a) com um relatório do Delegado de Polícia ao Ministério Público e Juiz; b) com a deflagração de medidas ostensivas judicialmente autorizadas, como prisões, busca e apreensão, afastamento de funções públicas ou outras medidas cautelares, sendo elabora o relatório apenas após tais medidas. Embora existam regras internas específicas⁸, uma investigação geralmente é chamada de operação quando apresenta uma fase ostensiva conforme a segunda possibilidade acima, chegando ao conhecimento público. Dentre os motivos que levam a uma ou outra conclusão, Garbi (2019) realizou pesquisa com Delegados de Polícia Federal que conduziram operações e apontou que os principais motivos que mais levam à realização de uma fase ostensiva (e, portanto, a tratar uma investigação como operação) são, dentre outros, a gravidade do prejuízo e a participação de organização criminosa nos crimes.

Mesmo havendo uma fase ostensiva, as investigações são concluídas com um relatório do Delegado de Polícia responsável. Assim, os dados para o mapeamento foram obtidos a partir do relatório do Delegado de Polícia Federal responsável pelas investigações das operações analisadas. O mapeamento buscou identificar as pessoas que foram responsabilizadas pelos crimes, se foi apontada a participação de servidores públicos do INSS nos crimes, quantos e de que tipo foram os benefícios fraudados e quais os meios utilizados para o cometimento do crime. Nos casos onde constava o número do benefício fraudado, foram buscadas informações no caso concreto a respeito do servidor responsável pela concessão do benefício e Agência da Previdência Social onde o benefício foi concedido e onde era mantido.

Para cada operação analisada, foi feito um breve relato detalhando os meios utilizados para o cometimento das fraudes, apresentando-se a rede mapeada. A diagramação da rede foi feita importando os dados no software *IBM Analyst Notebook*. Com esse software foram realizadas análises estatísticas dos atores da rede, conforme variáveis detalhadas em seção própria adiante, sendo apresentadas tabelas com os principais atores da rede, com maior relevância no critério de Grau de Centralidade. Nesta Etapa, foram analisadas sete operações de combate a crimes previdenciários já concluídas até 2019, sendo mapeadas as redes observadas nessas investigações. Os critérios para seleção das operações utilizadas nesta etapa estão detalhados mais adiante.

⁸ Não detalhadas aqui por terem sido classificadas como informação sigilosa.

Na **Etapa 2** foram verificados os elementos comuns nas redes mapeadas na Etapa 1. A Etapa consistiu na observação direta das redes e, posteriormente, no delineamento de uma rede básica, sendo depois delineado algoritmo de detecção dessa rede básica. Como guia para o delineamento da rede básica, foi utilizado o algoritmo de Tayebi e Glasser (2016), que sugere, em resumo, a seguinte sequência de comandos lógicos: a) identificar os dados dos eventos criminais e o índice de gravidade dos crimes; b) contar a quantidade de incidentes criminosos num intervalo de tempo determinado; c) extrair as redes de coautoria e detectar grupos criminosos; d) calcular a atividade de cada um dos grupos criminosos identificados; e) identificar possíveis grupos organizados; e, por fim, f) avaliar o lucro obtido pelo grupo organizado.

Em resumo, na Etapa 2 as operações já concluídas, mapeadas na Etapa 1, foram analisadas para identificar, a partir dos elementos comuns, os elementos a serem utilizados na etapa “c” do algoritmo proposto, ou seja, qual ponto comum será utilizado para apontar as possíveis conexões entre os grupos criminosos.

Na **Etapa 3** foram definidos procedimentos para testagem do algoritmo de detecção e predição, apontado na Etapa 2. Para isso, foi feito o mapeamento de investigações em andamento (em 2019) em quatro unidades da Federação. Inicialmente foi realizado um levantamento de dados a respeito de investigações em andamento por meio de um sistema interno denominado Siscart – Sistema de Controle Cartorário. Foram avaliados aproximadamente 2250 inquéritos policiais, abrangendo todos os inquéritos policiais em andamento nas DELEPREV, bem como investigações em andamento nas delegacias descentralizadas, e registradas no Siscart como sendo crimes previdenciários.

A escolha das unidades da Federação para teste do algoritmo foi feita por conveniência, em razão da disponibilidade de acesso aos dados, totalizando 12 delegacias, sendo quatro localizadas nas Superintendências Regionais e oito em cidades do interior dos estados. As unidades da Federação onde foi feito o teste do algoritmo podem ser divididas em três categorias pela quantidade de investigações em andamento, sendo uma de pequeno porte (cerca de 190 inquéritos policiais), duas de médio porte (cerca de 450 e 600 inquéritos policiais, respectivamente), e uma de grande porte (cerca de 1000 inquéritos policiais), totalizando a amostra citada de aproximadamente 2.250 inquéritos policiais. A amostra representa aproximadamente 13% do total de inquéritos sobre fraudes contra a Previdência Social em andamento no momento da pesquisa (aproximadamente 17.200 inquéritos policiais). Em razão características inerentes à Análise de Redes Sociais os resultados não podem ser generalizados, ou seja, extrapolados para todo o universo.

Os inquéritos foram inicialmente classificados em três categorias: a) fraudes em custeio, b) fraudes em benefício ou c) outros. Para os inquéritos sobre fraudes em benefício foi feita ainda classificação com relação ao tipo de fraude/benefício fraudado (sendo os principais itens observados: aposentadoria, auxílio-doença, saque pós-óbito, benefícios da Lei Orgânica de Assistência Social - LOAS, pensão por morte e salário-maternidade).

Após essa primeira classificação, em cada unidade foram selecionados os inquéritos policiais que investigam fraudes em benefícios. O processo de coleta de dados foi feito em bancos de dados e *in loco*, com planilhas preenchidas pelo próprio pesquisador. Para cada unidade da federação o processo foi replicado, tendo sido obtidas inicialmente informações gerais a respeito das investigações em andamento, como o número dos inquéritos policiais e unidades vinculadas. Nessa etapa, foram considerados para análise todos os inquéritos em andamento na Delegacia de repressão e combate a crimes previdenciários da Superintendência Regional da Polícia Federal na Unidade da Federação, bem como todos os inquéritos policiais assinalados como de matéria previdenciária em andamento em todas delegacias descentralizadas (localizadas em cidades do interior) da Unidade da Federação. Para cada inquérito de fraudes em benefício, foi(ram) buscada(s) o(s) benefício(s) possivelmente fraudado(s) e que está(ão) sob investigação. Para cada benefício identificado foram buscadas informações em sistemas disponíveis sobre o servidor do INSS responsável pela concessão/habilitação do benefício e Agência da Previdência Social onde o benefício foi concedido e onde era mantido no momento da consulta.

Com todos os dados estruturados, foi feita a descaracterização dos dados a fim de não permitir a identificação dos envolvidos, posto que se trata de investigações em andamento, sigilosas nos termos do art. 20 do Código de Processo Penal (Brasil, 1941). Neste ponto, os dados das quatro unidades da Federação foram organizados e ganharam códigos próprios. Assim, cada **inquérito policial** ganhou um código **IPL1, IPL2, IPL3** etc; cada **Número de Benefício** possivelmente fraudado ganhou um código **NB1, NB2, NB3** etc; cada **Servidor** do INSS citado ganhou um código **Servidor1, Servidor2, Servidor3**; cada **Agência da Previdência Social** ganhou um código **APS1, APS2, APS3** etc; cada **pessoa** citada (envolvida no inquérito ou titular de benefício) ganhou um código **Pessoa1, Pessoa2, Pessoa3** etc.

Os dados foram então importados para o software *IBM Analyst Notebook*, próprio para diagramação e Análise de Redes Sociais. Na diagramação os atores foram representados com ícones próprios (ícones do próprio software) e vínculos. Essa modelagem seguiu uma lógica jurídico-investigativa, definindo-se o vínculo entre o inquérito policial e o benefício investigado

representando com vínculos simples, e a partir do benefício foi representando vínculo direcional para o servidor responsável e agência de concessão.

Após a importação dos dados no software *IBM Analyst Notebook*, foram realizadas as análises estatísticas disponíveis no software, tendo as redes sido organizadas primeiramente da forma “compacto em leque” (opção disponível no software) sendo, contudo, algumas delas rediagramadas para melhor visualização de pontos específicos, por exemplo, a vinculação dos benefícios fraudados a um determinado servidor ou APS. Mapeadas as redes, a primeira avaliação foi por observação direta, feita a partir de uma visão geral da rede, procurando identificar: a) a rede principal (com maior número de atores conectados), b) redes de subgrupos que não se conectam à rede principal, c) agrupamentos de vínculos que se destaquem na rede. Neste ponto, as redes do subgrupo formadas por inquéritos policiais com maior número de vínculos e que se destacaram foram analisadas individualmente.

Foi então feita a análise dos atores a partir das estatísticas do software. Os dados foram ordenados de maneira decrescente, utilizando como ordem o valor obtido na variável “grau” (grau de centralidade). De acordo com a classificação de Wassermann e Faust (1994), as redes formadas nos inquéritos policiais podem ser classificadas como do tipo duo modal, posto que apresentam conjuntos diferentes de atores. A análise da centralidade de grau se mostrou como relevante para a compreensão da rede na medida em que atores com maior centralidade de grau possuem mais visibilidade na rede e possuem contato direto ou são adjacentes a outros atores (Wasserman & Faust, 1994), sendo que a centralidade de um ator não é dada apenas pela quantidade de vínculos que possui, mas “pela quantidade de ligações que seus conectados apresentam” (Brand & Verschoore, 2014, p. 219).

Em razão do grande número de atores em cada rede, em cada unidade da federação foram identificados os dez primeiros resultados tanto para os servidores com maior grau de centralidade quanto para as Agências da Previdência Social. Para cada um destes foi destacado um subgrupo da seguinte forma: a) no software é selecionado o ator (Servidor1, por exemplo); b) a partir dele são selecionados os vínculos e extremidades a ele relacionados; c) são selecionados os vínculos e extremidades a partir de todos os atores no item anterior; d) todos estes atores e vínculos são exportados para um novo diagrama, reorganizados de forma “compacta em leque” (opções disponíveis no software).

Os resultados de todas estas redes do subgrupo constam dos apêndices deste trabalho (Apêndice I com os subgrupos da UF1, Apêndice II com os subgrupos da UF2, Apêndice III com os subgrupos da UF3 e Apêndice IV com os subgrupos da UF4). Esse mapeamento inicial foi utilizado como base para análises gerais das unidades, tendo se mostrado útil especialmente

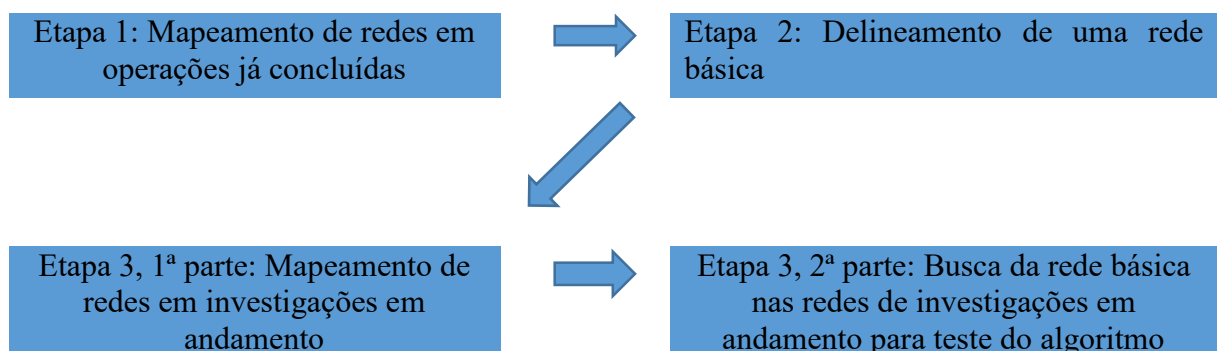
para a detecção de grupos criminosos existentes em investigações em andamento, tenham resultado de operações ou não. Essa detecção de grupos nas operações em andamento tem muita utilidade prática pois pode servir de base para a vinculação de novas notícias de crime recebidas com grupos que já estão sob investigação, evitando a instauração de inquéritos independentes para investigações sobre um mesmo grupo criminoso.

Com os resultados obtidos na Etapa 2, foi feita aplicação do algoritmo ali proposto, sendo obtidas novas redes seguindo a lógica da busca por díades formadas pelos atores APSxx-Servidorxx, que se conectam a um outro conjunto de atores, os inquéritos policiais. Em outras palavras, foi feita a identificação das díades APSxx-Servidorxx, identificando-se o total de números de benefícios sob investigação (NBs) vinculados a tais díades bem como o número de inquéritos policiais (IPLs) onde estes NBs estão sob investigação. De acordo com os critérios da ARS, entende-se que essas redes formadas pelas investigações em andamento com base na lógica da Figura 2 (ver seção 5.1) se adequam melhor à ideia de redes diádicas por afiliação (*dyadic two-mode network*; Wassermann e Faust, 1994). São apresentados como resultados: a) os quantitativos de grupos criminosos potencialmente identificados; b) a quantidade de eventos aos quais estão vinculados, ou seja, a quantidade de inquéritos policiais relacionados; c) o percentual de possíveis conexões em relação ao total de investigações em andamento.

4.1. Desenho da pesquisa

Detalhadas as etapas de realização da pesquisa, estas podem ser concatenadas apresentando a lógica do presente trabalho, modelado conforme fluxo apresentado na Figura 1.

Figura 1. Fluxo da pesquisa



4.2. Seleção das operações concluídas

Na pesquisa realizada a respeito de investigações de combate a fraudes previdenciárias, identificou-se o trabalho de Almeida (2019), onde foi feita análise sobre a eficácia de operações policiais de combate a fraudes previdenciárias, abordando 20 operações deflagradas entre 2003 e 2018 realizadas pela Delegacia de Repressão a Crimes Previdenciários no Maranhão e para as quais já foi oferecida denúncia pelo Ministério Público perante o Poder Judiciário. Como as operações ali mencionadas já possuem análise sobre sua eficácia, buscou-se os relatórios das mesmas para servir de base para o delineamento de uma rede básica das redes ali formadas.

Para definição das operações analisadas para a delineamento da rede básica, optou-se pela utilização do processo de saturação teórica dos relatórios mais recentes com base nos meios utilizados para realizar as fraudes, por entender-se que, por silogismo, investigações que identificam meios semelhantes de cometimento de fraude apresentariam características mais homogêneas entre si. Da análise dos relatórios foram identificados os seguintes meios: a) pessoas fictícias como beneficiários, ou seja, pessoas que só existem nos sistemas de identificação ou do INSS, por exemplo, com RG falso; b) pessoas fictícias como instituidores de benefício, com simulação de morte da pessoa fictícia para gerar benefício de pensão por morte; c) tipificação da atuação em grupo como associação criminosa; d) pessoas de um mesmo núcleo familiar como indiciados; e e) processo físico inexistente na agência do INSS onde o benefício foi concedido, isto é, os dados só existiam no sistema, sem documentos que o lastreavam. A Tabela 3 mostra uma classificação das sete operações utilizadas no estudo com base nos meios utilizados para fraudes.

Tabela 3

Meios utilizados para fraudes nas operações

Operação	Pessoa fictícia como beneficiário	Pessoa fictícia como instituidor	Associação criminosa tipificada	Envolvimento de servidor do INSS	Pessoas do mesmo núcleo familiar indiciados	Processo físico inexistente na APS	Vários benefícios no mesmo endereço
Fim de Linha	X		X	X	X		
Casa Cheia	X			X		X	X
Casa Cheia II			X		X		
Intervenção		X			X	X	X
Intervenção II	X			X			X
Aquestos	X			X	X		
D. Fratres II	X		X		X		X

Fonte: compilação de dados dos relatórios das investigações

O último item observado foi a utilização de pessoas fictícias como instituidor de benefício e não como titular do benefício. Como titular, o criminoso “cria” uma pessoa virtualmente e muitas vezes arruma documentos falsos com os quais, por exemplo, abrem uma conta no banco a partir da qual recebem o valor do benefício no lugar da pessoa inexistente. Já como instituidor, a pessoa fictícia é cadastrada como contribuinte do INSS e tem sua morte simulada, passando a gerar um benefício de pensão por morte para o cônjuge sobrevivente. Entendendo saturada a amostra, foram feitas mais duas observações sem terem sido observados outros meios ou ardis para o cometimento dos crimes.

4.3. Análise de Redes Sociais - ARS

Uma das técnicas mais utilizadas nas ciências sociais para se identificar e descrever vínculos e conexões entre diferentes atores sociais consiste na Análise de Redes Sociais (ARS), com uso policial e/ou de inteligência em órgãos como os norte-americanos Federal Bureau of Investigation (FBI) (Johnson et al, 2013) e National Security Agency (NSA) (NSA, 2016), e a British Police (Gunnel, Hillier & Blakeborough, 2016). De fato, conforme apontado no referencial teórico, a ARS provou ser uma ferramenta valiosa para o estudo de grupos criminosos, ajudando a verificar os membros centrais das redes criminosas, a existência de subgrupos, as interações entre indivíduos e subgrupos, o fluxo de informações na rede, os membros sensíveis e / ou relações cuja remoção poderia eventualmente levar à destruição da rede (Ferrara et al, 2014). Nessa linha, a utilização da ARS pode ajudar na compreensão da forma de atuação de organizações criminosas na área previdenciária, sendo o método escolhido para ser utilizado no presente trabalho.

A forma como os indivíduos ou atores se relacionam é objeto de estudo de várias áreas da ciência. Sua grande relevância foi resumida de maneira clara por Collins (1988), segundo o qual a vida social é relacional e é somente porque brancos e negros agem de uma certa forma quando se relacionam que o conceito de “raça” se torna uma variável importante, e é o padrão de relação em torno das pessoas de diferentes raças que faz com isso se torne importante⁹. Por tal relevância, toma-se neste trabalho a Análise de Redes Sociais como embasamento para a análise do cenário que será na sequência descrito.

⁹ No original: “Social life is relational; it is only because, say, blacks and whites occupy particular kinds of patterns in network in relation to each other that “race” becomes an important variable. To regard race as a cause of social mobility is misleading, since it is really the pattern of network connections around persons of different races that makes this trait significant” (Collins, 1988, p. 413).

A Análise de Redes Sociais (ARS) guarda relação inerentemente interdisciplinar, envolvendo a teoria social, a matemática, a estatística e a informática e englobando teorias, modelos e aplicação que são expressas em termos de conceitos relacionais ou processos. Assim, a noção de grupo social pode ser vista vários aspectos, podendo ser: uma Ator gráfica e suas generalizações; a noção de uma comunidade que interage; um círculo social e sua estrutura de afiliações; isso sem incluir a noção matemática dos grupos. Do ponto de vista da Análise de Redes Sociais, o ambiente social pode ser expresso como padrões ou regularidades nas relações entre unidades que interagem, o que se denomina de estrutura. Essa relação entre os atores, definida como laço entre as unidades, é um componente fundamental da teoria de redes. Do ponto de vista da Análise de Redes Sociais, os atores e suas ações são vistos como interdependentes em vez de unidades autônomas, independentes e os laços relacionais entre os atores são canais para transferência ou fluxo de recursos (sejam materiais ou não-materiais). (Wasserman & Faust, 1994).

Dado um conjunto de atores, a Análise de Redes Sociais pode ser utilizada para estudar a medida das variáveis estruturais dos atores no conjunto. A estrutura relacional de um grupo ou de um sistema social mais amplo consiste no padrão de relacionamentos entre os atores. O conceito de rede enfatiza o fato que cada indivíduo tem ligação com outros indivíduos, podendo estar ligados a um, alguns ou muitos outros indivíduos. A expressão “rede social” se refere ao conjunto de atores e ligações entre eles. A análise da rede vai procurar modelar essas ligações para descrever a estrutura de um grupo, a partir da qual poderá ser estudado o impacto dessa estrutura no funcionamento do grupo ou a influência dessa estrutura nos indivíduos do grupo (Wassermann & Faust, 1994, p. 9).

4.3.1 Conceitos

Os principais conceitos da Análise de Redes Sociais que serão utilizados no presente trabalho utilizam como base as definições de Wasserman e Faust (1994), entendendo-se relevante pontuar os seguintes conceitos:

Atores (também chamado de “nós”). Atores são indivíduos, corporações ou unidades sociais coletivas. Exemplos de atores são pessoas em um grupo, departamentos dentro de uma corporação, agências de serviços públicos em uma cidade ou países no sistema mundial. (Wassermann & Faust, 1994, p. 17). Os atores não são observados individualmente ou por suas características, mas na sua relação com os demais atores da rede.

Atributos. São adjetivos ou características dos atores, como a idade, formação ou a instituição a que está vinculado, dentre outros (Bez, Faraco & Angeloni, 2010). Indivíduos possuem atributos pessoais e a ARS se preocupa com a forma que tais atributos (raça, gênero ou educação, por exemplo) interferem nas relações entre os atores, observando como estes mudam suas respostas em relação uns aos outros conforme mudam ou se assemelham os atributos (Marin & Wellman, 2011)

Ligação (também chamado “laço relacional” ou “aresta”). Indivíduos são conectados uns aos outros por laços invisíveis formando uma rede de conexões, como uma rede de pesca ou da mesma forma que um longo pano é formado pelo entrelaçamento dos fios (Scott, 1988). Os atores são ligados uns aos outros por meio de laços sociais. A característica que define uma ligação é estabelecida pela conexão entre um par de atores. Alguns dos exemplos comuns de ligações empregados na análise de redes, conforme Wassermann e Faust (1994), são os seguintes:

- Avaliação de uma pessoa por outra (por exemplo, amizade ou respeito);
- Transferência de recursos materiais (por exemplo, transações comerciais ou empréstimo de coisas);
- Associação ou filiação (por exemplo, pessoas em um evento social ou pertencentes a um mesmo clube social);
- Interação comportamental (por exemplo, mandar mensagens);
- Movimento entre lugares ou status (por exemplo, migração, mobilidade física ou social);
- Conexão física (por exemplo, uma rua, um rio, ou uma ponte conectando dois pontos);
- Relações formais (de autoridade);
- Relação biológica (afinidade, parentesco ou descendência).

Mais do que os atributos dos atores, o analista de redes sociais procura observar as relações entre os atores (Prell, Hubacek & Reed, 2009), sendo que a força da ligação entre os atores é uma combinação de tempo, intensidade emocional, intimidade e serviços recíprocos (Granovetter, 1973).

Díade. No nível mais básico, é a ligação ou relação estabelecida entre dois atores, representando a menor estrutura social, com a relação entre dois atores (Scott & Carrington, 2011). A ligação é uma propriedade do par e, conseqüentemente, não é considerada como

pertencente a um único ator. Uma díade consiste em um par de atores e possíveis ligações entre eles (Wassermann & Faust, 1994);

Triade. Relações entre subconjuntos maiores de atores também podem ser estudadas. Nesse caso, as análises focam em tríades, que são um subconjunto de três atores e as possíveis ligações entre eles. Há interesse particular em saber se as tríades são transitivas (se o ator *i* gosta do ator *j*, e o ator *j* gosta do ator *k*, então o ator *i* também vai gostar do ator *k*) ou se a tríade é balanceada (se os atores *i* e *j* gostam um do outro, então *i* e *j* devem ser similares nas avaliações que tem de um terceiro ator *k* e, se *i* e *j* não gostam um do outro, eles devem diferir na avaliação de um terceiro ator *k*). (Wassermann e Faust, 1994, p. 19);

Subgrupo. Um subgrupo é um subconjunto de atores e todas as ligações entre eles. Localizar e estudar subgrupos utilizando critérios específicos tem sido uma preocupação importante na Análise de Redes Sociais. (Wassermann & Faust, 1994);

Grupo. O poder da análise de redes está na habilidade de modelar as relações entre sistemas de atores. Um grupo é definido pela interação entre seus membros (Scott & Carrington, 2011), sendo que o grupo é um conjunto de atores cujas ligações serão mensuradas, devendo ser possível argumentar que esses atores fazem parte de um conjunto mais ou menos delimitado, fazendo parte de um conjunto finito de atores limitado por razões conceituais, teóricas ou empíricas e cujas medidas da rede serão tomadas. (Wassermann & Faust, 1994);

Como os atores podem fazer parte de grupos diferentes dentro de uma mesma rede, isso pode acabar levando a um superdimensionamento da amostra (Marin & Wellman, 2011), razão pela qual a restrição quanto a um número limitado de atores é um requisito analítico. Não é possível imaginar as ligações se estendendo até um grupo infinito de atores, o que tornaria impossível realizar a análise dos dados de tal rede (Wassermann & Faust, 1994);

Relação. O conjunto de ligações de um tipo específico entre membro de um grupo é denominada relação. Por exemplo, as amizades entre pares de crianças em uma sala de aula ou o conjunto de ligações diplomáticas formais mantidas por pares de países são definidas como relações. Para um grupo de atores, devemos medir todas as diferentes relações (no caso das relações diplomáticas, podemos medir o volume de negócios entre cada par de países). Importante notar que a relação se refere a um conjunto de ligações de um determinado tipo com medidas específicas para cada par de atores. Essas ligações só existem entre pares específicos de atores. (Wassermann & Faust, 1994);

Redes sociais. As redes sociais são compostas por um grupo relevante de atores conectados por uma ou mais relações (Marin & Wellman, 2011). Definidas as ideias de ator, grupo e relação, as redes sociais podem ser definidas como sendo o(s) agrupamento(s) finito(s)

de atores e a(s) relação(ões) entre eles. A presença da informação relacional é crítica e definidora da rede social. (Wassermann & Faust, 1994). As redes sociais são formadas por um conjunto de atores, um conjunto de relações entre pares de atores e possíveis atributos dos atores ou dos vínculos (Katsaros, Dimokas & Tassiulas, 2010);

Dados de redes. Os dados de redes sociais são constituídos de pelo menos uma variável estrutural medida em um conjunto de atores. A grande questão é identificar quais variáveis serão medidas e quais técnicas são mais apropriadas para fazer tal medida. Para a análise das transações comerciais entre países, as técnicas de observação direta trarão dificuldade de aplicação, sendo provavelmente mais fácil fazer a análise a partir de dados de arquivo sobre as transações. De outro lado, a amizade entre pessoas pode ser melhor analisada mediante questionários ou entrevistas do que usando dados de arquivo ou históricos. Assim, é a natureza do estudo que determina qual o conjunto de atores que será pesquisado e qual a amostra que deverá ser colhida. (Wassermann & Faust, 1994);

As variáveis estruturais são medidas em pares de atores e compõem a pedra fundamental da análise de dados de redes sociais. As variáveis estruturais medem as ligações de um tipo específico entre pares de atores. Por exemplo, as variáveis estruturais podem medir as transações entre corporações, amizade entre pessoas ou negócios entre países. (Wassermann & Faust, 1994). A centralidade é vista como a localização estratégica de um ator em determinada rede (Katsaros, Dimokas & Tassiulas, 2010). Segundo Freitas e Pereira (2005), atores com baixa centralidade são periféricos na rede, sendo que se estes forem removidos não fazem efeitos significativos na rede. Uma rede altamente centralizada é caracterizada por ter um ou poucos atores centrais que concentram a maior parte das ligações, ajudando a formar grupos e servindo de base para ações coletivas tendo, por outro lado, desvantagens para relações de longa duração ou soluções de problemas (Prell, Hubacek & Reed, 2009).

4.3.2 Tipos de redes

O modo da rede diz respeito ao conjunto de atores cujas variáveis serão medidas. As redes monomodais (ou redes de um-modo) tem as variáveis estruturais medidas em relação a um conjunto de um só tipo de atores, sendo este o tipo mais comum de redes (Bez, Faraco & Angeloni, 2010). Neste tipo de rede cada ator pode, ou não, ligar-se com outros atores da sua rede, ou seja, um ator pode alcançar qualquer outro ator. Um exemplo seria de uma sala de aula em que a amizade determina o tipo de relação. Nas redes monomodais, as relações medidas são usualmente vistas como representando uma conexão específica. Essa medida, tomada no nível

de pares de atores, pode ser de muitos tipos podendo ser principalmente vistas como atitudes, papéis e transações. (Wassermann & Faust, 1994, p. 37).

Em outros tipos de redes, as variáveis estruturais são medidas em dois ou mais conjuntos de atores. Os dados da rede que contém os dois conjuntos de atores formam uma rede duomodal (ou rede de dois-modos), conforme definição de Wassermann e Faust (1994). A medição de dados das redes duomodais podem envolver: a) de dois conjuntos de atores (ou redes duomodais diádicas) ou b) de um conjunto de atores e um conjunto de eventos (ou redes de afiliação). Em outras palavras, as redes monomodais envolvem as relações entre um grupo de atores similares enquanto as redes duomodais envolvem as relações entre dois grupos de atores diferentes (Zhang, 2010). Bez, Faraco e Agenloni (2010) acrescentam que as redes duomodais com dois conjuntos de atores são também conhecidas como bipartidas e são constituídas de dois grupos distintos de atores ou de conjunto de atores e um conjunto de eventos e as relações que possuem entre si, sendo que os atores possuem os mesmos atributos. No entanto, as relações são formadas de um grupo para o outro, e não dentro de um mesmo grupo.

As redes de afiliação envolvem um conjunto de atores e um conjunto de eventos com os atores afiliados. Nas redes de afiliação, os atores (primeiro modo) estão relacionados uns aos outros por meio de sua afiliação a eventos (segundo modo). Os eventos comumente estão definidos como se fossem membros de um clube, como o comparecimento a um evento social, fazer parte de uma mesa diretora ou socializar em um grupo pequeno. (Wassermann & Faust, 1994, p. 40).

4.3.3. Variáveis

Nas Etapas 1 e 3 da pesquisa foram avaliadas as seguintes variáveis para análise das redes sociais mapeadas:

a) **Atores:** os atores que serão levantados são os seguintes atores nos processos: a) inquéritos policiais (IPL): conjunto de documentos que formalizam a investigação policial como depoimentos, laudos periciais, provas, etc.; b) número dos benefícios previdenciários (NB): processos realizados pela Previdência Social onde são feitos pagamentos às pessoas beneficiárias, por exemplo, um processo de aposentadoria; c) agências da Previdência Social (APS): unidade onde foi realizado o processo para concessão do benefício; e d) Servidor do INSS: servidores públicos envolvidos no processo de concessão do benefício previdenciário.

Em razão da necessidade de descaracterização das investigações em andamento, nas redes serão utilizadas as nomenclaturas: IPL1, IPL2, IPL3, NB1, NB2, NB3, APS1, APS2, APS3, Servidor1, Servidor2, Servidor3 e assim por diante.

b) **Vínculos** (*relational tie*), foram mapeados os seguintes vínculos: b.1) inquérito-benefício: visa detalhar quais números do benefício – NB – estão sendo investigados em cada inquérito policial – IPL – possibilitando, por exemplo, identificar eventuais duplicidades, ou seja, dois inquéritos que investigam um mesmo benefício previdenciário; b.2) benefício-agência: identificando a agências da Previdência Social – APS – na qual o benefício foi concedido ou era mantido; b.3) benefício-servidor: benefícios sob investigação por suspeita de fraude investigados em inquéritos diferentes, mas que tenham sido concedidos/habilitados por um mesmo servidor do INSS.

c) Medidas de centralidade: c.1) **intermediação**; c.2) **proximidade**; c.3) **grau**; c.4) **eigenvector**, que podem ser definidos da seguinte forma:

c.1) **Intermediação**, também chamada de *betwenness centrality*, definida como a medida do “número de caminhos que passam por cada unidade” (IBM, 2017, 1). É medida pela proporção de todo o fluxo entre dois atores que ocorre nos caminhos dos quais um determinado ator faz parte (Scott & Carrington, 2011);

c.2) **Proximidade**, também chamada de *closeness centrality*, definida como “a proximidade de um ator para os outros atores na rede social” (IBM, 2017, 1). Essa medida descreve a eficiência da propagação da informação de um ator para todos os outros (Katsaros, Dimokas & Tassiulas, 2010), sendo a soma das distâncias geodésicas entre o nó *i* para todos os *n-1* outros nós na rede (Scott & Carrington, 2011);

c.3) **Grau de centralidade**, também chamada de *degree centrality*, definida como a medida do “nível de conexão de uma Ator ao contar o número de vínculos diretos que cada Ator possui com outros usuários na rede” (IBM, 2017, 1). Essa medida considera um ator como proeminente se os vínculos deste ator o tornam visível aos outros atores da rede (Katsaros, Dimokas & Tassiulas, 2010). Essa medida também é chamada de centralidade de informação;

c.4) **Eigenvector**, definida como “o nível de conexão de uma Ator o nível de influência direta que esse ator pode ter com outros atores conectadas na rede” (IBM, 2017, 1). Também chamado de centralidade geodésica. Essa medida explora a distância (ou seja, o caminho mais curto) entre atores com objetivo de definir as medidas de centralidade (Katsaros, Dimokas & Tassiulas, 2010); e

d) Medida de agrupamento: **K-core**, também chamada de “coeficiente de agrupamento”, definido como “um grupo máximo de atores, sendo que todos os quais estão

ligados a pelo menos k outras unidades no grupo” (IBM, 2017, 1). Segundo Bez, Faraco e Angeloni (2010), o K-core determina a fração média de pares de atores adjacentes a um ator e que também são próximos de outros. A definição do k-core é muito atrativa para algumas aplicações, posto que se um ator tem ligações o suficiente com outros membros de um grupo, ele deve se sentir conectado ao grupo mesmo que ele não conheça muitos membros daquele grupo, de forma que a ideia do k-core depende mais das conexões do que da imersão do ator em um subgrupo (Scott & Carrington, 2011).

As variáveis acima serviram de base para as Etapas 1 e 2. Identificada a rede básica, observou-se que a forma de composição seria melhor descrita utilizando como nós: a) as díades Servidor-APS e b) os IPLs, servindo como vínculos os NBs fraudados. Com isso, tratando-se de dois grupos diferentes de atores, a rede foi melhor descrita como sendo duomodal por afiliação onde cada díade Servidor-APS se conecta a um evento (inquérito policial) por meio de um benefício (NB) fraudado (conforme Figura 10, na seção 5.2).

4.4. Limitações dos dados e das análises

A rede básica delineada foi baseada em operações que investigaram fraudes em benefícios. Embora o número de investigações sobre fraudes em benefícios seja superior ao número de investigações sobre fraudes em custeio, estas últimas não foram objeto de análise por não terem sido abrangidas pela rede básica aqui delineada. Na revisão de literatura foram encontrados na literatura estrangeira textos abrangendo detecção de fraudes em custeio de previdência, não tendo sido encontrados textos nos periódicos nacionais de estratos superiores.

Identificou-se que muitos dos inquéritos policiais, apesar de investigarem fraudes em benefício, não possuem um número de benefício identificado, seja porque ainda não foi descoberto, e a investigação está em andamento justamente para buscar identificar tal número, seja porque não há um número específico, como em um caso onde era investigada a possível atuação de um intermediador em buscar pessoas para cometer fraudes.

Durante a pesquisa constatou-se que muitos dos dados buscados, apesar de constarem em sistemas informatizados, não se encontram armazenados de maneira estruturada. Isso significa que foi necessária varredura manual para mineração dos dados realmente úteis à pesquisa. Algumas das dificuldades encontradas na coleta de tais dados foram as seguintes:

a) com relação ao nome: homônimos. No INSS aceita sobrenome abreviado. No Siscart o campo é de livre digitação, então foram vistos erros de digitação. Isso trouxe muita

dificuldade no cruzamento entre os dados dos “titulares” dos benefícios com os dados das pessoas vinculadas aos inquéritos policiais, como testemunhas, indiciados, etc.

b) um dado que evitaria a ocorrência de homônimos é o número do CPF, que poderia ser utilizado como chave primária, conforme utilizado por Silva (2016). Ocorre que a informação sobre o número do CPF não é obrigatória nos sistemas atualmente utilizados na Polícia Federal, o que faz com que o dado não seja confiável (a maioria dos registros sequer possuía a informação). Anota-se, contudo, que foi identificado o desenvolvimento de novo sistema para controle dos inquéritos policiais denominado “E-Pol” onde, em tese, o nome das pessoas será necessariamente vinculado à base do CPF da Receita Federal.

c) os dados de endereçamento são de difícil cruzamento em termos informáticos, conforme detalhado no tópico sobre a UF4, posto que a quantidade de possíveis variações é enorme (por exemplo, rua abreviada como “r.”, rua por extenso, avenida, alameda, beco, quadra, número, casa, lote, bloco, apartamento, rua com nome de data marcada como número, rua com nome de pessoa abreviado parcialmente ou não, entre várias outras).

Um dos objetivos do trabalho foi analisar o modelo delineado dentro das investigações em andamento na Polícia Federal em algumas unidades da federação. Assim sendo, o recorte foi feito de maneira longitudinal. Uma possível variação abrangeria a análise da evolução e/ou resiliência dos grupos ao longo do tempo a qual não foi aqui abordada posto que para a maior parte dos grupos, as atividades criminosas em conjunto não têm uma longa duração temporal (Tayebi & Glasser, 2012, p. 572).

As análises de redes sociais partem da presunção que os indivíduos ou grupos nas redes não agem estrategicamente para tentar não ser detectados (Michalak, 2017). Assim sendo, é possível que, especialmente se tratando de grupos criminosos organizados, sejam adotadas estratégias a fim de ocultar vínculos entre os membros das organizações criminosas, a fim de dificultar a detecção.

5. RESULTADOS

Os resultados da pesquisa são apresentados nesta seção, que está dividida em três tópicos. Inicialmente, são apresentados os resultados referentes às redes observadas em operações já deflagradas (Etapa 1). Após, são apresentados os pontos comuns nas investigações analisadas, o delineamento da rede básica e de algoritmo de detecção/predição (Etapa 2). Prosseguindo, são apresentadas as redes observadas em investigações em andamento e teste de aplicação do algoritmo proposto (Etapa 3).

5.1. Etapa 1: mapeamento de operações já concluídas

Nas subseções seguintes são descritas sete operações passadas da Polícia Federal que em 2019 se encontram encerradas¹⁰ A descrição das operações é feita com base nos relatórios gerados nas investigações. Além disso, é apresentado o mapeamento e a descrição das redes dos grupos criminosos observados nessas operações. Para cada operação é apresentada uma figura que mostra a rede criminosa específica, bem como uma tabela com os atores centrais identificados.

A lógica observada nos relatórios das investigações segue o raciocínio de que em um Inquérito Policial - IPL são investigados benefícios fraudulentos (identificados pelo Número do Benefício - NB), concedidos em uma determinada Agência da Previdência Social - APS por um determinado servidor, conforme representado na Figura 2.

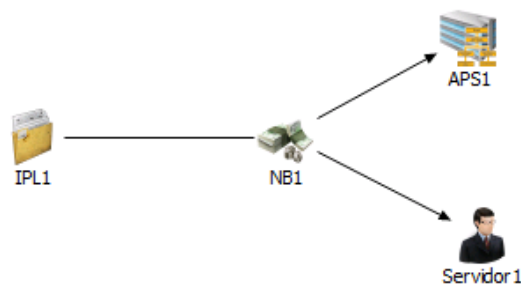


Figura 2. Modelo de redes observado nas operações analisadas.

¹⁰ No momento da pesquisa já havia denúncia do Ministério Público Federal e estavam em curso as respectivas ações penais.

Nesse caso da Operação Fim de Linha, foi possível constatar elementos como a criação fictícia de pessoas, tendo sido possível observar a conexão entre investigações diferentes por envolverem o mesmo servidor do INSS participante do esquema bem como o agrupamento de vários dos benefícios fraudados por terem sido concedidos em uma mesma APS e por apresentarem convergência de endereços (várias pessoas apresentavam o mesmo endereço, seja no cadastro do INSS seja no endereço declarado para emissão do CPF, convergindo para o endereço da Pessoa61 acima citada). A rede descrita no relatório da investigação é representado na Figura 3 (ressaltando que os inquéritos policiais estão indicados como IPLxx, os números de benefícios fraudados como NBxx, as agências da Previdência Social como APSxx e os servidores como Servidorxx).

A lista dos atores com maior relevância na rede consta do Tabela 4. É possível verificar que o IPL3 é o principal ator, resultado esperado, pois foi o principal inquérito policial utilizado nas investigações. Merecem ser destacados na rede os papéis do Servidor7, com altos valores nas variáveis “intermediação” e “proximidade” bem como da APS5, com altos valores nas variáveis “grau” e “*eigenvector*”. O resultado é coerente com o relatório das investigações, eis que o elemento de conexão entre o IPL2 e o IPL3 (inquéritos policiais diferentes) foram os benefícios fraudulentos concedidos pelo Servidor7 na APS5.

Tabela 4
Centralidade dos atores da rede da Operação Fim de Linha

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-core
IPL3	27,59	3,54	40,00	72,30	3
APS5	5,34	3,48	28,57	56,89	3
Servidor7	6,11	3,50	15,71	40,00	3
APS9	0,43	3,42	10,00	12,621	2
IPL2	0,13	3,39	7,14	11,50	3
APS6	0,49	3,42	5,71	6,86	2
NB53	0,06	3,48	4,28	24,65	3
NB14	2,10	3,47	4,28	11,78	2
NB55	0,06	3,48	4,28	24,65	3
NB56	0,06	3,48	4,28	24,65	3

Fonte: autoria própria

5.1.2. Operação Casa Cheia

A Operação Casa Cheia (Inquérito Policial nº 380/2015-SR/DPF/MA) foi deflagrada em maio de 2015 e o Inquérito Policial concluído em julho de 2017. Na investigação foi

apontada a responsabilidade de seis pessoas, sendo três delas servidoras do INSS. Foi apontada a concessão fraudulenta de 70 benefícios previdenciários, com prejuízo estimado de R\$1,65 milhões. A conclusão da investigação foi que o *modus operandi* ali identificado era a concessão do benefício de Amparo Social ao Idoso, previsto na Lei Orgânica de Assistência Social (LOAS), sendo que os supostos beneficiários eram inexistentes, e os responsáveis pela fraude sacavam e ficavam com o valor dos benefícios.

Nesse caso específico, foi identificado que dentre os processos fraudados, 28 dos beneficiários supostamente moravam no mesmo endereço, uma residência comum, e outros 42 moravam também no mesmo endereço, outra residência comum, endereço da Pessoa195, indiciada nesta investigação e que posteriormente foi também investigada na Operação Casa Cheia II, conforme detalhado na próxima seção. A investigação demonstrou que dentre os processos fraudados houve convergência naqueles concedidos por três servidores do INSS que estavam diretamente ligados aos demais envolvidos. Estes três servidores teriam sido responsáveis pela concessão de 13 dos benefícios fraudados. Assim, conforme consta do relatório da investigação, o foco daquela foi concentrado nos processos concedidos pelos servidores identificados. Além disso, constatou-se que os processos concessórios dos benefícios não existiam fisicamente na APS responsável, ou seja, os dados foram inseridos no sistema pelos servidores sem a existência de quaisquer documentos que respaldassem a decisão de concessão dos benefícios.

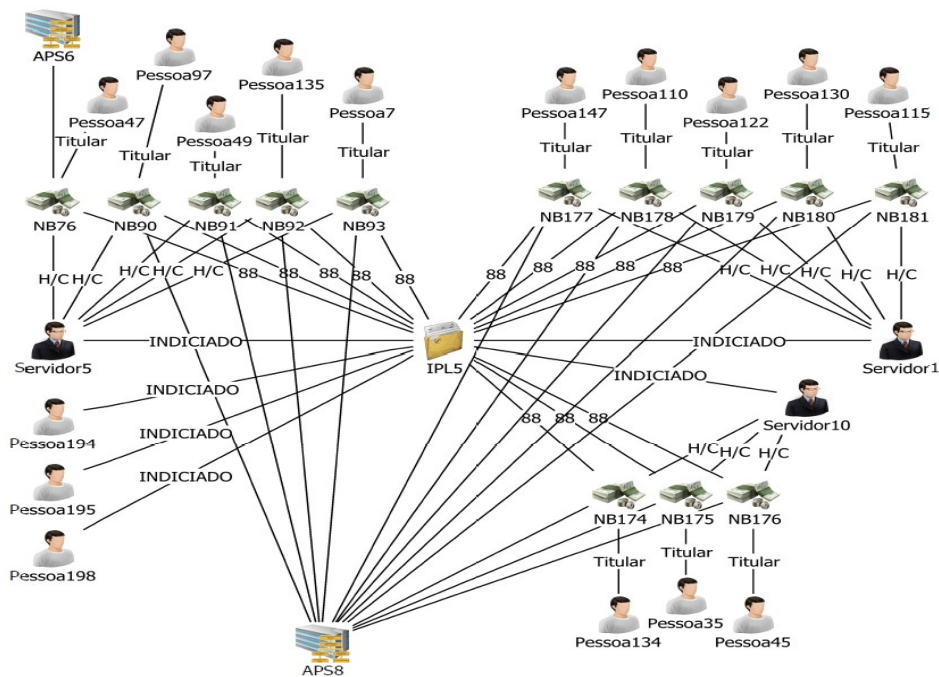


Figura 4. Rede da Operação Casa Cheia

Na Figura 4 é possível ver que os benefícios fraudados estão interligados a uma mesma investigação e a uma mesma APS. É possível observar também que embora todos os benefícios apresentem titulares diversos, cinco deles foram concedidos pelo Servidor1, cinco pelo Servidor5, e três dos benefícios foram concedidos pelo Servidor10. A rede mapeada com os atores e os vínculos observados na Operação Casa Cheia são apresentados na Figura 4.

Observa-se que a estrutura básica de investigação dos diversos benefícios fraudados foi aglutinada em uma mesma investigação, possibilitando a responsabilização de todos os envolvidos nas fraudes (tanto servidores do INSS quanto intermediadores externos). No caso concreto, a responsabilização dos beneficiários seria impossível, posto serem pessoas inexistentes, criadas fraudulentamente apenas para a concessão indevida dos benefícios.

A lista dos atores com maior relevância na rede consta do Tabela 5. Novamente, na rede formada na Operação Casa Cheia, como esperado, o inquérito policial aparece como figura principal da rede do subgrupo. Em seguida aparece a APS8, local onde foram concedidos os benefícios fraudados. Em seguida aparecem os Servidor5, Servidor1 e Servidor10, passando a ser seguidos pelos processos fraudados e por fim os titulares dos benefícios. A análise do software guarda coerência com o observado no relatório da investigação policial, onde comprovou-se a participação dos servidores na concessão fraudulenta dos benefícios.

Tabela 5

Atores da Rede da Operação Casa Cheia

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-core
IPL5	59,64	69,38	55,88	74,30	3
APS8	21,27	53,12	35,29	50,80	3
Servidor5	3,69	48,57	17,64	32,13	3
Servidor1	2,37	47,88	17,64	33,63	3
Servidor10	0,71	45,33	11,76	24,25	3
NB179	6,01	44,15	11,76	26,51	3
NB92	6,05	44,15	11,76	26,26	3
NB93	6,05	44,15	11,76	26,26	3
NB76	11,58	44,15	11,76	18,27	2
NB177	6,01	44,15	11,76	26,51	3

Fonte: autoria própria

5.1.3 Operação Casa Cheia II

Como desdobramento da Operação Casa Cheia, abriu-se uma nova linha de investigação com foco na atuação de associação criminosa de pessoas com foco em fraudes previdenciárias em bairro específico da cidade de São Luís - MA, sendo este o objeto da

Operação Casa Cheia II (Inquérito Policial nº 943/2016-SR/DPF/MA). As investigações identificaram 107 benefícios fraudulentos, que geravam prejuízo de aproximadamente R\$90.000,00 mensais aos cofres públicos.

Nessa operação não foi identificada a participação direta de servidores do INSS, sendo que o vínculo entre os benefícios era feito pela Pessoa195, que agia como intermediador e conseguia os documentos falsos para que fossem obtidos benefícios de amparo social ao idoso previstos na Lei Orgânica de Assistência Social. Conforme citado anteriormente, detectou-se que nos cadastros do INSS que havia pelo menos 42 benefícios previdenciários cujas pessoas possuíam o mesmo endereço da Pessoa195; destes, 35 tiveram a fraude comprovada com a documentação produzida nas investigações.

Também foi apurado que a Pessoa190 era responsável por conseguir certidões falsas para conseguir os benefícios fraudulentos, e que a Pessoa187 utilizava os documentos fornecidos pela Pessoa195 para se passar por idoso, conseguir os benefícios e posteriormente fazer os saques. A Pessoa197 seria um dos intermediadores do esquema criminoso, possuindo em sua residência diversos documentos de identificação falsos. Os atores Pessoa183, Pessoa184 e Pessoa199 foram flagrados com identidades falsas (foram localizados documentos de identidade com suas fotos, mas com outros nomes) utilizadas para obtenção de benefícios fraudulentos. Os benefícios não eram objeto da investigação e foram identificados apenas com a busca e apreensão realizada em suas residências.

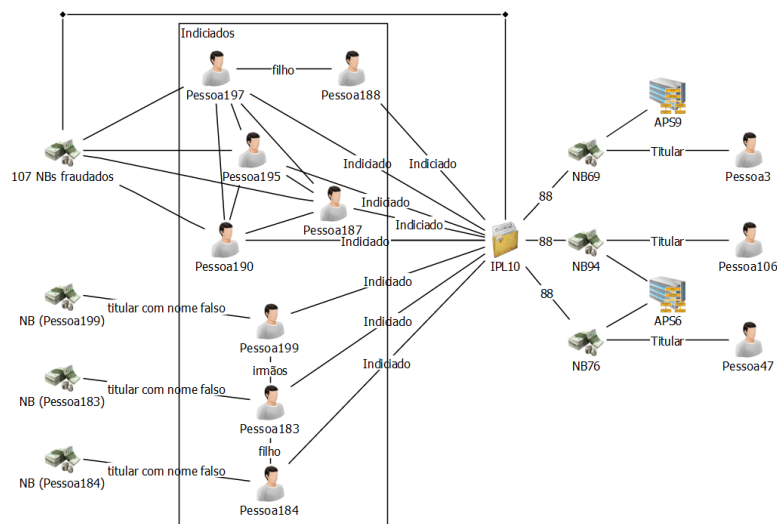


Figura 5. Rede da Operação Casa Cheia II

Com base nos dados obtidos no relatório do inquérito policial foi possível mapear apenas parcialmente a rede formada. O relatório cita a ocorrência de 107 benefícios fraudulentos, mas individualiza apenas três deles. Consta no relatório que foram observados

diversos benefícios concedidos fraudulentamente a pessoas inexistentes. Foram inseridos os vínculos entre os principais investigados (Pessoa197, Pessoa195, Pessoa 190 e Pessoa 187), resultando na Figura 5.

A lista dos atores com maior relevância na rede consta do Tabela 6. A análise da rede formada na Operação Casa Cheia II é coerente com o observado no relatório do inquérito policial. Na rede aqui observada, o núcleo constituído pelos responsáveis pela falsificação dos documentos e intermediação (Pessoa197, Pessoa190, Pessoa195 e Pessoa187) formam o cerne da quadrilha investigada. Nesta investigação não foi detectada a participação de servidores do INSS, não havendo também convergência em uma mesma Agência do INSS, posto que o momento da fraude era anterior à procura pelo órgão. Com o documento falso em mãos, não importava qual servidor ou APS fosse procurada, pois um dos membros da quadrilha se passava por idoso e acabava conseguindo o deferimento do benefício de forma fraudulenta.

Tabela 6
Atores da Rede da Operação Casa Cheia II

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-core
IPL10	82,38	72,41	61,90	70,07	5
Pessoa197	0,95	47,72	28,57	53,32	5
Pessoa190	0	46,66	23,8	49,84	5
Pessoa195	0	46,66	23,8	49,84	5
Pessoa187	0	46,66	23,8	49,84	5
107 NBs fraudados	0	46,66	23,8	49,84	5
Pessoa183	10,47	48,83	19,04	19,64	2
NB94	13,57	46,66	14,28	14,22	2
Pessoa199	9,52	46,66	14,28	16,95	2
NB69	18,57	46,66	14,28	13,71	1

Fonte: autoria própria

5.1.4. Operação Intervenção

A Operação Intervenção (Inquérito Policial nº 627/2015-SR/DPF/MA) foi deflagrada em maio de 2016, tendo a investigação concluída em agosto de 2016. Embora as investigações tenham sido iniciadas para apurar suposta fraude em benefício de pensão por morte, identificou-se fraudes em vários benefícios de amparo social ao idoso, previsto na Lei Orgânica de Assistência Social (LOAS).

As investigações iniciaram com a notícia que o ator denominado Pessoa36 possuiria uma pensão por morte obtida mediante fraude (a suposta cônjuge falecida seria inexistente e a documentação a seu respeito falsa) e seria intermediador para outras pessoas conseguirem obter

benefícios previdenciários de maneira fraudulenta. A partir do endereço da Pessoa36, verificou-se a existência de benefícios da LOAS para pessoas cadastradas naquele endereço, cujas carteiras de identidade foram comprovadas durante as investigações como sendo falsas. Com o cumprimento de medida judicial de busca e apreensão comprovou-se o envolvimento da Pessoa193 nas fraudes bem como foi localizada na residência da Pessoa36 documentação que evidenciou a existência de outros benefícios fraudulentos a ele relacionados, por exemplo, cartões de banco relativos aos NB95, NB96, NB97, NB98 e NB99. Comprovou-se posteriormente que todos estes benefícios foram concedidos pelo Servidor4, que acabou sendo investigado na Operação Intervenção II, conforme apresentado na próxima subseção.

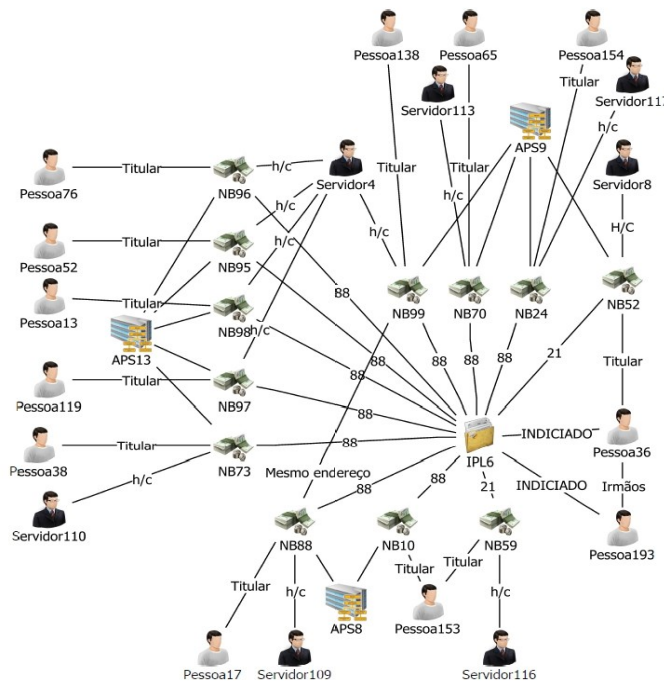


Figura 6: Rede da Operação Intervenção

Nas investigações identificou-se ainda que em um dos endereços onde foi realizada busca e apreensão havia documentos relativos a outros benefícios previdenciários obtidos de maneira fraudulenta, mas sem comprovação de vínculos entre os beneficiários ou com os servidores responsáveis pela concessão. Com base no relatório do inquérito policial foi possível traçar o mapeamento da rede formada pelos atores e vínculos observados na Operação Intervenção, conforme consta na Figura 6.

A lista dos atores com maior relevância na rede consta na Tabela 7. A análise estatística comprova a relevância do Servidor4 na rede, tanto assim que se tornou alvo de nova investigação (detalhada na Operação Intervenção II, a seguir). No mesmo sentido, percebe-se a

relevância da APS13, vinculada não só a vários benefícios investigados no IPL 6 mas é possível observar que quase todos os benefícios concedidos na APS13 foram concedidos pelo Servidor4.

Tabela 7

Atores da Rede da Operação Intervenção

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-Core
IPL6	74,12	62,96	41,17	78,71	3
Servidor4	3,32	36,95	14,70	33,60	3
NB88	14,46	44,15	14,70	28,47	2
APS13	3,80	35,41	14,70	31,40	3
NB99	9,3	44,15	14,70	35,72	2
NB73	12,33	41,97	11,76	25,16	2
NB70	12,30	41,97	11,76	23,24	2
NB96	7,32	41,97	11,76	31,34	3
NB24	12,30	41,97	11,76	23,24	2
NB98	7,32	41,97	11,76	31,34	3
NB97	7,32	41,97	11,76	31,34	3

Fonte: autoria própria

5.1.5. Operação Intervenção II

A Operação Intervenção II (Inquérito Policial 1498/2016-SR/DPF/MA) foi deflagrada em abril de 2017 e o Inquérito Policial concluído em maio de 2017. Na investigação foi apontada a responsabilidade de um servidor do INSS e, na investigação policial, foi comprovada a ação deste na concessão de 73 benefícios previdenciários de forma fraudulenta, com prejuízo estimado de R\$2,4 Milhões. Os benefícios fraudados eram do tipo previsto na Lei Orgânica de Assistência Social (LOAS) na modalidade de Amparo Social ao Idoso. Todos os benefícios foram concedidos na Agência de Previdência Social em Santa Rita - MA e pelo referido servidor. Estimou-se no relatório que os benefícios fraudados podem chegar a 95, sendo que o foco foi centrado nos 73 benefícios citados pois estava comprovada a falsidade documental dos documentos de identificação utilizados na concessão dos benefícios.

No caso concreto, observou-se que o relatório da investigação cita o contido na denominada Operação Hecket, que investigou inicialmente a concessão fraudulenta de 30 benefícios previdenciários pelo mesmo servidor, com o mesmo *modus operandi*. A principal diferença é que na investigação feita na Operação Hecket, os benefícios fraudados eram referentes à modalidade de salário-maternidade para trabalhadoras rurais. O relatório da Operação Intervenção II aqui analisado relata que o servidor respondia, por ocasião do relatório,

a mais de 20 ações penais no Poder Judiciário do Maranhão devido a fatos ligados à Operação Hecket.

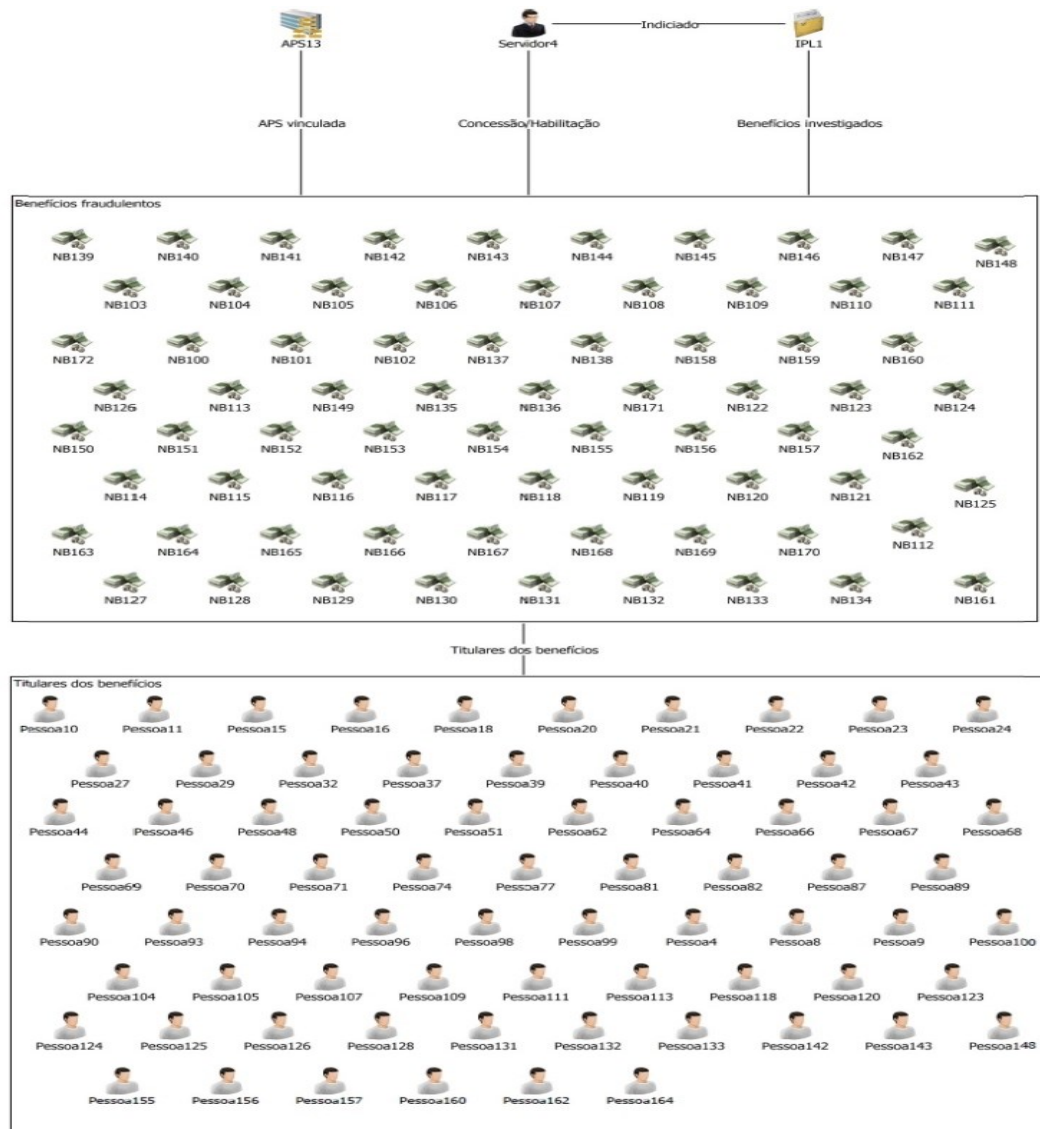


Figura 7: Rede da Operação Intervenção II

Com os dados constantes do Relatório da Operação Intervenção II foi possível mapear a rede formada, que é apresentada na Figura 7. A análise da rede mostra a estrutura básica definida com cada processo fraudado podendo ser caracterizado com a estrutura básica de um inquérito policial que investiga benefício fraudado concedido por um servidor em uma APS para um titular. No caso concreto, a investigação foi feita em apenas um inquérito policial, embora envolva 73 processos diferentes que, caso não fosse identificado o vínculo, ensejariam a existência de 73 inquéritos policiais diferentes. Observado a convergência de que os benefícios foram concedidos por um mesmo servidor em uma mesma APS, foi possível a

investigação de todo o conjunto em uma mesma investigação, ou seja, no mesmo inquérito policial.

A Tabela 8 traz os atores com maior grau de centralidade. Optou-se no mapeamento da rede por apresentar em conjunto os benefícios fraudulentos (na rede indicados como “benefícios fraudulentos”), bem como os titulares de tais benefícios (denominado na rede de “titulares dos benefícios”), apresentando vinculação única dos titulares com os benefícios, destes com o Inquérito Policial IPL1, o servidor concessor Servidor4 e a agência de concessão APS13. Como resultado, o conjunto de “benefícios fraudulentos” apresenta maior resultado na variável “grau” que o próprio inquérito policial (o que não foi observado nos demais casos acima). Em seguida, o ator de maior relevância foi o Servidor4, responsável não só pela concessão de todos os benefícios investigados, como sendo o principal investigado no inquérito. Em seguida, aparece o ator APS13, como sendo a agência do INSS onde os benefícios foram concedidos. Ressalte-se que a tanto o Servidor4 quanto a APS13 já haviam sido identificados como relevantes na rede da Operação Intervenção, e acabaram sendo focos principais da Operação Intervenção II.

Tabela 8

Atores da Rede da Operação Intervenção II

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-core
Benefícios fraudulentos	0,04474	0,68	2,66	89,92	2
Servidor4	0	0,68	1,33	66,96	2
IPL1	0	0,68	1,33	66,96	2
APS13	0	0,68	0,66	38,38	1
Titulares dos benefícios	0	0,68	0,66	38,38	1
Pessoa69	0	0,66	0	0	0
Pessoa70	0	0,66	0	0	0
Pessoa68	0	0,66	0	0	0
Pessoa67	0	0,66	0	0	0
Pessoa64	0	0,66	0	0	0

Fonte: autoria própria

5.1.6. Operação Aquestos

A Operação Aquestos (Inquérito Policial nº 680/2013-SR/DPF/MA) foi deflagrada em julho de 2015 e a investigação concluída em setembro de 2015. A investigação foi feita em razão de fraudes em benefícios de pensão por morte que resultaram em prejuízo estimado de R\$1.694.389,61 (no momento da conclusão das investigações). Identificou-se como *modus*

Na Figura 8, é possível verificar na rede que o benefício NB45, que estava sendo investigado no IPL8, na verdade foi concedido também pelo Servidor8 na APS9, tendo como titular a Pessoa103, que é irmã da Pessoa55, o principal investigado na Operação Aquestos. Já o IPL9, que investigava possível fraude no NB54, constatou-se que o titular do NB54 era a Pessoa1, que é irmão da Pessoa91, sendo que o benefício foi concedido na APS8, onde também foi concedido o benefício fraudulento NB28, cujo titular era a Pessoa60, constatada como pessoa inexistente, de modo que quem estava em posse dos documentos falsos e sacava o benefício era a Pessoa55. A lista dos atores com maior relevância na rede consta na Tabela 9.

Tabela 9
Atores da Rede da Operação Aquestos

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-Core
IPL7	57,82	34,64	34,09	73,738	3
APS9	12,37	28,38	20,45	53,680	3
Pessoa55	9,03	27,16	13,63	16,332	2
Pessoa91	13,50	27,84	13,63	16,700	2
NB57	13,00	26,99	9,09	17,305	1
NB33	10,88	27,32	9,09	18,10	2
NB41	4,34	28,20	9,09	33,20	3
NB32	8,2	28,94	9,09	30,77	2
NB36	7,46	28,20	9,09	29,29	2
NB39	6,07	27,84	9,09	32,47	3
NB45	5,83	23,28	9,09	18,20	2
NB35	7,24	29,53	9,09	34,53	3
Servidor8	2,38	24,71	9,09	24,28	3

Fonte: autoria própria

O resultado é coerente com o observado na investigação. O Inquérito principal (IPL7) aparece como ator mais relevante da rede. Em seguida aparece a APS9, agência onde foram concedidos vários dos benefícios fraudulentos. Logo após aparece o casal Pessoa55-Pessoa91 como atores mais relevantes na rede. Os benefícios NB57, NB33, NB41, NB32, NB36, NB39, NB45 e NB35 aparecem como relevantes na rede. Por fim, aparece o Servidor8, que foi o responsável direto pela concessão de vários dos benefícios fraudados.

5.1.7. Operação Duo Fratres II

A Operação Duo Fratres II (Inquérito Policial nº 221/2015-SR/DPF/MA) foi deflagrada em fevereiro de 2016 tendo as investigações sido concluídas em julho de 2017. A

vários dos benefícios havia a ocorrência de saques após o óbito do titular, ou seja, a fraude não estava na concessão do benefício, mas em sua manutenção após a morte do titular.

Com o material até então levantado foram cumpridas novas medidas judiciais de busca e apreensão, tendo sido identificados vários benefícios previdenciários fraudulentos, fraude no Programa Bolsa Família (suspeita de 182 benefícios fraudados), além de outras fraudes (mais de 10 carteiras de identidade com a mesma foto e nomes diferentes, por exemplo). Na Operação Duo Fratres II, 53 benefícios fraudados foram comprovados, e pelo menos 13 benefícios com saques pós-óbito, com prejuízo ao erário estimado em R\$1,15 milhão.

Com base nos fatos apontados no Relatório da Operação Duo Fratres II, é possível traçar a rede constante na Figura 9. A rede da Operação Duo Fratres II mostra que na investigação foram apurados vários benefícios onde não foi observada convergência com relação a servidores, e nem relação com a APS onde os benefícios foram concedidos. Conforme relatório da operação, o ponto comum entre as fraudes foi justamente o fato de que os fraudadores obtinham os cartões de banco para recebimento de benefícios que tinham sido regularmente deferidos e, após o falecimento das pessoas, passavam a receber indevidamente os benefícios.

A lista dos atores com maior relevância na rede consta do Tabela 10. Novamente os resultados são coerentes com o contido no relatório da investigação. Os principais atores na rede são o IPL4 (que vincula todos os NBs fraudados) e as APS2 e APS8 (onde foram concedidos alguns dos benefícios fraudados). Ocorre que a modalidade criminosa observada na operação não envolvida diretamente as pessoas investigadas, nem foi identificada a participação direta de servidores do INSS.

Tabela 10

Atores da Rede da Operação Duo Fratres II

Ator	Intermediação	Proximidade	Grau	<i>Eigenvector</i>	K-core
IPL4	64,22	5,13	34,65	92,86	3
APS2	0,29	4,78	6,93	20,65	3
APS8	0,20	4,77	6,93	19,48	2
NB30	3,17	4,94	3,96	16,68	2
NB62	4,81	4,94	3,96	15,79	1
NB64	3,17	4,94	3,96	16,68	2
NB89	4,81	4,94	3,96	15,79	1
NB37	4,81	4,94	3,96	15,79	1
NB22	3,99	4,94	3,96	16,22	2
NB19	4,81	4,94	3,96	15,79	1

Fonte: autoria própria

5.2. Etapa 2: Pontos comuns e delineamento de uma rede básica

Mapeadas as redes das operações já deflagradas, foi possível observar a existência de um elemento comum às redes dos processos de fraudes em benefícios, qual seja, em cada investigação era repetida várias vezes uma mesma estrutura básica composta por: (a) um benefício previdenciário concedido por (b) um servidor em (c) uma agência da Previdência Social, conforme mostra a Figura 10. Nas operações analisadas, a caracterização da atuação de grupos criminosos organizados ocorreu quando foi possível observar a repetição dessa estrutura básica por diversas vezes. Assim, se por um lado as investigações de fraudes em benefícios apresentam essa estrutura básica, quando é possível observar a repetição desta estrutura em vários benefícios diferentes, tal situação é vista como indicativo da existência de grupo criminoso organizado.

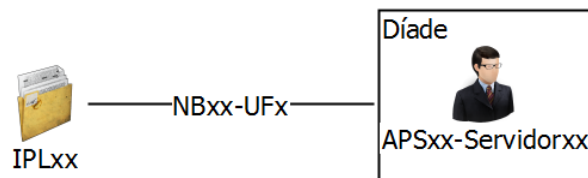


Figura 10. Estrutura de rede básica

A identificação da composição de grupos criminosos por meio uma estrutura básica que se replica pode facilitar o trabalho de detecção ou predição de tais grupos na medida em que, identificada a existência de uma mesma estrutura que se repete, tal fato pode ser indicativo da atuação de grupo criminoso organizado. Na pesquisa de campo constatou-se que os dados do número do benefício investigado não são armazenados em campo próprio nos bancos de dados (ou seja, o dado não está estruturado), tendo sido necessária mineração de dados por meio de análise individual dos inquéritos policiais e, por consequência, os dados sobre o servidor responsável pelo processo e APS de concessão/manutenção também eram desconhecidos¹¹. Com a ideia da formação dos grupos em blocos, as informações básicas de composição destes blocos podem/devem passar a ser armazenada de maneira estruturada nas bases de dados a fim de permitir a utilização de ferramentas informáticas no processo, o que ampliaria muito a possibilidade de análise de dados.

¹¹ Por ocasião da pesquisa de campo foi desde já apontado que o armazenamento de tais dados de maneira estruturada poderia permitir o cruzamento de dados em larga escala, tendo as primeiras iniciativas nesse sentido sido adotadas na Polícia Federal no âmbito da iniciativa denominada Projeto Prometeus, em fase de implementação pela CGPFAZ/DICOR.

Sob a ótica da administração e partindo das ideias de Morgan (1996) sobre as organizações, aponta-se inicialmente sua visão da organização como organismo vivo. A identificação de um bloco estrutural básico que se repete pode ser vista em seres vivos na forma de composição corporal que a biologia denomina de metameria¹² (ou simetria serial). Essa forma de repetição de blocos serviu para aqueles seres vivos resolverem um problema evolutivo de necessidade de aumento de tamanho, tendo como exemplo o poliqueto, anelídeo constante da Figura 11 e que repete várias vezes os blocos estruturais na formação de seu corpo. (Ferreira Júnior & Paiva, 2010).

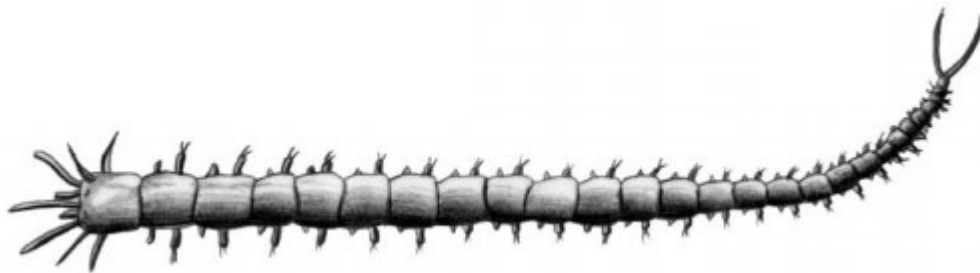


Figura 11. Poliqueto

Fonte: Ferreira Júnior e Paiva (2010).

Com essa ideia de repetição de estruturas de blocos em mente, *mutatis mutandi*, os grupos criminosos com atuação na área de fraudes previdenciárias parecem atuar de maneira similar: 1) monta-se uma estrutura capaz de fraudar um único benefício (um servidor do INSS em uma determinada APS ou um falsificador de documentos e uma pessoa para se passar pelo beneficiário, por exemplo); 2) se a fraude obtiver sucesso, a mesma estrutura é repetida por diversas vezes, fraudando diversos benefícios; 3) se a fraude não obtiver sucesso, muda-se a estrutura básica e tenta-se outra forma de cometer a fraude até obter sucesso.

Essa repetição de blocos estruturais foi observada de maneira clara na Operação Intervenção II. Naquele caso, durante os trabalhos investigativos da Operação Intervenção I foi detectada a participação do Servidor4 na concessão fraudulenta de benefícios dentro da APS13 (vide na seção 5.1.4). Identificado o bloco estrutural básico, foi possível chegar a 73 benefícios fraudados pelo mesmo servidor na mesma APS (vide seção 5.1.5), objeto de apuração da Operação Intervenção II. Essa reunião pode ser diagramada conforme Figura 12.

¹² Definida como a “repetição seriada de partes do corpo, incluindo representantes dos órgãos e sistemas” conforme Ferreira Júnior e Paiva (2010).

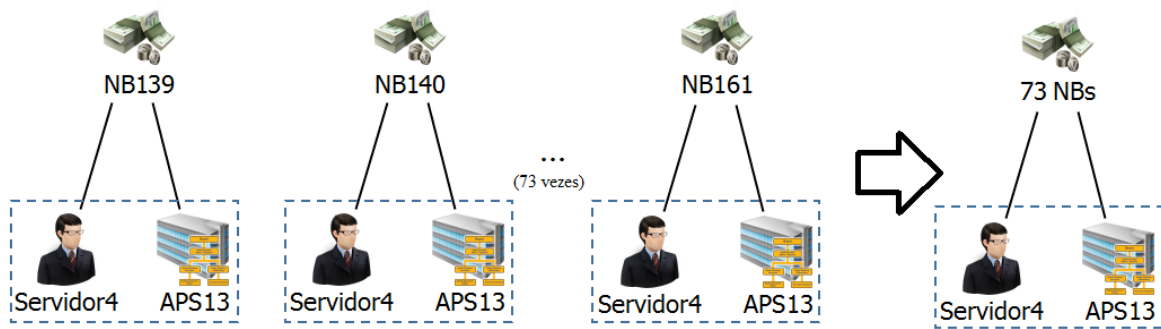


Figura 12. Reunião de NBs fraudados na Operação Intervenção II

A metáfora dos blocos reunidos que formam uma grande organização também foi usada por Morgan (1996) ao abordar os elementos de dominação das organizações. O autor cita o exemplo da Grande Pirâmide de Gizé, que foi construída com 2,3 milhões de blocos de pedra e fala que a construção da pirâmide serve também para explicar as “relações de poder assimétricas que resultam numa maioria trabalhando no interesse de uns poucos” (p. 304). Novamente a analogia com as organizações criminosas parece bastante cabível, não só pela repetição dos blocos estruturais básicos, mas especialmente pela estrutura montada no interesse de uns poucos que comandam essas organizações, de forma que tal raciocínio reforça a importância de identificar e punir os criminosos que estão no topo da estrutura.

Por fim, mas também de forma muito adequada para a compreensão das organizações criminosas, Morgan (1996) ao abordar conflitos e poder entre organizações, fala sobre a criação do que chama de ‘sistemas de controle de contra organização’, que são “indivíduos que coordenam suas ações para criar um bloco de poder rival”(p. 203). Na obra, Morgan cita, por exemplo, sindicatos que fiscalizam a administração ou agências reguladoras que coíbem ações monopolísticas de mercado. Extrapolando a comparação, há organizações criminosas que se colocam na posição de confronto ao Estado Democrático de Direito, buscando até mesmo substituir algumas de suas funções, como nos casos de organizações criminosas que controlam favelas (Soares, 2015).

Com a ideia da estrutura de rede básica que se repete para formar um grupo criminoso organizado, é possível repensar as redes mapeadas com a lógica de uma díade formada pelos atores APSxx-Servidorxx, vinculadas a um IPLxx por meio de um ou vários NBsxx, conforme representado na Figura 2, apresentada na seção de método. Com base nisso, foi feita uma reanálise das operações de combate a fraudes à Previdência Social aqui citadas, buscando identificar para quantas/quais operações essa rede básica era aplicável e em que proporção

poderia explicar os fenômenos ali observados. Os dados dessa reanálise estão agrupados no Tabela 11.

Tabela 11
Análise de aplicação do modelo-base a operações já concluídas

Operação	Análise com relação ao modelo-base
Fim de Linha	O modelo identificaria 31 benefícios fraudulentos conectados por 3 APS e 1 servidor.
Casa Cheia	O modelo aplicado identificaria 13 benefícios fraudulentos, conectados por 3 servidores e 1 APS.
Casa Cheia II	O modelo não explica a fraude observada, e identificaria apenas 2 benefícios conectados por 1 APS.
Intervenção	O modelo detectaria 12 benefícios, conectados por 1 servidor e em 3 APS.
Intervenção II	O modelo explica com sucesso a conexão dos 73 benefícios fraudulentamente obtidos.
Aquestos	O modelo identificaria 7 benefícios fraudulentos emitidos na mesma APS e por 1 servidor.
Duo Fratres II	O modelo identificaria 14 benefícios concedidos em 2 APS e concedidos por 2 servidores.

Fonte: autoria própria

Na investigação da Operação Fim de Linha seriam identificáveis 31 dos 64 benefícios fraudados; na Operação Casa Cheia, seriam identificáveis 13 dos 70 benefícios fraudados, mas a modelagem não explicaria os achados na Operação Casa Cheia II, onde identificaria apenas 2 benefícios conectados por uma mesma APS. Na Operação Intervenção essa repetição de estrutura identificaria 12 dos 34 benefícios fraudados, mas explicaria integralmente os 73 benefícios fraudados na Operação Intervenção II. Na Operação Aquestos, a modelagem explicaria 7 dos 14 benefícios fraudados. Na Operação Duo Fratres II, a modelagem explicaria 14 dos 107 benefícios fraudados.

Com tais dados, é possível apontar que o modelo identificaria (em maior ou menor grau) indicativos de conexão nas operações citadas, à exceção do contido na Operação Casa Cheia II. Seriam identificados 154 benefícios fraudulentos conectados por nove servidores e 12 APS. Nas operações investigadas foram citados 426¹³ benefícios que, em tese, seriam fraudulentos, o que representa um índice de 36,2% de detecção.

¹³ Os 42 benefícios que aparecem tanto na Operação Casa Cheia quanto na Operação Casa Cheia II foram descontados para não contarem em duplicidade. Os dados compilados são apresentados na seção de resultados.

Necessário reforçar que a detecção dessa estrutura básica não teria o condão de substituir o trabalho investigativo/intelectual do ser humano, mas se mostrou capaz de apontar elementos de conexão que indiquem possível atuação de grupos organizados. Nesse sentido, feita a detecção do possível grupo organizado, o trabalho investigativo poderia ser desenvolvido e já começaria um passo adiante, posto que as investigações partiriam de uma conexão já identificada.

Analisando formas de tornar a rede básica mais precisa, especialmente para tentar abranger casos não explicados como da Operação Casa Cheia II, são identificadas duas informações que podem ser agregadas: o tipo de benefício fraudado e o endereço vinculado ao beneficiário. O tipo de benefício fraudado mostrou homogeneidade em cinco das sete operações analisadas, sendo observada heterogeneidade na Operação Fim de Linha, com fraudes na concessão de vários tipos de benefício, e na Operação Duo Fratres II, onde a fraude não era na concessão do benefício e sim na manutenção, vez que ocorriam reiteradamente saques após o falecimento do beneficiário. Com relação ao endereço dos beneficiários, necessário observar as limitações relativas à dificuldade de estruturação dos dados de endereçamento para cruzamento via sistema informatizado, conforme detalhado na seção 4.5.

Por todo o exposto, o modelo de repetição de rede básica foi adotado como parâmetro para pesquisa nas redes das unidades da Federação mapeadas, sendo incluídas de maneira complementar dados com relação ao tipo de benefício fraudado (detalhamento nas redes dos subgrupos apresentadas nos Apêndices) bem como feita pesquisa por endereço dos titulares dos benefícios na UF4.

Com base no algoritmo de detecção de grupos criminosos de Tayebi e Glasser (2016) e incluídas as ideias da formação de grupos criminosos por meio da repetição dessa rede básica e participação de ao menos quatro pessoas (critério legal), o processo de detecção/predição de grupos criminosos organizados que foi feito nas unidades da Federação pode ser organizado logicamente na forma do algoritmo contido na Tabela 12.

Tabela 12

Algoritmo de detecção/predição de grupos criminosos em fraudes previdenciárias

Variáveis: NB: inteiro;
 APS: inteiro;
 Servidor: inteiro;
 Grupo_NB: cadeia de caracteres;

- 1: Para cada 'NB' no intervalo de tempo [t1, t2]; *///define intervalo de tempo de pesquisa*
- 2: Leia ('APS', 'Servidor');
- 3: 'Grupo_NB' = conjunto ('APS' // 'Servidor');

```

4:   Loop;
5:   Para cada 'Grupo_NB', contar('NB');           // verificar a quantidade de ocorrências do grupo
6:   Se contar('NB') >3, então exibir ('Grupo_NB'; 'contar('NB')')
7:   Senão 'não identificada atuação de grupo'
8:   Fim

```

Fonte: customização do algoritmo de Tayebi e Glasser (2016).

Nas seções seguintes são apresentados os resultados do mapeamento de investigações em andamento em quatro unidades da Federação bem como os resultados das buscas de conexão com base na identificação da rede básica apontada. A ideia é verificar se podem ser vistos nos inquéritos policiais em andamento os mesmos elementos básicos de composição de grupos criminosos organizados observados nas operações descritas, ou seja, verificar se a rede básica aqui descrita pode ser identificada de maneira repetitiva nas redes das unidades da Federação mapeadas, conforme se passa a expor.

5.3. Etapa 3: Teste do algoritmo em redes de investigações em andamento

Conforme detalhado na seção de método, foram coletados dados sobre investigações em andamento em quatro unidades da Federação para análise das redes e teste do algoritmo ora proposto. Nesta seção são apresentados os resultados do mapeamento das redes e do teste do algoritmo.

5.3.1. Teste do algoritmo na Unidade da Federação 1 – UF1

Foram analisados 385 inquéritos policiais para o mapeamento da rede 8. A primeira avaliação identificou dez inquéritos que não são de natureza previdenciária, tendo sido identificados ainda 101 inquéritos policiais a respeito de fraudes em custeio, e 274 sobre fraudes em benefício. Para os inquéritos de fraudes em benefício, foi feita classificação com relação ao tipo de fraude/benefício previdenciário fraudado e respectivos percentuais com relação ao total de inquéritos na unidade. As principais fraudes/benefícios fraudados foram: aposentadoria, com 23%, saques pós-óbito, com 15%, pensão por morte e auxílio-doença, ambos com 11%, e fraudes em benefícios da LOAS, com 10%.

Passou-se à análise individualizada dos inquéritos policiais, tendo sido obtidos os números de benefícios investigados em 137 inquéritos policiais. Nestes, foram identificados 281 números de benefícios (NBs), concedidos em 84 diferentes Agências da Previdência Social

- INSS (APS) por 155 diferentes servidores. Durante a estruturação dos dados, constatou-se grande volume de benefícios onde constava no lugar do servidor concessor um código que se identificou como sendo utilizado para casos onde é feita a concessão automática. Constatou-se que este código automático é utilizado em casos onde não há necessidade de análise detalhada por parte do servidor do INSS, por exemplo, nos casos de auxílio-doença, que, constatada pela perícia a doença do trabalhador segurado, o benefício é automaticamente concedido. Nas redes mapeadas foi inserido um ator com nome de “Automático” no lugar do servidor responsável pela concessão, vinculado ao NB em tais casos.

No caso da UF1, foram incluídas também informações a respeito de pessoas vinculadas aos inquéritos policiais, como testemunhas, declarantes, entre outros, bem como informações da APS de manutenção anterior, como informações complementares aos dados já levantados. A rede formada contou então com 1193 atores e 1515 vínculos. Foi possível gerar a rede apresentada na Figura 13.



Figura 13. Rede dos inquéritos em andamento na UF1

A visão geral da rede formada na UF1 permite observar a ocorrência de uma grande rede principal e algumas redes do subgrupo independentes (Área 1 na rede). Visualmente, é possível perceber contração na Área 2, correspondentes a vínculos envolvendo a APS353 (rede no Anexo I). Na Área 3, constata-se concentração de vínculos relativos ao IPL654, e na Área 4, os vínculos referentes ao IPL309. As redes geral e dos subgrupos da UF1 foram analisadas com maior detalhamento no Apêndice I, onde foram analisados os atores com maior grau de

centralidade e as redes observadas nos subgrupos gerados a partir destes atores, dentre outras análises.

Foram então aplicadas as regras do algoritmo da Tabela 12 (vide seção 5.2). Para funcionamento do algoritmo, foi feita a combinação (concatenação) dos atores APS e Servidor, aplicando a lógica da Figura 2 (vide seção 4.1), sendo então avaliados os vínculos entre as díades APS-Servidor com os IPLs por meio de NBs fraudulentos. Foram selecionados então apenas os conjuntos APS-Servidor que possuem quatro ou mais NBs suspeitos de fraude. A rede dos grupos criminosos consta da Figura 14.

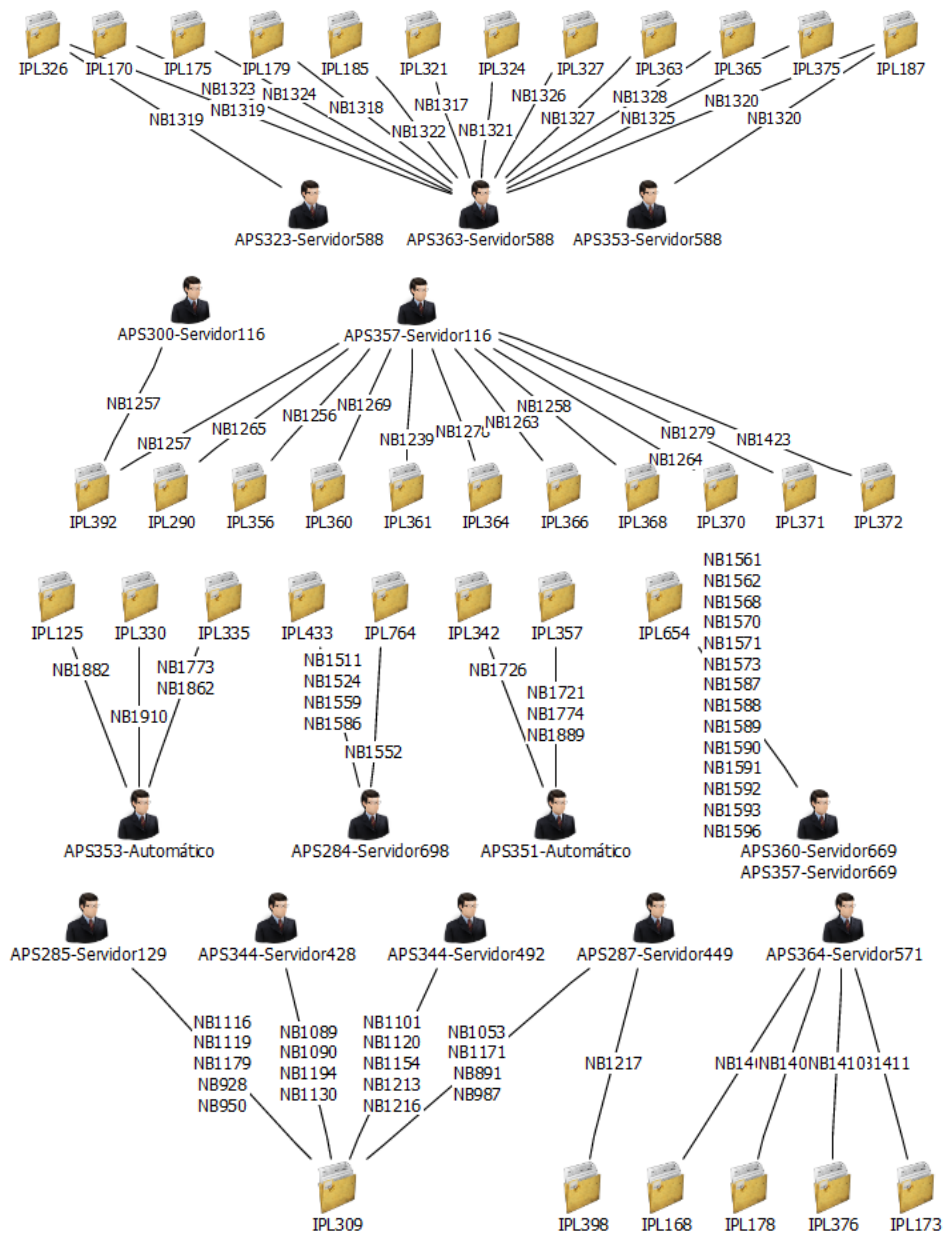


Figura 14. Rede de grupos criminosos detectados da UF1

O algoritmo detectou na UF1 255 diferentes díades APS-Servidor, das quais apenas 12 apresentaram quatro ou mais vínculos. Dentre estas últimas, duas dizem respeito a APSs vinculadas a “servidor automático”. Já o Servidor669 aparece tanto na díade com a APS357 quanto com a APS360. Assim sendo, foram detectados nove prováveis grupos criminosos, vinculados à concessão de 65 NBs investigados em 32 IPLs.

5.3.2. Teste do algoritmo na Unidade da Federação 2 – UF2

Foram analisados 224 inquéritos policiais da unidade na capital e delegacias descentralizadas. Na primeira análise, foram observados 14 inquéritos policiais de natureza diversa da previdenciária, bem como 15 inquéritos policiais com investigação sobre fraudes em custeio, e 195 sobre fraudes em benefício. Os inquéritos sobre fraudes em benefício foram classificados com relação ao tipo de fraude/benefício fraudado, sendo os principais resultados: a) saques pós-óbito, com frequência de 58%; b) benefícios da LOAS, com 12%; c) pensão por morte, com 9%; d) auxílio-doença, com 6%; e) aposentadorias, com 4%.

Procedeu-se então à identificação dos números dos benefícios (NB) previdenciários objetos de investigação, tendo sido identificados 164 inquéritos policiais, que investigam possíveis fraudes em 289 benefícios, concedidos em 58 APS, por 70 servidores. Na rede mapeada foram incluídas de maneira complementar dados sobre os titulares dos benefícios e pessoas vinculadas aos inquéritos policiais (testemunhas, investigados, etc), no total de 431 pessoas. A rede mapeada na UF2 é apresentada na Figura 15.

Na Figura 15 é possível observar ao menos três regiões de concentração de vínculos: no centro da rede, denominada de área 1, fica a APS236 (rede no Apêndice II); também no centro da rede, um pouco mais embaixo da área 1, aparece a denominada de área 2, onde fica o servidor “automático”; e na área 3 aparecem os atores conectados ao IPL1059. São observáveis ainda, na parte de cima à direita, três subgrupos que não se conectam à rede principal, cada um formado por um inquérito, um benefício fraudado e os respectivos atores conectados.

As redes geral e dos subgrupos da UF2 foram analisadas com maior detalhamento no Apêndice II, onde foram analisados os atores com maior grau de centralidade e as redes observadas nos subgrupos gerados a partir destes atores, dentre outras análises.

Foram então aplicadas as regras do algoritmo da Tabela 12 (vide seção 5.2), tendo sido feita a combinação dos atores APS e Servidor, sendo então avaliados os vínculos entre as díades APS-Servidor com os IPLs por meio de NBs fraudulentos, sendo selecionados os conjuntos

APS-Servidor que possuem quatro ou mais NBs suspeitos de fraude. A rede dos grupos criminosos consta da Figura 16.

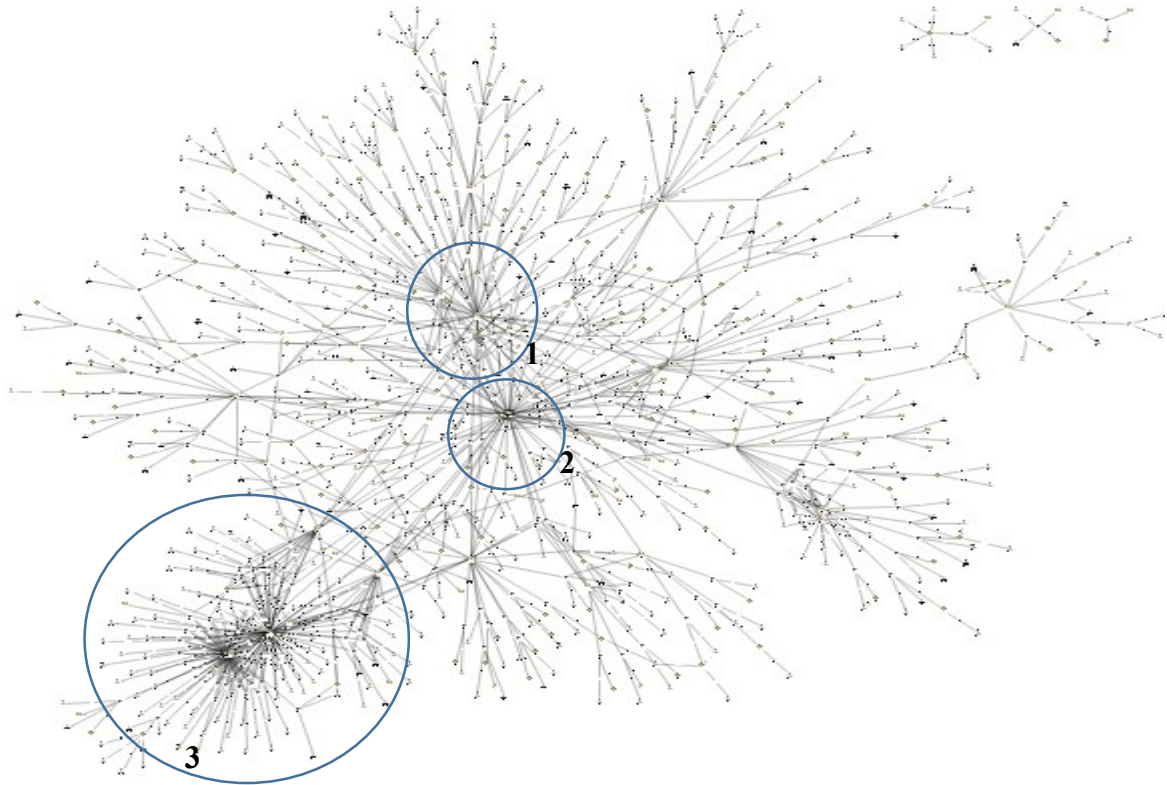


Figura 15. Rede dos inquéritos em andamento na UF2

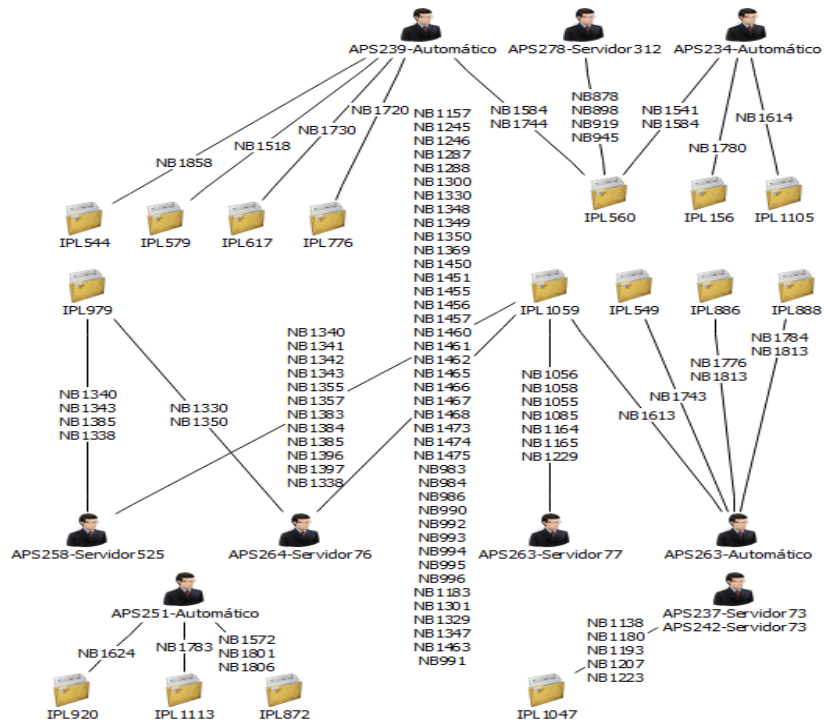


Figura 16. Rede de grupos criminosos detectados da UF2

O algoritmo detectou na UF1 141 diferentes díades APS-Servidor, das quais apenas dez apresentaram quatro ou mais vínculos. Dentre estas últimas, quatro dizem respeito a APSs vinculadas a “servidor automático” e o Servidor73 aparece tanto na díade com a APS237 quanto com a APS242. Assim sendo, foram detectados cinco prováveis grupos criminosos, vinculados à concessão de benefícios investigados em quatro IPLs, destacando-se o Servidor76 que teria concedido na APS264 o total de 43 NBs investigados.

5.3.3. Teste do algoritmo na Unidade da Federação 3 – UF3

Foram analisados 979 inquéritos policiais da DELEPREV da Superintendência Regional e delegacias descentralizadas localizadas em municípios do interior da UF. Na primeira análise foram observados 93 Inquéritos de natureza diversa da previdenciária, 120 inquéritos policiais sobre fraudes em custeio e 766 sobre fraudes em benefício. Para os inquéritos policiais sobre fraudes em benefício, foi feita classificação com relação ao tipo de fraude/benefício fraudado, sendo os principais resultados: a) saques pós-óbito, com frequência de 29%; b) benefícios da LOAS, com 22%; c) auxílio-doença, com 13%; d) aposentadorias, com 11%; e) pensão por morte, com 5%.

Foram identificados 1031 benefícios previdenciários possivelmente fraudados em 593 inquéritos policiais. Tais benefícios foram concedidos em 200 APS por 416 servidores, num total de 2240 atores e 3208 vínculos, cuja rede consta da Figura 17.

Uma visão geral permite perceber algumas redes do subgrupo que não se conectam com a rede principal da UF3, marcada na rede como área 1. A aglomeração marcada na área 2 apresenta concentração de vínculos de benefícios concedidos na APS97. Na área 3 estão concentrados os vínculos referentes a benefícios investigados no IPL939 e concedidos na APS96. A área 4 concentrou os vínculos referentes a benefícios concedidos de maneira automática. A área 5 acabou aproximando os vínculos de benefícios investigados no IPL889 e os concedidos nas APS37, APS40 e APS44. A área 6 reuniu vínculos de benefícios concedidos na APS114 e a área 7 agrupou vínculos de benefícios objeto do IPL864.

As redes geral e dos subgrupos da UF3 foram analisadas com maior detalhamento no Apêndice III, onde foram analisados os atores com maior grau de centralidade e as redes observadas nos subgrupos gerados a partir destes atores, dentre outras análises.

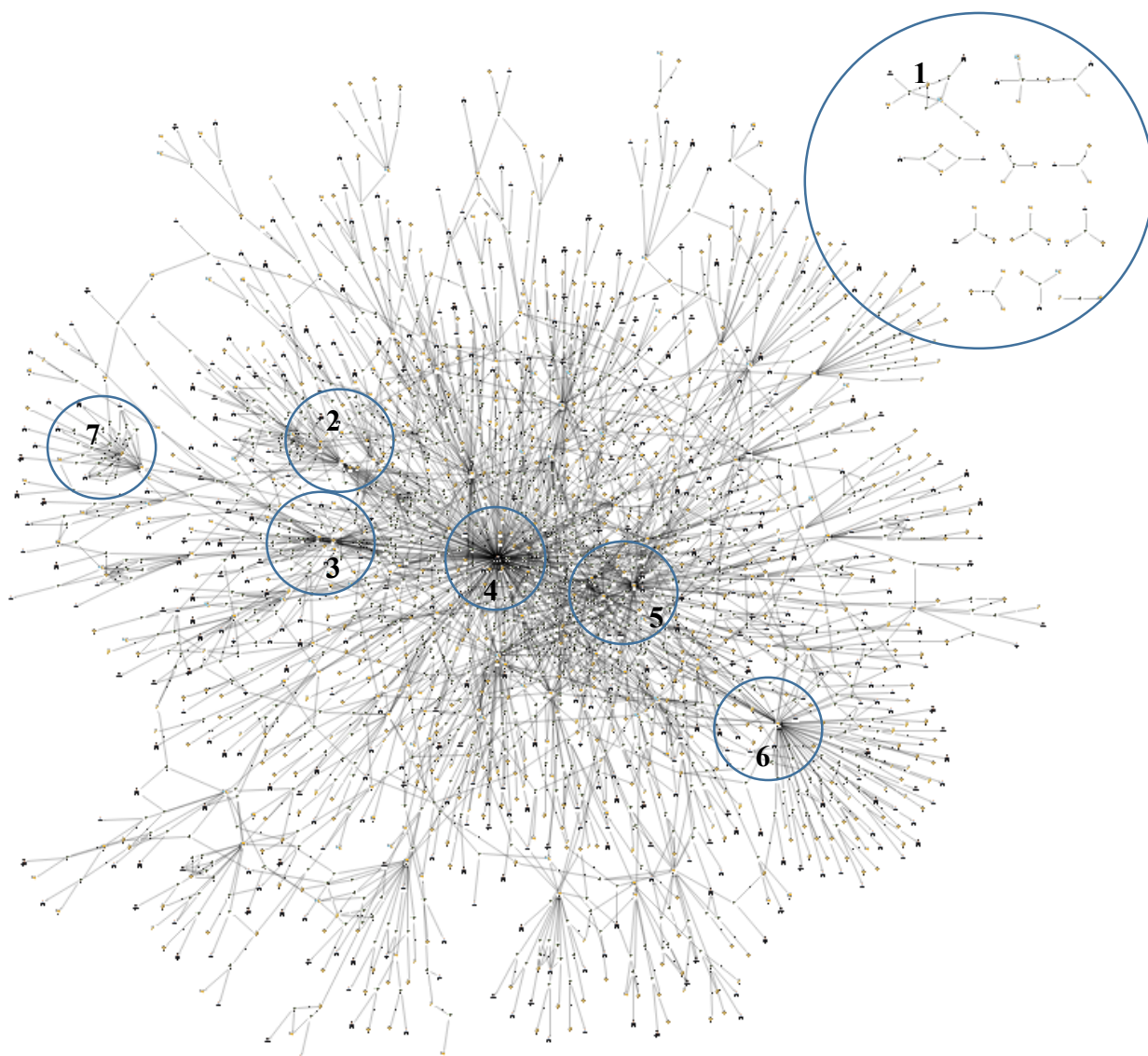


Figura 17. Rede dos inquéritos em andamento na UF3

Aplicadas as regras do algoritmo da Tabela 12 (vide seção 5.2), foi implementada a lógica da Figura 2 (vide seção 4.1) e avaliados os vínculos entre as díades APS-Servidor e IPLs por meio de NBs fraudulentos. As díades que possuem vínculo com quatro ou mais NBs investigados foram consideradas como indicativas de existência de grupos criminosos. A rede dos grupos criminosos consta da Figura 18.

O algoritmo detectou na UF2 667 diferentes díades APS-Servidor, das quais apenas 40 apresentaram quatro ou mais vínculos. Dentre estas últimas, 21 dizem respeito a APSs vinculadas a “servidor automático” e o Servidor419 aparece nas díades com a APS97 e APS109. Assim sendo, foram detectados 18 prováveis grupos criminosos, vinculados à concessão de 101 NBs investigados em 55 IPLs.

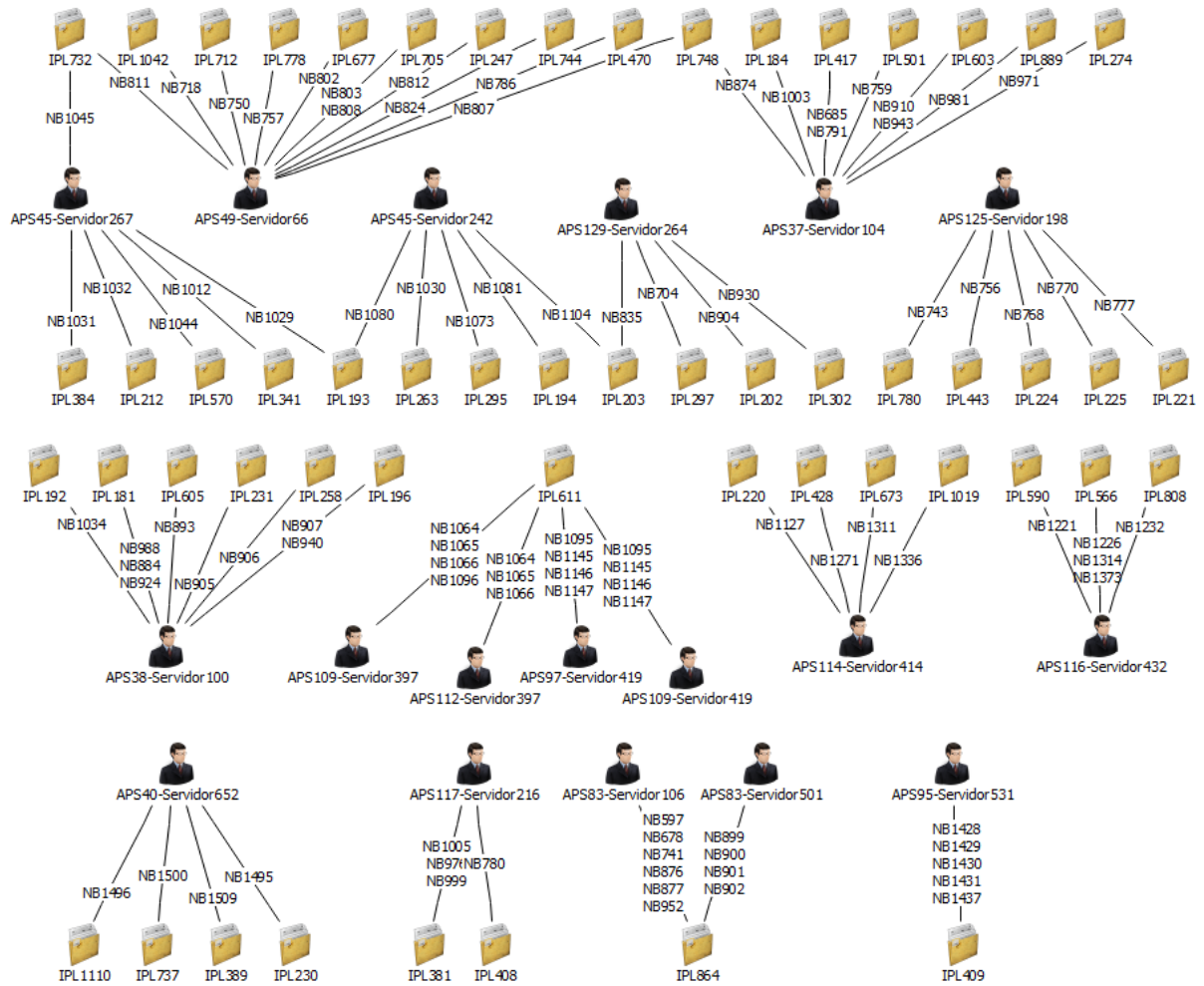


Figura 18: Rede de grupos criminosos detectados UF3

5.3.4. Teste do algoritmo na Unidade da Federação 4 – UF4

Foram analisados 599 Inquéritos policiais da unidade na capital e delegacias descentralizadas localizadas em municípios do interior da UF. Na primeira análise foram observados 17 Inquéritos de natureza diversa da previdenciária, 79 inquéritos policiais sobre fraudes em custeio e 503 sobre fraudes em benefícios. Destes últimos, foi feita a análise sobre o tipo de fraude/benefício fraudado, que apontou a incidência principalmente de inquéritos policiais sobre: a) saques pós-óbito, 63%; benefícios da LOAS, 12%; c) auxílio-doença, 8%; d) aposentadoria, 7%; e) seguro-defeso, 2%.

Identificou-se um número alto de investigações a respeito de fraudes na manutenção do benefício (saques pós-óbito). Assim, na UF4 foram avaliados apenas os inquéritos com possível fraude na concessão do benefício para fins do mapeamento da rede da UF4, não sendo

incluídas as fraudes na manutenção do benefício (saque pós-óbito, por exemplo), para permitir a avaliação de possíveis diferenças com relação às demais UFs. Assim, foram identificados 205 benefícios possivelmente fraudulentos investigados em 128 dos inquéritos policiais, concedidos por 92 servidores do INSS em 32 APS. A rede então conta com 651 atores e 908 vínculos, sendo diagramada conforme Figura 19.

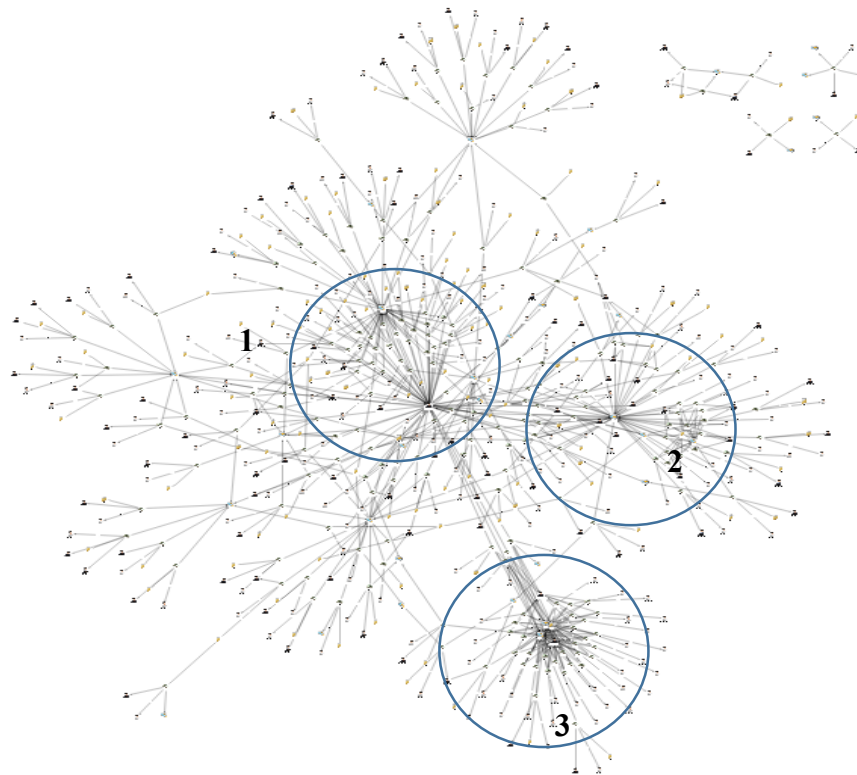


Figura 19. Rede dos inquéritos em andamento na UF4

Uma visão geral da rede permite identificar pelo menos três áreas de concentração de vínculos. A área 1 engloba os vínculos referentes aos benefícios com concessão automática (ator “Automático”) bem como os vínculos de benefícios concedidos na APS5. A área 2 reúne os vínculos de benefícios concedidos na APS2 (rede no anexo IV). A área 3 engloba os benefícios fraudados investigados no IPL720 e concedidos pelo Servidor668, passando-se a observar a rede formada em referido inquérito.

As redes geral e dos subgrupos da UF4 foram analisadas com maior detalhamento no Apêndice IV, onde foram analisados os atores com maior grau de centralidade e as redes observadas nos subgrupos gerados a partir destes atores, dentre outras análises.

Aplicadas as regras do algoritmo da Tabela 12 (vide seção 5.2), foi implementada a lógica da Figura 2 (vide seção 4.1) e avaliados os vínculos entre as díades APS-Servidor e IPLs por meio de NBs fraudulentos. As díades que possuem vínculo com quatro ou mais NBs

investigados foram consideradas como indicativas de existência de grupos criminosos. A rede dos grupos criminosos consta da Figura 20.

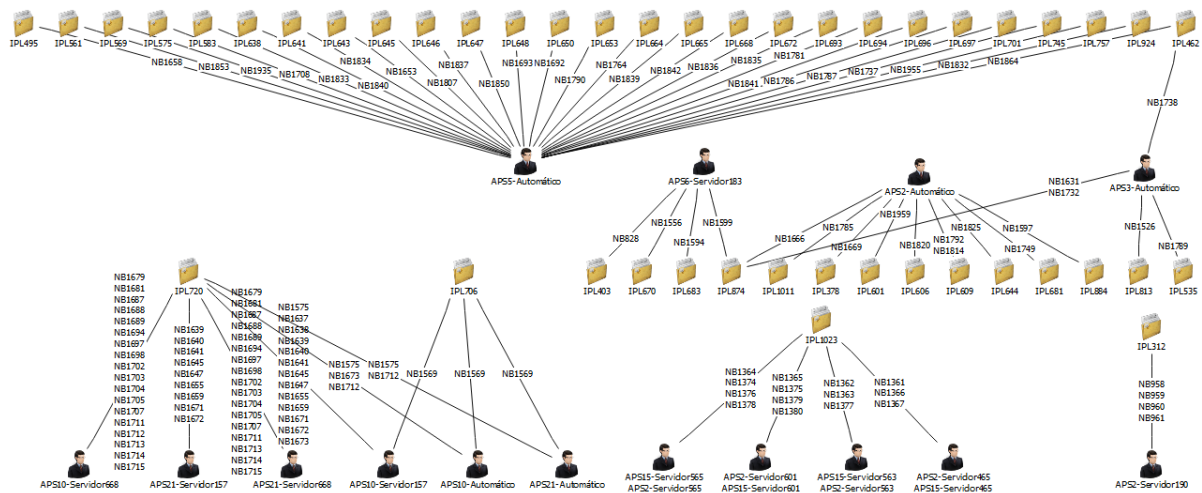


Figura 20. Rede de grupos criminosos detectados UF4

O algoritmo detectou na UF1 137 diferentes díades APS-Servidor, das quais apenas 14 apresentaram quatro ou mais vínculos. Dentre estas últimas, aponta-se que: a), quatro dizem respeito a APSs vinculadas a “servidor automático”; b) os atores Servidor668 e Servidor 157 aparecem nas díades com a APS10 e APS21; c) os atores Servidor601 e Servidor565 aparecem em díades com a APS2 e a APS15. Assim sendo, foram detectados efetivamente seis prováveis grupos criminosos, vinculados à concessão de 82 NBs investigados em oito IPLs.

Como abordagem complementar e com certa natureza exploratória, para a UF4 tentou-se executar cruzamento com relação aos endereços dos beneficiários. Para os benefícios investigados foi feita estruturação dos dados referentes aos endereços dos benefícios declarados perante o INSS. Os dados de endereçamento são de difícil utilização por não apresentarem estruturação (informaticamente falando). Ocorre que devido ao sistema de endereçamento utilizado no Brasil, normalmente o endereço não apresenta uma estrutura fixa, o que dificulta o cruzamento de dados em larga escala.

Exemplificando a dificuldade encontrada no endereço, imagine-se três benefícios hipotéticos, onde os titulares escreveram seus endereços das seguintes formas: a) Rua Vinte e Seis de Abril, número 12, Goiânia-GO; b) R. 26 de abril, n. 12, Goiânia-GO; c) Rua 26 de abril, casa 12, Goiânia-GO. Um carteiro que fosse entregar uma encomenda em referidos endereços provavelmente teria pouca dificuldade em constatar que todos se referem ao mesmo local. Mas em termos informáticos a identificação de todos os locais como o mesmo endereço é bem mais

complexa. A quantidade de possíveis variações é enorme: rua abreviada como “r.”, rua por extenso, avenida, alameda, beco, quadra, número, casa, lote, bloco, apartamento, rua com nome de data marcada como número, rua com nome de pessoa abreviado parcialmente ou não (por exemplo Av. Get. Vargas), dentre tantas outras variações (que não são objeto do presente trabalho).

Assim, os dados disponíveis foram estruturados de forma a manter apenas o nome do endereço principal e os complementos (quadra, casa, lote, número, apto., etc) em colunas separadas. Identificados os possíveis endereços com repetição, os dados foram cruzados com os demais dados já obtidos referentes à espécie do benefício, os titulares e os inquéritos policiais nos quais os benefícios são investigados. Os resultados obtidos constam da Tabela 13.

Tabela 13

Endereços duplicados em benefícios de inquéritos da UF4

NB	Endereço	Espécie	Titulares	IPL
NB1575	Endereço1	88	Pessoa291	IPL720
NB1569	Endereço1	88	Pessoa873	IPL706
NB1781	Endereço2	88	Pessoa1009	IPL694
NB1787	Endereço2	88	Pessoa532	IPL701
NB1786	Endereço2	88	Pessoa627	IPL697
NB1361	Endereço3	80	Pessoa212	IPL1023
NB1378	Endereço3	80	Pessoa212	IPL1023
NB1377	Endereço3	80	Pessoa325	IPL1023
NB960	Endereço4	80	Pessoa912	IPL312
NB959	Endereço4	80	Pessoa912	IPL312
NB1009	Endereço5	21	Pessoa43	IPL517
NB1693	Endereço5	88	Pessoa947	IPL648
NB1594	Endereço6	88	Pessoa26	IPL683
NB1835	Endereço6	88	Pessoa869	IPL693
NB1658	Endereço7	88	Pessoa632	IPL495
NB828	Endereço8	88	Pessoa214	IPL403
NB1556	Endereço8	88	Pessoa491	IPL670

Fonte: autoria própria

Analisando os dados, foi possível observar que:

- a) o endereço1 consta em 2 benefícios investigados em 2 IPLs diferentes (IPL720 e IPL6);
- b) o endereço2 consta em 3 benefícios investigados em 3 IPLs diferentes (IPL694, IPL701 e IPL697);
- c) o endereço3 aparece em 3 benefícios diferentes, mas que já estão todos sendo investigados no mesmo inquérito;

- d) no mesmo sentido, o endereço4 aparece em 2 benefícios investigados no mesmo IPL312;
- e) o endereço5 aparece vinculado a 2 benefícios investigados em 2 IPLs diferentes (IPL517 e IPL648);
- f) o endereço6 aparece vinculado a 2 benefícios que são objeto de investigação em 2 inquéritos policiais (IPL683 e IPL693). Em pesquisa breve foram identificados outros 2 benefícios com o mesmo endereço 6 mas que não são objeto de investigação em inquéritos em andamento na UF4;
- g) no endereço7 foi identificado 1 benefício objeto do IPL495. Foram identificados outros dois benefícios cujos titulares declararam o mesmo endereço, mas estes não são objeto de investigação em inquéritos da UF4;
- h) no endereço8 foram identificados 2 benefícios que são investigados em 2 inquéritos diferentes. Em pesquisa breve foram identificados outros 4 benefícios cujos titulares declaram o mesmo endereço8, mas tais benefícios não são objeto de investigação em nenhum inquérito policial em andamento na UF4.

Com isso, foi possível observar que em uma amostra relativamente pequena de inquéritos policiais (128 inquéritos policiais sobre fraudes em benefícios da UF4), 14 inquéritos apresentaram algum tipo de vinculação por endereço com outras investigações, ou mesmo com outros benefícios que não são objeto de investigação, ao menos no momento em que foi feito o recorte para a presente análise.

5.3.5 Síntese dos resultados

Na **Etapa 1** foram mapeadas as redes criminosas formadas em sete operações de combate a fraudes contra a Previdência Social já concluídas. Essas operações investigaram crimes que representaram grande prejuízo financeiro ao erário, tendo sido fraudados diversos benefícios previdenciários. Os objetos, processos fraudados e valores aproximados de prejuízos a respeito das operações analisadas na Etapa 1 constam na Tabela 14.

Dos dados da Tabela 14, é possível ver que as operações abrangem vários tipos de benefícios fraudados, sendo o mais comum o de fraudes em benefícios da Lei Orgânica de Assistência Social – LOAS, sendo quatro das operações referentes a fraudes neste tipo de benefício. Observa-se ainda que o número de benefícios fraudados varia entre nove e 107 benefícios fraudados, sendo que o prejuízo estimado varia entre cerca de R\$650.000,00 indo

até R\$2.400.000,00. Observou-se ligeira diferença entre os dados divulgados na imprensa no momento da deflagração e os constantes dos relatórios. Tal divergência pode ser relativizada ante o fato de que, no momento da deflagração, ainda não se tem completa a produção e análise de provas. As medidas cumpridas no momento da deflagração, como a busca e apreensão, servem justamente para trazer para a investigação os elementos de prova, e somente posteriormente, com a análise das provas obtidas, é que se tem mais robustez quanto à prova produzida. Por tais motivos, optou-se por apresentar na Tabela 14 os dados obtidos no relatório das investigações, e não os divulgados à imprensa na deflagração.

Tabela 14

Operações deflagradas, objeto, processos fraudados e prejuízo

Operação	Objeto	Processos fraudados	Prejuízo
Fim de Linha	Pensão por morte, LOAS e outros	64	R\$ 897.145,90
Casa Cheia	LOAS	70	R\$ 1.650.000,00
Casa Cheia II	LOAS	107	R\$ 1.620.000,00
Intervenção	LOAS	34	R\$ 666.158,99
Intervenção II	LOAS	73	R\$ 2.400.000,00
Aquestos	Pensão por morte	9	R\$ 1.694.389,61
Duo Fratres II	Pós-óbito	107	R\$ 1.150.000,00

Fonte: Compilação de dados dos relatórios das investigações e matérias jornalísticas^{14 15 16 17 18 19 20}

Na Etapa 2 foi feita observação e comparação entre as redes observadas na Etapa 1. Observou-se que os grupos criminosos que atuam em fraudes previdenciárias apresentam sempre uma estrutura de rede básica, que é repetida por diversas vezes, enquadrando-se no critério legal que exige a prática reiterada de crimes. Com base nessa conclusão, foi sugerido um algoritmo de detecção/predição de fraudes, customizado às necessidades específicas da PF com base no algoritmo de Tayebi e Glasser (2016), conforme seção 5.2.

Na Etapa 3, o algoritmo foi testado em quatro unidades da Federação. Para estas unidades, foi feito o mapeamento completo dos inquéritos em andamento e que versam sobre investigações a respeito de crimes previdenciários. As redes foram mapeadas e analisadas

¹⁴ <http://g1.globo.com/ma/maranhao/noticia/2015/08/pf-prende-suspeitos-por-fraudes-que-custaram-r-950-mil-ao-inss-no-ma.html>

¹⁵ <http://g1.globo.com/ma/maranhao/noticia/2016/05/pf-cumpre-12-mandados-em-acao-contra-crimes-previdencia-rios-no-ma.html>

¹⁶ <http://www.pf.gov.br/agencia/noticias/2016/10/pf-combate-crimes-previdenciarios-no-maranhao>

¹⁷ <https://imirante.com/sao-luis/noticias/2017/04/11/policia-federal-cumpre-mandados-judiciais-em-operacao-contra-crimes-previdenciarios-no-maranhao.shtml>

¹⁸ <http://www.pf.gov.br/agencia/noticias/2017/04/pf-combate-crimes-previdenciarios-no-maranhao>

¹⁹ <http://www.previdencia.gov.br/2015/07/combate-as-fraudes-casal-de-estelionatarios-e-alvo-de-operacao-da-forca-tarefa-em-sao-luis-ma/>

²⁰ <https://g1.globo.com/ma/maranhao/noticia/pf-desarticula-quadrilha-que-desviou-r-115-milhao-da-previdencia-no-maranhao.ghtml>

conforme Apêndices I a IV, sendo geradas redes para os subgrupos de todos os atores de maior grau de centralidade. Foi então aplicado o algoritmo que identificou a repetição de díades compostas pelos atores APS-Servidor, apresentando os casos onde foi observada repetição de quatro ou mais vezes de uma mesma díade. Tal ocorrência foi entendida como indicativa da existência de grupo criminoso organizado, a ser confirmada ou rechaçada pelo trabalho investigativo.

Com os dados obtidos na Etapa 3, foi feito comparativo entre o número de inquéritos policiais identificáveis no mapeamento completo como apresentando conexões com outros inquéritos policiais, seja por apresentarem benefícios concedidos por um mesmo servidor ou em uma mesma agência da Previdência Social. Os números foram compilados na Tabela 15, de onde é possível constatar que a avaliação da repetição de vínculos identificou possíveis conexões, na média, em 58,5% dos inquéritos policiais, representando aproximadamente 1320 dos 2250 inquéritos policiais analisados.

Tabela 15

Percentual de IPLs identificáveis pelo modelo proposto

UF	IPLs na rede principal	IPLs em andamento na unidade	IPLs sobre fraudes em benefícios	Percentual de IPLs identificáveis pelo modelo-base proposto:	
				% do total de IPLs UF:	% dos IPLs de fraude em benefício:
UF1	137	385	274	35,6%	50,0%
UF2	158	224	195	70,5%	81,0%
UF3	593	979	766	60,6%	77,4%
UF4 ²¹	128	599	503	21,4%	25,4%
Geral	1016	2187	1738	46,5%	58,5%

Fonte: autoria própria

Aplicado o algoritmo proposto, foi possível realizar a identificação de grupos criminosos atuando em investigações atuais com as mesmas características de grupos criminosos organizados observados em investigações anteriores. Os quantitativos de grupos identificados constam da Tabela 16.

²¹ Na UF4 a análise não abrangeu todos os inquéritos de benefícios, conforme detalhado na seção 4.3.4

Tabela 16
Quantitativos de grupos identificados pelo algoritmo

Local	Deteccões totais	NBs vinculados	IPLs vinculados	Grupos detectados
UF1	12	65	32	9
UF2	10	81	4	5
UF3	40	101	55	18
UF4	14	82	8	5
Total	76	329	99	37

Fonte: autoria própria

Buscou-se uma estimativa para analisar a percentagem de detecção de grupos criminosos, tendo sido levantados os dados da tipificação inserida no cadastro do inquérito policial. Essa informação é cadastrada no início das investigações, então é comum que haja modificações à medida que as provas vão sendo produzidas. Assim, existem inquéritos que não começaram buscando a comprovação de atuação de grupos criminosos, mas que acabam chegando a tal conclusão e de outro existem inquéritos que começam para verificar a existência de grupos criminosos, o que acaba não sendo comprovado com as investigações. Nesse sentido, o número de investigações cadastradas no sistema de controle parece ser uma boa baliza indicativa do mínimo de inquéritos onde são investigados grupos criminosos, não sendo possível fixar a quantidade exata ou máxima, posto que depende das provas produzidas em cada investigação.

Isto posto, buscou-se no sistema de controle de inquéritos (Siscart) a tipificação provisória cadastrada nos inquéritos policiais das unidades da Federação analisadas. Foram localizados inquéritos com a tipificação da associação criminosa (art. 288 do Código Penal) em dez inquéritos policiais da UF1, em dois inquéritos policiais da UF2, em 14 inquéritos policiais da UF3 e em nenhum inquérito policial da UF4. Destes, apenas dois inquéritos da UF1 eram sobre fraudes em custeio e todos os demais eram sobre fraudes em benefícios.

Conforme dados da Tabela 16, foram identificados inquéritos relacionados a grupos criminosos no total de nove inquéritos policiais na UF1, cinco inquéritos policiais na UF2, 18 inquéritos policiais na UF3 e cinco inquéritos policiais na UF4. Com isso, é possível afirmar que o algoritmo detectou mais inquéritos policiais com atuação de grupos criminosos do que há anotação no sistema eletrônico de controle (Siscart).

A análise visual das redes dos subgrupos apresentadas nos Apêndices I a IV permite identificar a ocorrência de vários inquéritos policiais com indicativo de atuação de grupos

criminosos. Os inquéritos policiais constantes dos subgrupos analisados nos apêndices foram também detectáveis pelo algoritmo, sendo tal resultado esperável, uma vez que os inquéritos mapeados para formação das redes dos Apêndices I a IV possuem o perfil que o algoritmo se propõe a detectar, qual seja, investigações sobre fraudes em benefícios praticados por grupos criminosos formados a partir da repetição de uma estrutura de rede básica.

Apresentados os resultados, passa-se na próxima seção à sua análise à luz dos aspectos teóricos levantados no referencial teórico.

6. DISCUSSÃO E IMPLICAÇÕES DOS RESULTADOS

Na Etapa 1 foi feito o mapeamento de redes em operações de combate a crimes previdenciários já concluídas. A análise de redes de organizações criminosas pode ajudar a identificar sua estrutura e lideranças (Musotto, 2016; Calderoni, 2017), ajudando a entender as conexões entre os perfis criminais (Mastrobuoni & Patacchini, 2012), sendo que a metodologia da ARS tem sido utilizada para a compreensão de grupos criminosos (Zhao, 2009) e no auxílio ao trabalho policial (Duvenage, 2010).

O mapeamento da estrutura de organizações criminais a partir dos dados de operações policiais já foi utilizado em trabalhos anteriores, como por Calderoni (2014) para o mapeamento da rede da *N'drangheta*, formada na região da Calábria, também objeto de análise por Berlusconi (2016), com dados de outra operação policial contra o mesmo grupo. A análise de redes de grupos criminosos por meio de dados de operações policiais se mostra também como útil como forma de superar o fato que os vínculos entre criminosos muitas vezes se apresentam de forma incompleta, incorreta ou inconsistente, por se tratar de atividade ilegal onde os envolvidos procuram formas de ocultar suas relações (Xu & Chen, 2005)

Embora não seja o objetivo do trabalho, foi feita uma compilação dos dados sobre número de servidores envolvidos, número de não-servidores indiciados (responsabilizados) e o número de benefícios fraudados, os quais foram analisados em relação ao prejuízo detectado em cada operação (dados da seção 5.3.5). Mesmo não sendo o quadro ideal em razão do pequeno tamanho da amostra, foi feito um esboço de regressão múltipla com os dados disponíveis, que apontam no sentido que a presença de um servidor do INSS no grupo criminoso faz o prejuízo aumentar em quase um milhão de reais (por servidor envolvido), ao passo que cada benefício fraudado gera prejuízo em média de cerca de R\$23.000,00 (vinte e três mil reais). A memória de cálculo é apresentada no Apêndice V e sugere-se como lacuna de pesquisa o aprofundamento de métodos de regressão múltipla para identificação de fatores que influenciam no prejuízo gerado por organizações criminosas (no caso, uma forma de medição de “desempenho”).

Com base nos dados observados nas operações já concluídas, na Etapa 2 foi identificado que os grupos criminosos objeto das operações policiais analisadas eram constituídos seguindo o conceito biológico da metameria, ou seja, é formado uma rede básica capaz de cometer uma fraude em benefício e essa estrutura é repetida por diversas vezes, passando a formar um grupo criminoso organizado. A utilização da ARS para mapeamento de redes criminosas e criação de modelagem padrão também já foi explorada na literatura revisada

(Bright et al, 2015), podendo auxiliar na criação de melhores processos, técnicas e ferramentas para auxiliar o trabalho policial (Petersen & Wiil, 2013), especialmente para vencer o novo desafio gerado com a necessidade de tratamento do volume cada vez maior de informações para conseguir extrair conteúdo útil (Sudhahar et al, 2015; Rasheed; Wiil & Niazi, 2015).

Tem-se ainda que as organizações criminosas possuem o dinamismo inerente às organizações informais, sendo necessário que as agências de aplicação da lei sejam capazes de se adaptar a elas (Gadekar, 2017), ante o que é inevitável a utilização de ferramentas informáticas em apoio ao trabalho policial posto que “à medida que a complexidade dos crimes aumenta, ocorrem erros humanos, o tempo de análise aumenta e os criminosos têm mais tempo para destruir provas e escapar da prisão” (Chen et al, 2004).

Identificada a rede básica de constituição dos grupos criminosos organizados atuantes em fraudes previdenciárias, passou-se à elaboração e proposição de sequência lógica de ações para a detecção ou predição de ações de grupos criminosos organizados, chegando-se ao algoritmo proposto na seção 5.2, elaborado a partir de customização do algoritmo proposto por Tayebi e Glasser (2016). Esses mesmos autores analisaram redes de coautoria criminal a partir de dados de ocorrências policiais no Canadá (Tayebi & Glasser, 2011; 2012).

Algoritmos de detecção ou predição de atividade tem sido objeto de análise da literatura, por exemplo, com a análise do algoritmo COPLINK, desenvolvido pela Universidade do Arizona (EUA), feita por Nissan (2012) e que concluiu que a ferramenta se mostrou como eficiente na identificação de ligações entre pessoas, embora o faça a partir de dados estruturados. A mesma ressalva pode ser aplicada ao algoritmo aqui proposto, eis que também faz a detecção a partir de dados estruturados. Para suprir essa limitação, Alzaidy (2010) sugere a necessidade de ferramentas que façam a mineração e classificação automatizadas de dados de inteligência sobre redes criminosas para alimentar os bancos de dados da polícia e possibilitar o posterior cruzamentos destes, sendo também necessário aprimorar a forma de compartilhamento de informações na aplicação da lei por várias agências e órgãos (Hollywood et al, 2015).

A identificação dessa estrutura de composição por meio da repetição de uma rede básica levou ao mapeamento da rede de maneira a buscar as díades APS-Servidor vinculadas aos inquéritos policiais por meio de números de benefícios fraudados. Com isso, a rede detectada passou a possuir características que se enquadram melhor na classificação que a ARS denomina de redes diádicas de dois modos por afiliação. Ao falar sobre as redes de afiliação, Wassermann e Faust (1994) definem que essas redes, apesar de terem atores de grupos diferentes, fazem parte de uma mesma entidade social de forma que o contato entre os

indivíduos que fazem parte dessa mesma entidade torna-se mais provável. Trazendo a ideia para o objeto de estudo, quando a díade APS-Servidor tem mais vínculos (em um ou em vários inquéritos) isso faz com que essa díade ganhe centralidade na rede, fato que foi compreendido como possível indicativo da atuação de grupo criminoso organizado (sujeito a confirmação por investigação policial mais aprofundada). As matrizes de correlação das redes por afiliação das UF1, UF2, UF3 e UF4 constam dos Apêndices I a IV.

Na Etapa 3 foi feito o mapeamento de investigações em andamento, analisando as redes observadas e aplicando o algoritmo proposto buscando verificar a detecção proposta na prática. Na avaliação, foram identificadas possíveis conexões entre 58,5% das investigações em andamento e foram identificados 37 proáveis grupos criminosos organizados (sendo nove na UF1, cinco na UF2, 18 na UF3 e cinco na UF4). Todos os grupos criminosos observáveis nas redes mapeadas (e constantes dos Apêndices I a IV) foram detectados pelo algoritmo proposto.

Na literatura revisada, o objeto mais próximo do assunto identificado foi com a utilização de algoritmos para detecção de fraudes contra o sistema previdenciário da Bélgica. A principal diferença é que o algoritmo ali analisado busca identificar fraudes em custeio, cometidas por empresas que não pagam devidamente as contribuições previdenciárias, enquanto o algoritmo proposto no presente trabalho visa a detecção de grupos criminosos atuantes em fraudes em benefícios. Feita esta distinção, anota-se que foi identificada a utilização da ARS para identificar fraudes contra o sistema previdenciário da Bélgica com um modelo que chamou de “*spider construction*” (Van Vlasselaer et al, 2013), depois feito novo estudo avançando para o modelo denominado Afraid (Van Vlasselaer et al, 2015), que teria produzido melhoria de 15% em relação a modelos manuais de análise para detecção de fraudes. Foi identificado ainda naquele ambiente a análise do algoritmo Gotcha! (Van Vlasselaer et al, 2016) o qual teria ampliado para 55% a detecção de fraudes, aplicando-se tanto a fraudes pretéritas quanto à predição de futuras fraudes por empresas, estando no mesmo sentido do trabalho de Baesens, Van Vlasselaer e Verbeke (2015).

Analisando o desempenho de métodos de detecção de fraudes, Gadekar (2017) aponta que performance e precisão são inversamente proporcionais, ou seja, os métodos de melhor performance não apresentam boa precisão, enquanto os métodos mais precisos pecam pela baixa robustez. Nessa linha, entende-se que o algoritmo proposto guarda posição mediana nos dois critérios, pois apresentou boa taxa de detecção, mas o fez em ambiente onde a probabilidade de confirmação da fraude é bem maior. Nesse ponto, necessário esclarecer que a detecção foi testada em investigações já em andamento, parecendo razoável afirmar que um benefício que já é objeto de inquérito policial em andamento apresenta probabilidade de ser

fraudado muito maior que um benefício escolhido aleatoriamente na base de dados do INSS. E nesse ponto as possibilidades de avanço na detecção de fraudes são imensas: o aumento da troca de informações entre a PF e o INSS, no âmbito das Forças-Tarefa por exemplo, por aumentar a base de dados de detecção de fraudes, na medida em que muitas dos processos que apresentam falhas (sejam por erro ou por fraude) acabam sendo resolvidos em processos administrativos no INSS, sequer chegando ao conhecimento da polícia.

Esse incremento na base de dados pesquisada pode levar à identificação de vínculos ainda maiores que os aqui relatados, o que parece promissor em termos de aumento da detecção da atuação de grupos criminosos e que, em última análise, podem auxiliar na identificação de todos os envolvidos e responsabilização dos verdadeiros líderes dos grupos criminosos e não apenas dos empregados, eis que o combate efetivo às organizações criminosas somente ocorre quando são identificados os membros mais influentes e de alto nível (Taha, 2019).

Do ponto de vista da PF, o algoritmo seria de implementação relativamente simples, mas envolveria a adoção de algumas providências. A primeira delas seria buscar uma forma de estruturar a informação a respeito dos números dos benefícios investigados, para que tal informação possa ser facilmente resgatável e utilizada para cruzamentos de informações. Seria necessário também fazer com que os bancos de dados do INSS se comuniquem com a PF a fim de trazer de maneira automatizada as informações a respeito de tais benefícios como servidores envolvidos no processo, agência de concessão e de manutenção, por exemplo, informações que o INSS possui e fornece por meio das Forças-Tarefa, mas que precisa ser consultada manual e individualmente.

Em funcionamento, vislumbra-se que o algoritmo proposto, além da função primária de detecção ou predição de organizações criminosas, pode ser utilizado para situações como: a) consulta a respeito da existência de inquéritos em andamento quando analisadas novas notícias de crime, melhorando a qualidade da consulta por meio da identificação de vínculos anteriormente ocultos; b) identificação de investigações em duplicidade ou conexas, para as investigações já em andamento; c) análise de investigações que se expandem e acabam se sobrepondo, ressaltando que neste caso e no do item anterior essa identificação pode ser feita inclusive entre unidades de localidades diferentes; d) identificação de inquéritos a respeito de operações que foram deflagradas e as investigações ainda não foram concluídas.

A respeito do último ponto, observou-se durante as análises das redes constantes dos Apêndices I a IV, que havia pontos de concentração referentes a inquéritos policiais que serviram de base para operações deflagradas. Isso ocorre porque, apesar de já ter ocorrido a deflagração, as investigações ainda não foram concluídas. A inclusão destes inquéritos na rede

mapeada mostrou relevância posto que é possível que outros inquéritos em andamento estejam também vinculados àquelas investigações e tal vínculo não tenha sido até aquele momento percebido.

Analisando tais inquéritos, identificou-se que, em alguns casos de operações de combate a fraudes contra a Previdência Social, havia uma investigação principal (original) onde eram investigados e responsabilizados os membros principais do grupo criminoso (financiadores do grupo, servidores envolvidos, agenciadores, etc). Depois desse primeiro passo, o INSS realizava auditoria em todos os benefícios fraudados pelo grupo criminoso. À medida que o INSS ia realizando as auditorias, os relatórios destas eram encaminhados à PF, que instaurava um inquérito policial para investigar cada titular de benefício fraudado. Esses inquéritos eram chamados informalmente de “filhotes” ou de “rescaldo”. Por serem focados nos titulares dos benefícios, e não nos líderes dos grupos criminosos, esses inquéritos acabavam gerando um volume muito grande de trabalho e tinham pouco impacto na redução de novas ocorrências, eis que a identificação dos líderes ou membros mais sensíveis e cuja remoção poderia desarticular a rede (Ferrara et al, 2014) já estava sendo tratada em outra investigação.

Diante de tal contexto, o Ministério Público Federal (MPF) editou a Orientação Normativa nº 36 de 26 de setembro de 2018, que orienta os representantes do MPF a pedirem o arquivamento de inquéritos policiais de “rescaldo” nos quais o MPF entenda que os fatos: a) não modificam o panorama probatório atual; b) não são suficientes para um aumento substancial das penas dos investigados na operação originária; c) dizem respeito às condutas dos titulares dos benefícios, salvo quando encerrarem alto grau de reprovabilidade, como a magnitude da lesão; d) nada acrescentam acerca das condutas dos servidores e intermediadores já investigados; e) não apresentam indícios da participação de outros servidores e/ou intermediadores, além dos já investigados no IPL de origem (MPF, 2018). Com tal medida, espera-se diminuição dos inquéritos policiais fruto de “rescaldo” de operações de combate a fraudes em benefícios previdenciários, o que liberaria recursos humanos e materiais pra atuação em outros trabalhos.

Como abordagem complementar na Etapa 3 foi realizada a busca por processos de benefícios que estão sob investigação e cujos titulares apresentem endereços semelhantes. Essa abordagem foi feita com certas características exploratórias, especialmente diante do contido nas operações Casa Cheia e Casa Cheia II. Foram analisados os endereços de titulares de benefícios investigados em 128 inquéritos policiais, tendo sido identificados 14 inquéritos onde os endereços apresentaram algum tipo de vinculação. A abordagem apresentou grande dificuldade de implementação em razão das muitas formas diferentes de endereçamento aceitas

nos sistemas. Assim, a identificação de vínculos por meio do endereçamento parece caminho promissor, com cerca de 11% de casos vinculados sendo necessário, contudo, que seja buscada alguma forma de padronização de endereçamento ou mesmo de técnica de mineração de dados que possa identificar e reconhecer quando duas anotações diferentes se referem ao mesmo endereço (“R. Padre João Vieira Santos, nr. 23” é o mesmo endereço que “Rua Pe. João V. Santos, 23, por exemplo).

Anota-se ainda que durante o processo de análise das variáveis dos atores da rede, observou-se que as variáveis grau de centralidade e intermediação abrangiam os principais atores da rede. Em outras palavras, os atores que apresentaram maiores valores nestas duas variáveis foram os principais atores da rede, de forma que as medições feitas para as demais variáveis apresentavam correlação positiva com estas e foram mantidas no trabalho para melhor detalhamento das medições feitas.

7. CONSIDERAÇÕES FINAIS

O objetivo geral do trabalho passava por descrever a estrutura de relacionamentos de redes de grupos criminosos em investigações anteriores (operações) da Polícia Federal sobre crimes previdenciários a fim de propor um modelo de detecção/predição de redes de grupos criminosos em investigações atuais e futuras, passando pelos objetivos específicos de: a) Identificar e selecionar operações anteriores a 2019 da PF de combate a fraudes previdenciárias para análise de suas redes; b) Identificar uma rede básica que se aplique aos grupos criminosos já detectados anteriormente e que atuavam em crimes previdenciários, delineando algoritmo de detecção ou predição de grupos criminosos; e c) Testar o algoritmo delineado em redes de investigações atuais da PF em quatro diferentes unidades da Federação.

A identificação das redes formadas por grupos criminosos em operações anteriores foi feita conforme consta da Seção 5.1, tendo sido mapeadas e detalhadas as redes em sete operações de combate a fraudes previdenciárias, atingindo o primeiro objetivo específico. Da análise dos dados de tais operações foi possível identificar uma rede básica, sendo identificado que os grupos criminosos observados se formaram, em regra, a partir da repetição desta rede básica, sendo então delineado algoritmo de detecção/predição de tais grupos criminosos (Tabela 12), baseado no algoritmo de Tayebi e Glosser (2016), atingindo-se o segundo objetivo específico, conforme descrito na Seção 5.2.

Foi feito o mapeamento das redes formadas em investigações em andamento a respeito de crimes previdenciários em quatro unidades da federação, sendo mapeados aproximadamente 2.250 inquéritos policiais e aplicado o algoritmo delineado na etapa anterior. Mapeadas as redes, foi aplicado o algoritmo de detecção de grupos criminosos, sendo detectados 37 prováveis grupos criminosos organizados (sendo nove na UF1, cinco na UF2, 18 na UF3 e 5 na UF4), sendo atingido o terceiro objetivo específico. Por fim, na conclusão do trabalho, é aqui proposta a adoção de modelo de detecção/predição de grupos criminosos organizados baseado no algoritmo da Tabela 12, atingindo-se o último objetivo específico e o objetivo geral do trabalho.

Tratando-se de algoritmo, o mesmo pode ser implementado de diferentes maneiras pela PF, por exemplo, por meio de ferramentas informáticas de *business intelligence* que podem aliar o alto poder de processamento dos computadores atualmente disponíveis a interfaces amigáveis para os usuários policiais, realizando o trabalho mecânico de cruzamento de alto volume de informações retornando resultado que sirva de guia para as autoridades públicas

responsáveis pela avaliação de possíveis fraudes ou crimes contra a Previdência Social. E em consequência disso, as investigações podem passar a ser otimizadas ou priorizadas com base em critérios objetivos, com bases científica e estatística, alocando os recursos disponíveis onde possam proporcionar os melhores resultados possíveis.

Os resultados obtidos foram convergentes com a literatura revisada, tendo a estrutura do trabalho sido baseada em observações do passado para otimizar o trabalho policial na prevenção de novas ocorrências (Borowik, Wawrzyniak & Cichosz, 2018). O presente estudo inova ao estudar empiricamente e por meio da ARS a atuação de grupos criminosos organizados que praticam fraudes contra a Previdência Social bem como agrega conhecimento aos algoritmos de detecção/predição de grupos criminosos com o teste prático de aplicação do algoritmo em investigações já existentes no âmbito da PF no Brasil.

Apesar das dificuldades gerais encontradas na estruturação dos dados, foi possível apontar possível vínculo entre 58,5% das investigações em andamento, seja porque os benefícios investigados possuem o mesmo servidor concessor, seja porque os benefícios foram concedidos em uma mesma Agência do INSS. Conforme descrito, foi ainda possível identificar 37 prováveis grupos criminosos organizados envolvidos nas investigações analisadas. Nesse sentido, o algoritmo proposto pode alcançar resultados ainda maiores porquanto, em casos reais e até mesmo nas operações analisada, foi observado que, identificado um dos pontos de atuação de grupos criminosos organizados, o desdobramento das investigações acaba descobrindo vários outros benefícios fraudados pelo mesmo grupo e que sequer eram objeto de investigação. Em outras palavras, identificada a repetição da rede básica, a busca por outros processos envolvendo as mesmas pessoas pode levar à identificação de várias outras fraudes até então desconhecidas.

A contribuição teórica do presente trabalho consiste no aprofundamento do estudo das organizações criminosas utilizando a metodologia da análise de redes sociais, com foco no estudo de fraudes praticas em benefícios, matéria sobre a qual não foram identificados trabalhos nos estratos superiores de publicação.

A contribuição prática do trabalho reside na indicação de algoritmo que pode não só incrementar a identificação e/ou detecção de grupos criminosos atuantes na área de fraudes contra a Previdência Social, mas também possibilitar a alocação de recursos de forma a maximizar o trabalho da PF no combate a tais grupos criminosas com base em critérios objetivos e com metodologia científica. Em tal contexto, a implementação por parte da PF do algoritmo proposto pode trazer frutos, na medida em que o modelo se mostrou viável para a identificação de vinculos entre diferentes fraudes como indicativos da possível atuação de

grupos criminosos organizados, sendo que essa verificação poderia ser implementada tanto no momento da análise de viabilidade de instauração de inquérito policial quanto posteriormente, por ocasião de retorno do inquérito à esfera policial com dilação de prazo. Implementado o sistema de consulta, o processo pode facilmente ser automatizado, sendo contudo necessárias algumas providências conforme discussão na seção de resultados. A predição/detecção de participação de servidores nos grupos criminosos ganha especial relevância quando se percebe o potencial poder de impacto do envolvimento de servidores, sendo que os dados iniciais apontam no sentido que cada servidor envolvido faz aumentar em cerca de um milhão de reais o prejuízo causado aos cofres públicos.

Sob outro ponto de vista, a definição de modelos e algoritmos de análise de atuação de grupos criminosos organizados pode (e deve) ser estendida a outras esferas. Com isso, futuras pesquisas podem buscar em grupos criminosos organizados a identificação de outras estruturas básicas de rede que se repetem ou outras formas de composição. Uma análise que parece viável é a busca de pontos de convergência a serem utilizados para identificação de conexões de grupos criminosos atuantes em áreas como fraudes a pagamentos de Requisições de Pequeno Valor - RPV, seguro desemprego (o qual, a despeito de ter essência trabalhista, guarda muitas semelhanças com as fraudes previdenciárias), contrabando/descaminho, dentre outras, podendo o algoritmo aqui proposto ser customizado em várias áreas de atuação do órgão. Em outra linha, a pesquisa aqui apresentada pode ser ampliada buscando-se, também em operações já realizadas, outras formas de composição de grupos criminosos organizados ou atuantes em outras áreas.

REFERÊNCIAS

- Agarwal, P. K. (2018). Public Administration Challenges in the World of AI and Bots. *Public Administration Review*, 00, 1-5. <https://doi.org/10.1111/puar.12979>
- Albanese, J. S. (1982). What Lockheed and La Cosa Nostra have in common: The effect of ideology on criminal justice policy. *Crime & Delinquency*, 28(2), 211-232.
- Almeida, D. M. J. D. (2019). *Fraudes na Previdência e Assistência Social: uma avaliação da eficácia das operações policiais no estado do Maranhão*.
- Alzaidy, R. (2010). *Criminal Network Mining and Analysis for Forensic Investigations* (Doctoral dissertation, Concordia University).
- Anesi, C; Rubino, G & Adorno, L. (2018). O PCC e a máfia italiana. Recuperado de <https://noticias.uol.com.br/reportagens-especiais/os-negocios-do-pcc-com-a-mafia-italiana>.
- Augustinis, V. F. D. (2011). *Gestão em redes para a construção de políticas públicas: um estudo sobre as atividades e prevenção e repressão à lavagem de dinheiro no Brasil* (Doctoral dissertation).
- Azevedo, R. G. D., & Sinhoretto, J. (2018). O sistema de justiça criminal na perspectiva da antropologia e da sociologia. *Revista brasileira de informação bibliográfica em ciências sociais-bib*, v. 1, p. 188-215, 2018.
- Baccara, M., & Bar-Isaac, H. (2008). How to organize crime. *The Review of Economic Studies*, 75(4), 1039-1067.
- Baesens, B., Vlasselaer, V. V., & Verbeke, W. (2015). *Fraud Analytics using descriptive, predictive and social network techniques. A guide to data science for fraud detection*. New Jersey, USA: John Wiley & Sons.
- Bahulkar, A., Baycik, N. O., Sharkey, T., Shen, Y., Szymanski, B., & Wallace, W. (2018). Integrative analytics for detecting and disrupting transnational interdependent criminal smuggling, money, and money-laundering networks. In 2018 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE.
- Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., & Piccardi, C. (2016). Link prediction in criminal networks: A tool for criminal intelligence analysis. *PloS one*, 11(4).
- Bez, G. S., Faraco, R. A., & Angeloni, M. T. (2010). Aplicação da técnica de análise de redes sociais em uma instituição de ensino superior. XXVI simpósio de gestão da inovação tecnológica, 1-16.
- Borowik, G., Wawrzyniak, Z. M., & Cichosz, P. (2018). Time series analysis for crime forecasting. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-10). IEEE.
- Brand, F. C., & Verschoore, J. R. (2014). A utilização de medidas de análise de redes sociais nas pesquisas em administração. *Revista Economia & Gestão*, 14(35), 212-237.
- Brandão, T.S. (2015). *Redes Sociais Da Criminalidade No Sistema Penitenciário Brasileiro: Estudo De Caso*. *Revista Caribeña de Ciencias Sociales*, (2015_10).

Brasil (1940). Código Penal. Recuperado de http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

_____. (1941). Código de Processo Penal. Recuperado de http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm

_____. (1988) Constituição da República Federativa do Brasil de 1988 (1988). BRASIL. Recuperado de http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm

_____. (2004). Decreto nº 5.015 de 12 de março de 2004. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm

_____. (2006). Lei nº 11.343 d23 de agosto de 2006. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111343.htm

_____. (2010) Projeto de Lei no 8.045, de 2010, Pub. L. No. Projeto, 2010 (2010). Recuperado de http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1668776&filename=Tramitacao-PL+8045/2010

_____. (2012). Lei ° 12.694 de 24 de julho de 2012. Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12694.htm

_____. (2013). Lei nº 12.850 de 2 de agosto de 2013. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm

_____. (2019). Proposta de Emenda à Constituição 6/2019. Recuperado de https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=DC0CADE4DBD7A086C9E705E0630834BA.proposicoesWebExterno2?codteor=1712459&filename=PEC+6/2019

Bright, D. A., Greenhill, C., Reynolds, M., Ritter, A., & Morselli, C. (2015). 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*, 31(3), 262-278.

Calderoni, F., & Piccardi, C. (2014). Uncovering the structure of criminal organizations by community analysis: The infinito network. In 2014 Tenth International Conference on Signal-Image Technology and Internet-Based Systems (pp. 301-308). IEEE.

Calderoni, F., Brunetto, D., & Piccardi, C. (2017). Communities in criminal networks: A case study. *Social Networks*, 48, 116-125.

Chang, J. (2015). The maturity model in practice: chaos, reaction, evolution, and inclusion in law enforcement analytic models. *Police Practice and Research*, 16(2), 108120.

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: A general framework and some examples. *Computer*, 37(4), 50-56. <https://doi.org/10.1109/MC.2004.1297301>

Chuy, J. F. M. (2018). As redes sociais e a promoção de organizações terroristas: a resposta contraterrorista brasileira (Doctoral dissertation).

CNJ (2006). Recomendação nº 3 de 30 de maio de 2006. Recuperado de <https://atos.cnj.jus.br/atos/detalhar/855>

- Cocx, T. K., Kusters, W. A., & Laros, J. F. (2008). Enhancing the automated analysis of criminal careers. In *SIAM Workshop on Link Analysis, Counterterrorism, and Security* (Vol. 2008).
- Collins, R. (1988). *Theoretical sociology*. Harcourt College Pub.
- Cordeiro, M. P., Curado, J., & Pedrosa, C. (2014). Pesquisando redes heterogêneas: contribuições da teoria ator-rede. *A produção de informação na pesquisa social: compartilhando ferramentas*. Centro Edelstein de Investigações Sociais.
- Crocker, R., Skidmore, M., Webb, S., Garner, S., Gill, M., & Graham, J. (2019). Uncovering organized shoplifting and theft networks. *Policing: A Journal of Policy and Practice*, 13(4), 377-385.
- Cruz, A. P. G. (2013) Encontro Internacional Participação, Democracia e Políticas Públicas: aproximando agendas e agentes 23 a 25 de abril de 2013, UNESP, Araraquara (SP).
- Daniele, G., & Geys, B. (2015). Organised crime, institutions and political quality: Empirical evidence from italian municipalities. *The Economic Journal*, 125(586), F233-F255.
- Devan, S. & Gangadharan, S. (2014). Crime analysis and prediction using data mining. In *2014 First International Conference on Networks & Soft Computing (ICNSC2014)* (pp. 406-412). IEEE.
- Diniz, M. H. (2008). *Dicionário jurídico*.
- Duvenage, M. A. (2010). *Intelligence analysis in the knowledge age: An analysis of the challenges facing the practice of intelligence analysis* (Doctoral dissertation, Stellenbosch: University of Stellenbosch).
- Fedro, G. I. (1823). *Fábulas de Fedro, liberto de Augusto*. Traducidas de latin á castellano. Barcelona: Sierra e Martí.
- Ferrara, E., De Meo, P., Catanese, S., & Fiumara, G. (2014). Detecting criminal organizations in mobile phone networks. *Expert Systems with Applications*, 41(13), 5733-5750.
- Ferreira Júnior, N & Paiva, P.C. (2005). *Introdução à zoologia*. Rio de Janeiro: Fundação Cecierj.
- Fossati, M. (2020) "Narcosur": a aliança entre a máfia italiana (ou calabresa) e o PCC. Recuperado de <https://www.gazetadopovo.com.br/republica/trafico-drogas-narcosur-alianca-mafia-italiana-pcc/>.
- Freitas, M. C., & Pereira, H. D. B. (2005). Contribuição da análise de redes sociais para o estudo sobre os fluxos de informações e conhecimento. *Proceedings CIFORM-Encontro Nacional de Ciência da Informação VI*, Salvador-BA.
- Gadekar, D. P. (2017). Study and analysis of online social networking mining and security methods 1 1, 2(4), 450-453.
- Garbi, F. (2019). Conversão de investigações comuns em operações policiais federais.
- Garoupa, N. (2007). Optimal law enforcement and criminal organization. *Journal of Economic Behavior & Organization*, 63(3), 461-474.

- Gilmour, S. (2008). Understanding organized crime: a local perspective. *Policing: A journal of policy and practice*, 2(1), 18-27.
- Gomes, L. F., & Silva, M. R. D. (2015). *Organizações criminosas e técnicas especiais de investigação: questões controvertidas, aspectos teóricos e práticos e análise da Lei 12.850/2013*. Salvador: JusPODIVM.
- Gottschalk, P., & Smith, C. (2016). Detection of white-collar corruption in public procurement in Norway: The role of whistleblowers.
- Granovetter, M. (1973). The strength of weak ties. *Am. J. Sociol.* 78:1360-1380.
- Gunnell, D., Hillier, J., & Blakeborough, L. (2016). Social network analysis of an urban street gang using police intelligence data. Home Office.
- Habib, G (2018). *Leis penais especiais*. Salvador: Juspodivm.
- HMIC (2015). A review of the fitness for purpose of the current structure of policing in england & wales. Retrieved from <https://www.justiceinspectores.gov.uk/hmicfrs/media/closing-the-gap-20050911.pdf>.
- Hollywood, J. S., Boon Jr, J. E., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015). High-priority information technology needs for law enforcement. Rand Corporation.
- IBM (2017). Centralidade e medidas de centralidade. Recuperado de https://www.ibm.com/support/knowledgecenter/pt-br/SS3J58_9.0.8/com.ibm.i2.anb.doc/sna_centrality.html.
- INSS (2017). Breve histórico. Recuperado de <https://www.inss.gov.br/aceso-a-informacao/institucional/breve-historico/>
- Johnson, J., Reitzel, J. D., Norwood, B., McCoy, D., Cumming, B., & Tate, R. (2013). Social network analysis: A systematic approach for investigating. *FBI Law Enforcement Bulletin*. Available at <https://leb.fbi.gov/2013/march/social-network-analysis-a-systematic-approach-for-investigating>, 350.
- Katsaros, D., Dimokas, N., & Tassiulas, L. (2010). Social network analysis concepts in the design of wireless Ad Hoc network protocols. *IEEE Network*, 24(6), 23-29. doi:10.1109/mnet.2010.5634439
- Leighton-Daly, M. (2018). Identity Theft and Tax Crime: Has Technology Made It Easier to Defraud the Revenue. *eJTR*, 16, 578.
- Lenz, H. J. (2014). Data Fraud Detection: A First General Perspective. In *International Conference on Enterprise Information Systems* (pp. 14-35). Springer, Cham.
- Libório, B. & Menezes, L F. (2018). *Ciro subestima tamanho do efetivo da PF e exagera poder de compra sob Lula*. Recuperado de <https://aosfatos.org/noticias/ciro-subestima-tamanho-do-efetivo-da-pf-e-exagera-poder-de-compra-sob-lula/>
- Lima, R. B. (2017). *Manual de Processo Penal-Volume Único*. Salvador: Editora Jus Podivm.
- Lin, S., & Brown, D. E. (2002). Outlier detection and data association for data mining criminal incidents. *WIT Transactions on Information and Communication Technologies*, 28.

Marin, A., & Wellman, B. (2011). Social network analysis: An introduction. The SAGE handbook of social network analysis, 11.

Marselli, R., & Vannini, M. (1997). Estimating a crime equation in the presence of organized crime: evidence from Italy. *International Review of Law and Economics*, 17(1), 89-113.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), 803-814.

Masson, C., & Marçal, V. (2018). Crime organizado . Grupo Gen-Editora Método Ltda..

Mastrobuoni, G., & Patachini, E. (2012). Organized crime networks: An application of network analysis techniques to the American mafia. *Review of Network Economics*, 11(3).

Mathimagal, N. M. (2018). Social Network Analytics (SNA) Fraud, 118(20), 191-202.

Michalak, T. P., Rahwan, T., & Wooldridge, M. (2017). Strategic social network analysis. In *Thirty-First AAAI Conference on Artificial Intelligence*.

Mischen, P. A., & Jackson, S. K. (2008). Connecting the dots: Applying complexity theory, knowledge management and social network analysis to policy implementation. *Public Administration Quarterly*, 314-338.

MJSP (2017). Portaria 1.252 de 20 de novembro de 2017. Regimento interno da Polícia Federal. Recuperado de <http://www.pf.gov.br/institucional/acessoainformacao/institucional/regimento-interno-da-policia-federal-1>.

Morgan, G. (1996). *Imagens da Organização*. São Paulo: Atlas.

Moro, S.F. (2016) A justiça e os decaídos. Recuperado de <https://opinioao.estadao.com.br/noticias/geral,a-justica-e-os-decaidos,10000054313>

MPF (2018). Orientação nº 36 de 26 de setembro de 2018. Recuperado de http://www.mpf.mp.br/atuacao-tematica/ccr2/orientacoes/documentos/orientação-no-36-orienta_sobre_arquivamento-rescaldos.pdf.

Musotto, R. (2016) Social and spatial network analysis of organised crime (Doctoral dissertation, Università DEGLI Studi DI Messina).

Nissan, E. (2012). An overview of data mining for combating crime. *Applied Artificial Intelligence*, 26(8), 760-786.

NSA (2016). Technology Transfer program. Office of Research & Technology applications.

Nucci, G. de S. (2008). *Código Penal Comentado*. São Paulo: Revista dos Tribunais.

Nucci, G.S. (2013). *Organização criminosa: comentários à Lei 12.850, de 02 de agosto de 2013*. Editora Revista dos Tribunais.

Pacelli, E. (2013) *Curso de processo penal*, 17ª ed. São Paulo: Atlas, 2013.

Petersen, R. R. (2013). *Criminal Network Investigation: Processes, Tools and Techniques* (Doctoral dissertation, Syddansk Universitet).

Pickett, B. M., & Lingenfelter, C. M. (2011). *Influence strategy: principles and levels of analysis*.

Pontes, J; Anselmo, M.A. (2019) Crime.gov: quando a corrupção e o governo se misturam. Rio de Janeiro: Objetiva.

Prell, C., Hubacek, K., & Reed, M. (2009). Stakeholder Analysis and Social Network Analysis in Natural Resource Management. *Society & Natural Resources*, 22(6), 501-518. doi:10.1080/08941920802199202

Rasheed, A., Wiil, U. K., & Niazi, M. (2015). Evaluating PEVNET: A framework for visualization of criminal networks. In *International Conference on Multidisciplinary Social Networks Research* (pp. 131-149). Springer, Berlin, Heidelberg.

Sarvari, H., Abozinadah, E., Mbaziira, A., & McCoy, D. (2014). Constructing and analyzing criminal networks. In *2014 IEEE Security and Privacy Workshops* (pp. 84-91). IEEE.

Scott, J. (1988). Social network analysis. *Sociology*, 22(1), 109-127.

Scott, J., & Carrington, P. J. (2011). *The SAGE handbook of social network analysis*. SAGE publications.

Silva, G. H. M. A. D. (2016). Um modelo de visualização de dados utilizando banco de dados orientado a grafo suportado por big data.

Soares, V. B. (2015). (Des) organizando o espaço social de favelas: o campo burocrático do Estado em ação no contexto da 'pacificação' (Doctoral dissertation).

Sudhahar, S., De Fazio, G., Franzosi, R., & Cristianini, N. (2015). Network analysis of narrative content in large corpora. *Natural Language Engineering*, 21(1), 81-112.

Taha, K., & Yoo, P. D. (2019). Shortlisting the influential members of criminal organizations and identifying their important communication channels. *IEEE Transactions on Information Forensics and Security*, 14(8), 1988-1999.

Tayebi, M. A., & Glasser, U. (2011). Organized crime structures in co-offending networks. In *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing* (pp. 846-853). IEEE.

Tayebi, M. A., & Glasser, U. (2012). Investigating organized crime groups: a social network analysis perspective. In *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 565-572). IEEE.

Tayebi, M. A., & Glässer, U. (2016). Social network analysis in predictive policing. In *Social Network Analysis in Predictive Policing* (pp. 7-14). Springer, Cham.

TCU (2003). Acórdão 314/2003. Recuperado de <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20030410/TC%20015.889.doc>.

TCU (2018). Acórdão 1057/2018, Processo TC 17.519/2017-9, sessão 09/05/2018. Recuperado de <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/pesquisa/acordãocompleto/1751920179.PROC>.

Tokubayev, K. Z. (2015). Organized Crime in Kazakhstan: State and Solutions. *Mediterranean Journal of Social Sciences*, 6(3 S3), 329-329.

Toledo, L. D. S. G. (2011). Distribuição e mobilidade espacial de uma amostra de usuários de drogas recrutados pelo método Respondent-driven Sampling, Rio de Janeiro, 2009 (Doctoral dissertation).

Tourinho Filho, F. da C. (2009). Código de Processo Penal Comentado. São Paulo: Saraiva, vol. 1 p. 73.

Tsetini, M. (2015). Computer Forensics on Financial Crimes.

Van Vlasselaer, V. Van, Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). AFRAID: Fraud detection via active inference in time-evolving social networks. 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), (1), 659-666. <https://doi.org/10.1145/2808797.2810058>

Van Vlasselaer, V., Meskens, J., Van Dromme, D., & Baesens, B. (2013). Using social network knowledge for detecting spider constructions in social security fraud. Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining - ASONAM '13, 813-820. <https://doi.org/10.1145/2492517.2500292>

_____. (2017). GOTCHA! Network-Based Fraud Detection for Social Security Fraud. Management Science, 63(9), 3090-3110. <https://doi.org/10.1287/mnsc.2016.2489>

Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications (Vol. 8). Cambridge university press.

Williams, P., & Godson, R. (2002). Anticipating organized and transnational crime. Crime, Law and Social Change, 37(4), 311-355.

Xu, J., & Chen, H. (2005). Criminal network analysis and visualization. Communications of the ACM, 48(6), 100-107. doi:10.1145/1064830.1064834

Zhang, M. (2010). Social network analysis: history, concepts and research. Handbook of social network technologies and applications.

Zhao, Y. (2011). Computerised link analysis system: development and testing of a new link analysis system (Doctoral dissertation, Yu Zhao)

Apêndice I - Individualização das redes dos subgrupos da UF1

A listagem dos dez servidores com maior grau de centralidade na rede é apresentada na Tabela 17 e a listagem das dez Agências da Previdência Social (APS) com maior grau de centralidade na rede consta da Tabela 18. Da Tabela 17 é possível ver que o servidor com maior grau de centralidade na rede é o servidor vinculado aos processos de concessão automática. Apresentam os maiores valores de grau de centralidade os servidores Servidor669, Servidor588, Servidor116, Servidor129, Servidor428, Servidor 449, Servidor492, Servidor698, Servidor144 e Servidor571, sendo que a maior parte deles já foi objeto de operação de combate a fraudes previdenciárias, conforme será apresentado e analisado na seção de “discussão e implicações dos resultados”. Com relação às APS, apresentaram mais alto grau de centralidade: APS353, APS357, APS285, APS284 e APS354, todas também com alguma operação de combate a fraudes à previdência vinculada.

Para cada servidor e APS listados nas tabelas 17 e 18 foi gerada um subgrupo, cujos dados principais estão na Tabela 19 e cujas redes foram comentadas individualmente conforme Tabela 20 e Tabela 21.

Tabela 17

Servidores com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	<i>Eigenvector</i> %	K-Core
Automático	10,25	2,12	2,18	0,13	3
Servidor669	0,003	2,05	1,17	0,03	4
Servidor588	1,74	2,07	1,00	0,02	3
Servidor116	0,02	2,05	0,92	0,02	2
Servidor129	0,0006	2,10	0,41	1,16	3
Servidor428	0,001	2,09	0,41	1,15	3
Servidor449	0,21	2,10	0,41	0,90	3
Servidor492	0,0008	2,09	0,41	1,15	3
Servidor698	0,02	2,05	0,41	0,01	3
Servidor144	0,24	2,11	0,33	0,71	3
Servidor571	0,003	1,95	0,33	0	2

Fonte: autoria própria

Tabela 18

APS com maior grau de centralidade na UF1

Ator	Intermediação%	Proximidade%	Grau%	<i>Eigenvector</i> %	K-Core
APS353	21,50	2,14	5,03	7,43	3
APS357	18,26	2,13	3,85	1,02	4
APS285	11,61	2,13	3,02	4,34	3
APS360	3,53	2,08	1,84	0,03	4
APS351	5,82	2,12	1,67	0,98	3
APS284	4,92	2,13	1,51	0,95	3
APS287	5,02	2,12	1,42	1,43	3
APS354	3,04	2,12	1,42	2,76	3
APS363	3,10	2,08	1,09	0,02	3
APS345	0,11	2,11	0,92	2,52	3

Fonte: autoria própria

A observação da rede mostrou que, como regra geral, cada inquérito policial está vinculado a apenas um benefício. Contudo, a análise dos dados dos subgrupos (Tabela 19) mostra que em alguns casos era maior a proporção entre a quantidade de NBs e a quantidade de IPLs. Buscando informações sobre tais IPLs, constatou-se que eram, também regra geral, investigações que serviram de base para operações, mas cujas investigações ainda não haviam sido concluídas. Esse aumento na proporção de NBs por IPL foi observado nas redes dos subgrupos Servidor669, Servidor129 (e outros), Servidor698, APS353, APS357, APS285, APS284 e APS354. De outro lado, foi observado também que alguns conjuntos de Servidor-APS estavam vinculados a números praticamente idênticos de NBs e IPLs, conforme observável nos subgrupos: Servidor588, Servidor116 e Servidor571. Essa diferença é analisada na seção de “discussão e implicação dos resultados”.

Tabela 19

Dados das redes do subgrupo formadas com atores de maior grau de centralidade

Rede do subgrupo do ator:	APS na rede do subgrupo	NBs na rede do subgrupo	IPLs na rede do subgrupo	Servidores na rede do subgrupo	Total de atores na rede do subgrupo	Total de vínculos na rede do subgrupo
---------------------------	-------------------------	-------------------------	--------------------------	--------------------------------	-------------------------------------	---------------------------------------

Servidor669	3	14	1	1	18	56
Servidor588	4	12	13	1	36	50
Servidor116 (Servidor129, Servidor428, Servidor449, Servidor492 e Servidor144)	2	11	11	1	25	34
Servidor698	35	97	2	81	215	251
Servidor571	1	5	2	1	9	15
APS353 (APS357 e APS360)	1	4	4	1	10	12
APS285	25	60	23	42	151	214
APS351	9	53	33	22	117	184
APS284	10	36	17	29	92	125
APS287	7	20	12	9	49	69
APS354	7	18	11	11	47	61
APS363	6	17	10	10	43	60
APS345	8	17	6	13	44	58
	4	13	13	2	32	42
	8	11	1	10	30	46

Fonte: autoria própria

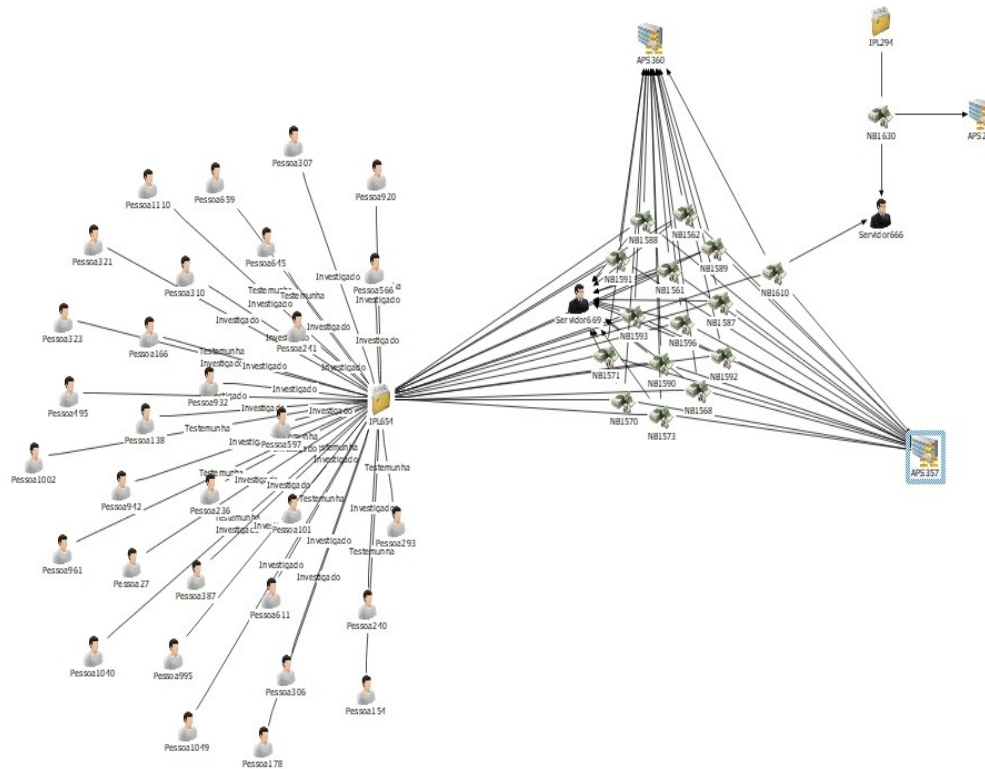
Passa-se a apresentar as redes formadas a partir dos servidores com maior grau de centralidade na rede da UF1. As redes mapeadas a partir dos subgrupos dos servidores constam da Tabela 20 e as redes mapeadas a partir das agências constam da Tabela 21.

Tabela 20

Redes de subgrupos formadas a partir dos Servidores da UF1

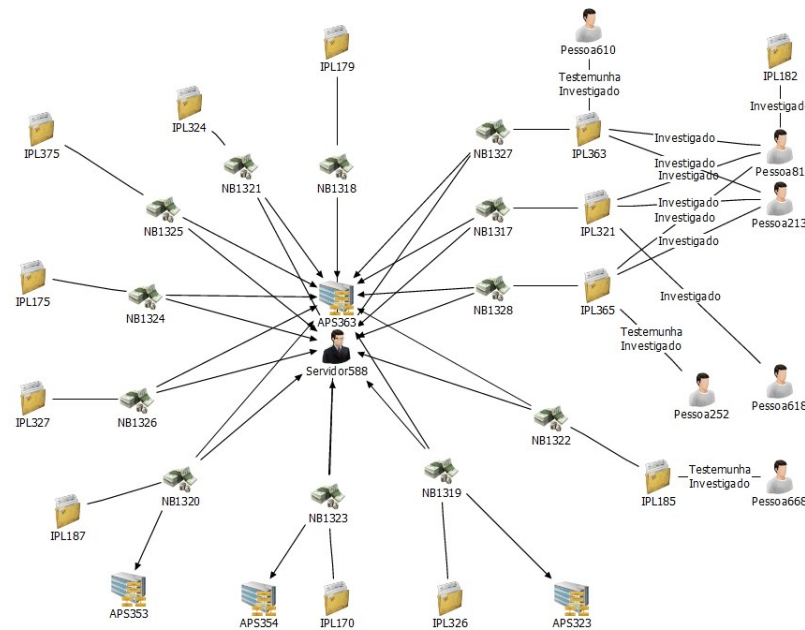
Ator	Rede	Comentário
------	------	------------

Servidor669



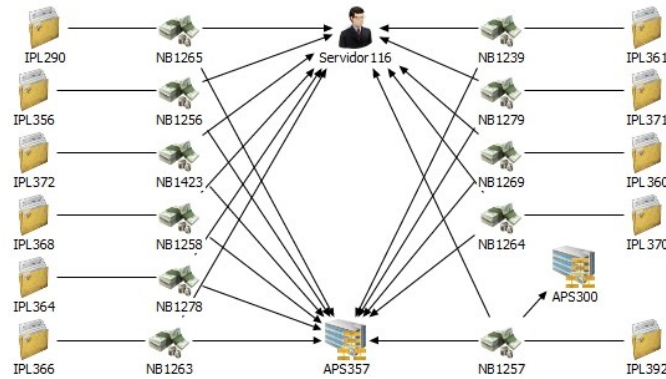
Identificou-se que a rede deste subgrupo foi formada no âmbito de uma operação da UF1, mas que ainda não estava concluída. No subgrupo estão 15 NBs, concedidos pelo Servidor666 na APS357 (mas que depois passaram a ser mantidos na APS360). Um dos benefícios foi concedido por outro servidor (Servidor666), o qual também foi responsável pela concessão do benefício NB1630 que é objeto de investigação no IPL294. Desta forma, é possível que haja conexão também entre o IPL294 e o IPL664.

Servidor588



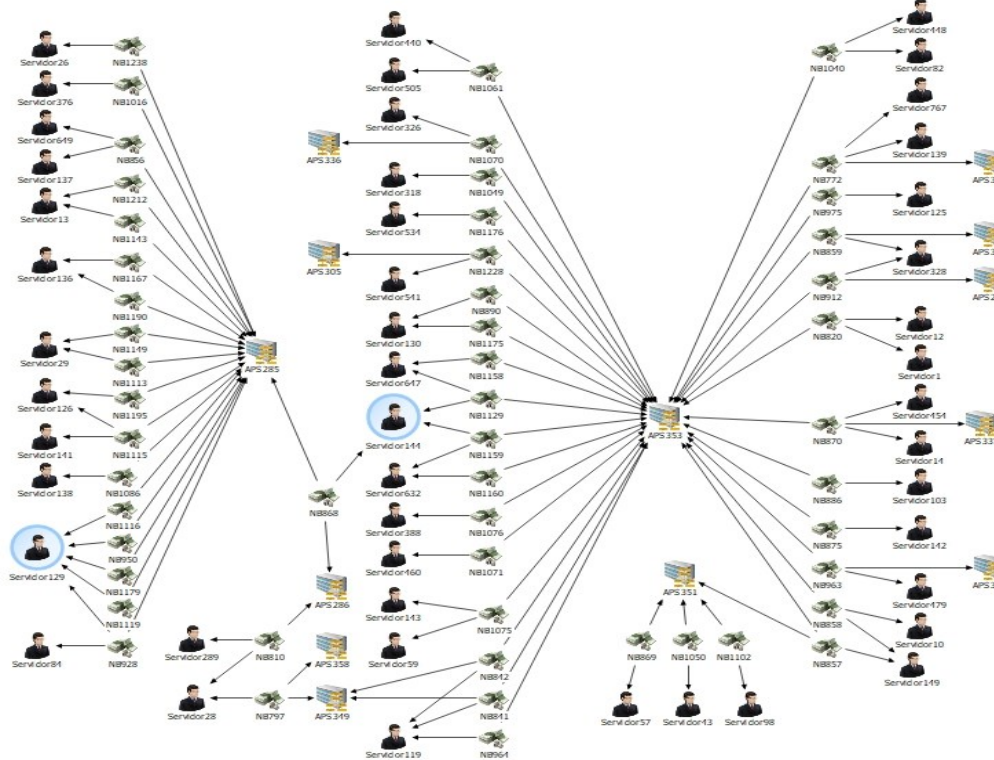
Analisando a rede do subgrupo, é possível observar que benefícios concedidos pelo Servidor588 na APS363 estão sendo investigados em pelo menos 12 inquéritos policiais diferentes. Além disso, os inquéritos IPL363, IPL321 e IPL365 também possuem as Pessoa81 e Pessoa213 como investigados em comum. Em consulta às investigações, constatou-se que alguns dos inquéritos (IPL179, IPL175, IPL170 e IPL185) são desdobramentos de uma mesma investigação realizada contra o Servidor588. De outro lado, não foram localizadas informações que o vínculo com relação aos demais inquéritos fosse conhecido. Desta forma, o algoritmo aponta para a possível conexão das fraudes investigadas nos 12 inquéritos, posto que contaram com a participação do mesmo servidor e foram realizadas na mesma APS.

Servidor116



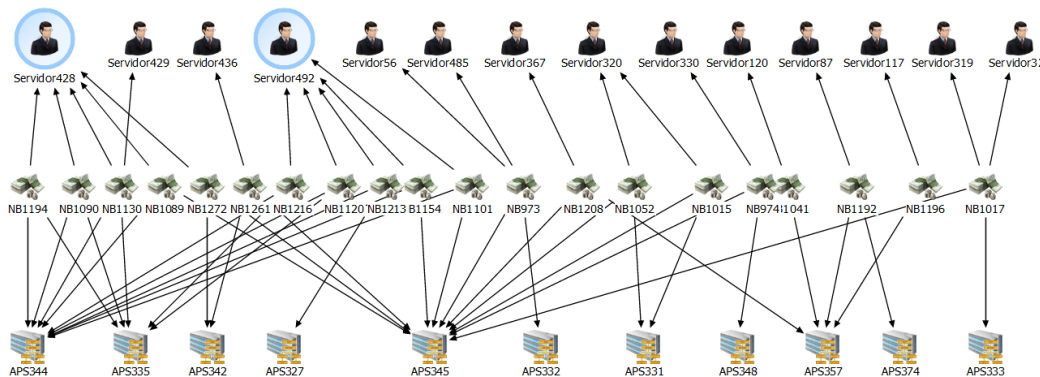
De maneira semelhante ao ocorrido com relação ao Servidor588, a rede formada a partir do Servidor116 apontou a existência de 11 inquéritos, apurando 11 benefícios fraudulentos, todos concedidos pelo Servidor116 na APS357. Além de tais vínculos, observou-se que vários deles tem *modus operandi* semelhantes, posto que nos inquéritos IPL290, IPL360, IPL371, IPL392, IPL356, IPL364, IPL366 e IPL361 a fraude consistiria na inserção de vínculos empregatícios inexistentes para obtenção fraudulenta de aposentadoria por tempo de contribuição. Não foi localizado padrão semelhante nos inquéritos IPL370, IPL372 e IPL368.

Servidor129 e
Servidor144



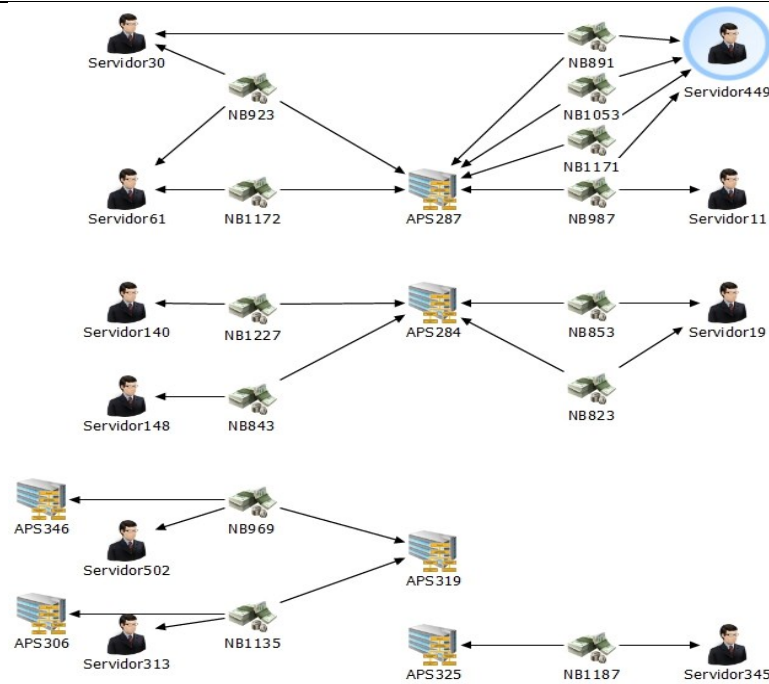
Os benefícios concedidos pelos Servidor129, Servidor428, Servidor449 e Servidor144 estão contidos na rede formada a partir o IPL309. Trata-se da área de concentração apontada na visão geral como Área4 (ver seção 4.3.1). Vinculados ao IPL309 foram identificados 97 benefícios previdenciários investigados. Constatou-se ainda que se trata da investigação referente a operação deflagrada na UF1, com apuração de fraudes em benefícios de pensão por morte concedidos mediante documentos falsos. A fim de facilitar a visualização desta rede, mesmo sendo todos os benefícios investigados em um mesmo inquérito policial foi feita a divisão em outros subgrupos menores

Servidor428 e
Servidor492



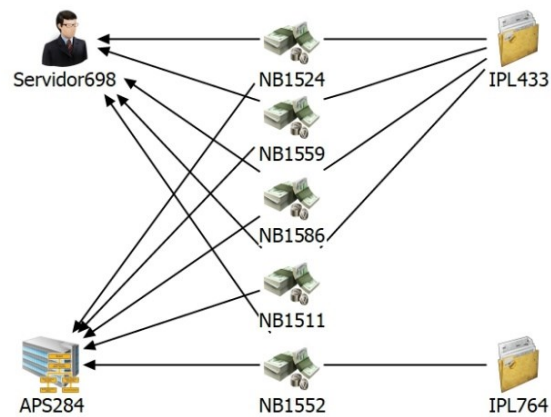
Neste primeiro diagrama é possível ver a participação do Servidor129 que atuou na concessão de 4 NBs fraudulentos, todos na mesma APS. Também é possível ver o Servidor144, que foi o responsável por 3 NBs fraudulentos, em 2 diferentes APS. No diagrama abaixo é possível ver a participação do Servidor428, responsável pela concessão de 5 NBs fraudados bem como pelo Servidor492, responsável por outros 5 NBs fraudados

Servidor449



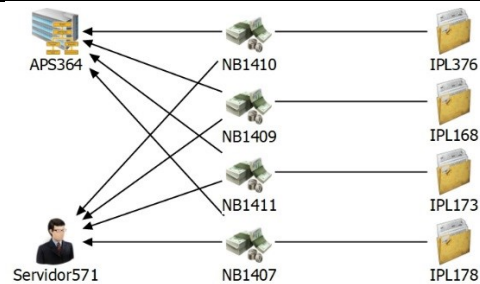
Por fim, é possível observar a seguir o Servidor449, responsável pela concessão/habilitação de 4 benefícios fraudados. Conforme visto, tratou-se de investigação de grande porte, constando no sistema cerca de 350 pessoas envolvidas entre testemunhas, investigados, presos, servidores envolvidos e beneficiários.

Servidor698



Do diagrama é possível observar que 5 NBs investigados no IPL433 foram concedidos pelo Servidor698, na APS284. Foi possível identificar ainda que o NB1552, que é investigado no IPL764 foi concedido na mesma APS284, o que pode indicar conexão entre os fatos.

Servidor571



Do diagrama é possível perceber que há NBs investigados em 4 diferentes IPLs que foram concedidos pelo mesmo servidor571 e na APS364. Analisados os casos específicos, constatou-se que os inquéritos IPL168, IPL173 e IPL178 foram desdobramentos de uma operação, não tendo sido identificado vínculo anterior com o IPL376.

Fonte: autoria própria

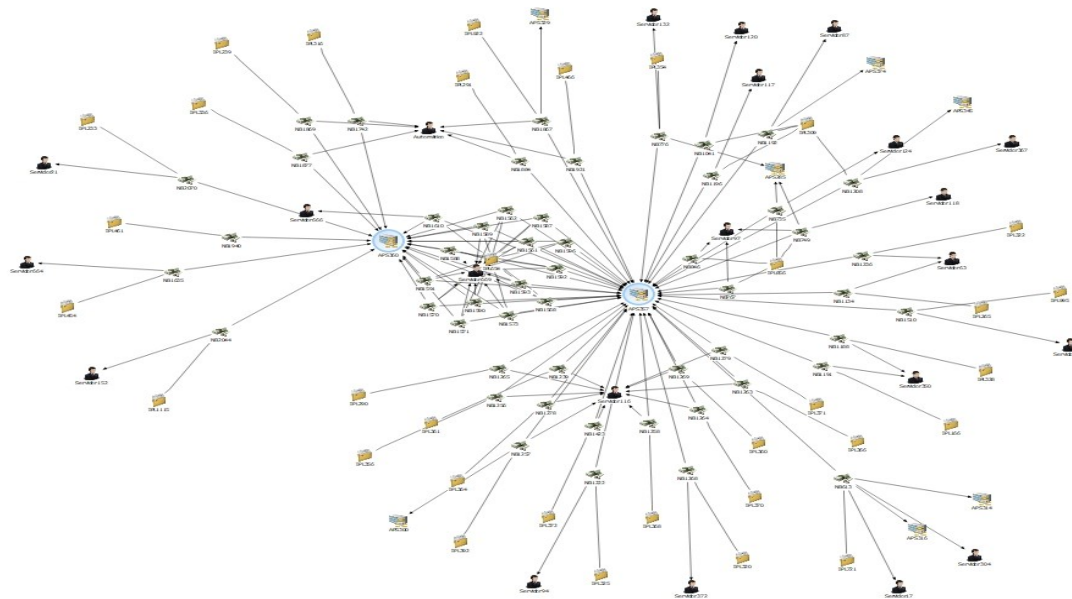
Tabela 21

Redes de subgrupos formados a partir das APSs da UF1

Ator	Rede	Comentário
APS353		<p>Analisando as APSs do Quadro 14, é possível ver que a APS353 já foi apresentada no diagrama junto com o Servidor129 e o Servidor144 (item d acima). De fato, traçando-se a rede do subgrupo a partir da APS353, é possível visualizar que 60 dos NBs fraudados da rede total foram concedidos ou são mantidos na APS353. De fato, estes NBs fraudados são objeto de investigação não só no IPL309 (do Servidor129 e Servidor144 citados) mas em um total de 23 inquéritos policiais.</p>

Analisando as APSs do Quadro 14, é possível ver que a APS353 já foi apresentada no diagrama junto com o Servidor129 e o Servidor144 (item d acima). De fato, traçando-se a rede do subgrupo a partir da APS353, é possível visualizar que 60 dos NBs fraudados da rede total foram concedidos ou são mantidos na APS353. De fato, estes NBs fraudados são objeto de investigação não só no IPL309 (do Servidor129 e Servidor144 citados) mas em um total de 23 inquéritos policiais.

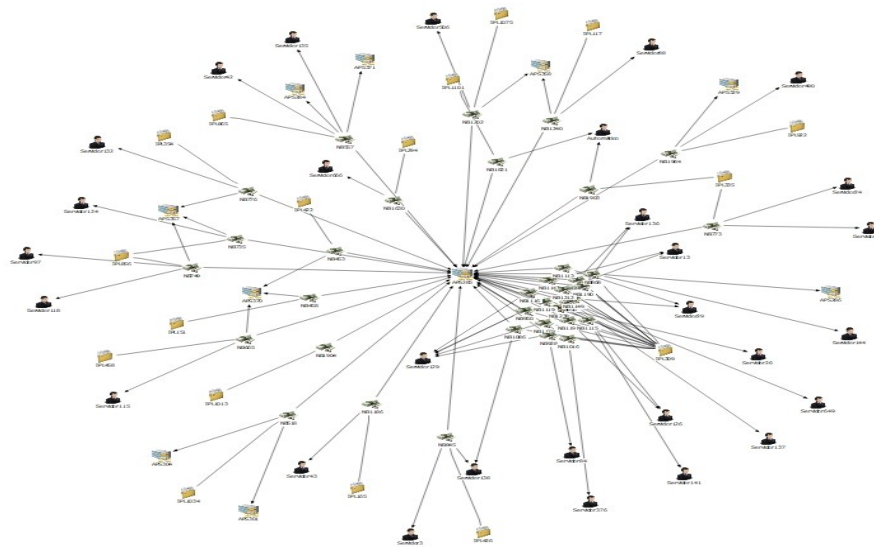
APS357 e
APS360



A APS357 bem como a APS 360 foram analisadas junto com o Servidor669, posto que os benefícios por ele concedidos e vinculados ao IPL654 estão vinculados a estas (os NBs foram concedidos em uma e eram mantidos na outra APS). De fato, a rede traçada a partir do subgrupo das APS357 e 360 abrange 53 benefícios fraudados investigados em 33 diferentes inquéritos policiais e concedidos por 21 diferentes servidores públicos.

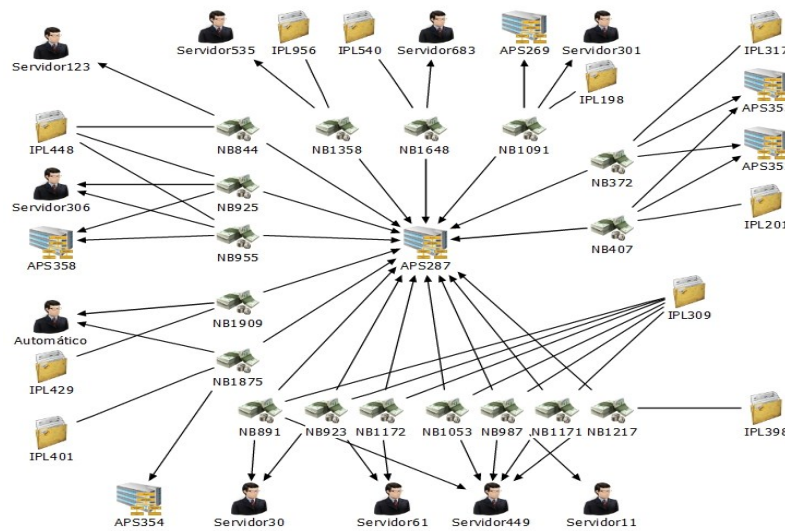
Demonstra alto grau de centralidade na rede do subgrupo o Servidor116, responsável pela concessão de vários dos benefícios ligados à APS357.

APS285



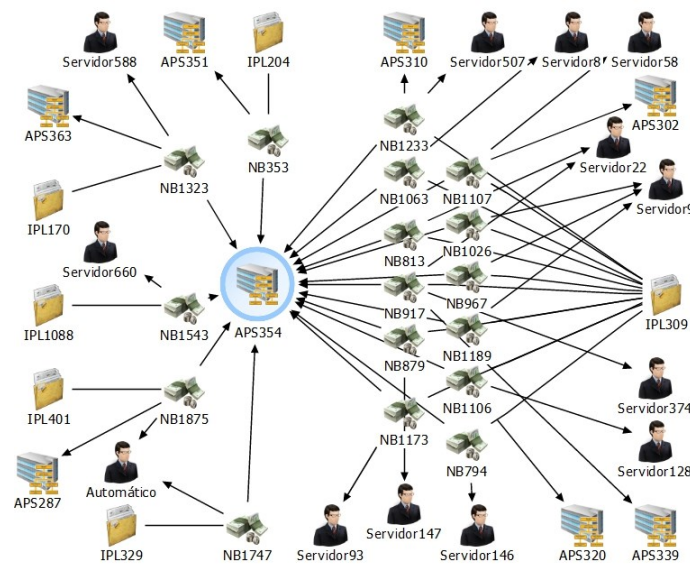
Tem-se que a APS285 também foi abordada junto com o Servidor129 e Servidor144. Traçando-se a rede do subgrupo a partir da APS285, temos uma rede do subgrupo que abrange 36 benefícios fraudados, concedidos por 28 diferentes servidores em 17 inquéritos policiais, inclusive no IPL309 acima citado.

APS287



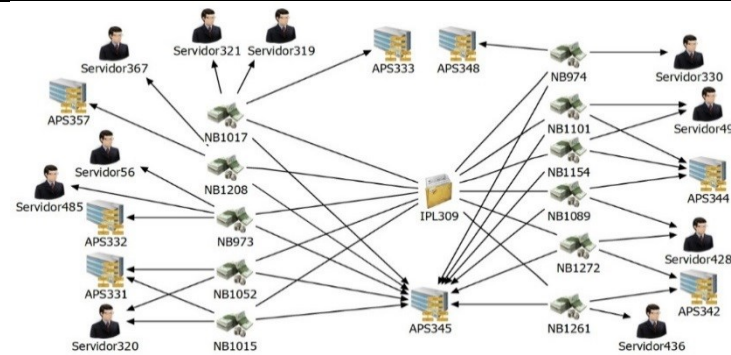
Na APS287 foram concedidos alguns dos benefícios investigados no IPL309, com destaque para os concedidos pelo Servidor449, conforme citado. No subgrupo traçada a partir da APS287, constam 17 benefícios, concedidos por 10 diferentes servidores, investigados em 10 inquéritos policiais. A observação da rede do subgrupo permite visualizar que os benefícios objeto do IPL448 foram todos concedidos pelo mesmo Servidor306, na mesma APS287

APS354



Na APS354 foram concedidos benefícios investigados em 6 inquéritos diferentes, com destaque para os benefícios objeto do IPL309. Dos NBs vinculados a tal IPL, pelo menos 3 foram concedidos pelo Servidor9 e outros 2 pelo Servidor22, o que sugere seja melhor averiguada a possível participação dos mesmos nas fraudes.

APS345



Na APS345 foram concedidos 11 dos NBs investigados no IPL309, pelo menos dois deles pelo Servidor492 acima citado. Não foram observados NBs fraudados e vinculados à APS345 que não sejam os investigados no IPL309

Fonte: autoria própria

Foi gerada listagem com análise das variáveis em relação a todos os 1193 atores da rede. Na tabela 22, em ordem decrescente pelo grau de centralidade, são colacionados os primeiros 80 resultados da rede formada na UF1, entendendo-se abrangidos os principais atores da rede.

Tabela 22

Medições dos principais atores da rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core	Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
IPL309	68,3403	2,1838	37,5	99,42817	3	Servidor669	0,003205	2,0553	1,1745	0,035503	4
APS353	21,50976	2,1466	5,0336	7,43325	3	APS363	3,109088	2,0883	1,0906	0,024266	3
APS357	18,26646	2,1345	3,8591	1,028356	4	IPL1101	1,931432	2,075	1,0906	0,010176	1
IPL654	4,953424	2,0579	3,8591	0,040676	4	IPL856	1,30039	2,066	1,0067	0,029305	3
APS285	11,6192	2,1391	3,0201	4,34973	3	Servidor588	1,745254	2,07	1,0067	0,023916	3
Automático	10,25368	2,1201	2,1812	0,133696	3	APS345	0,111141	2,1113	0,9228	2,520146	3
APS360	3,533405	2,0814	1,8456	0,039477	4	Servidor116	0,023174	2,0521	0,9228	0,025731	2
IPL448	2,477645	2,078	1,8456	0,08308	3	APS286	2,767068	2,1285	0,8389	0,484378	3
APS351	5,824294	2,1249	1,6779	0,985306	3	APS344	0,004069	2,0968	0,755	2,075993	3
APS284	4,925329	2,1319	1,5101	0,950655	3	APS364	3,188556	2,0354	0,6711	0,000467	2
APS287	5,027666	2,1269	1,4262	1,430869	3	APS369	0,317101	2,0704	0,6711	0,058282	3
APS354	3,046138	2,1224	1,4262	2,76449	3	IPL433	0,649511	2,0508	0,6711	0,009794	3

APS358	2,42385	2,117	0,5872	0,252737	3	NB973	0,496692	2,1392	0,4195	4,82904	2
APS361	2,471551	2,0723	0,5872	0,017342	2	Servidor129	0,000657	2,1052	0,4195	1,162213	3
IPL357	0,498329	2,069	0,5872	0,009795	3	Servidor428	0,001163	2,0964	0,4195	1,152108	3
IPL463	0,968252	2,0351	0,5872	0,000566	1	Servidor449	0,215942	2,103	0,4195	0,907921	3
IPL764	0,83939	2,0506	0,5872	0,002249	2	Servidor492	0,000805	2,0963	0,4195	1,153161	3
IPL922	0,555993	2,1006	0,5872	0,050744	3	Servidor698	0,020305	2,0514	0,4195	0,01182	3
IPL136	0,646346	2,0423	0,5034	0,004706	2	PS367	0,008171	2,0627	0,3356	0,066697	2
IPL335	0,163445	2,0891	0,5034	0,087258	3	IPL1064	0,48476	2,0379	0,3356	0,000309	1
IPL353	0,807229	2,0655	0,5034	0,016762	1	IPL1075	0,48476	2,0622	0,3356	0,010327	1
NB557	1,49786	2,1065	0,5034	0,251666	2	IPL1115	0,48476	2,0017	0,3356	0,000101	1
NB613	0,807229	2,0919	0,5034	0,048952	1	IPL321	0,337581	2,0114	0,3356	9,08E-05	3
APS335	0,000767	2,0963	0,4195	1,149619	3	IPL354	0,409219	2,0656	0,3356	0,012079	2
APS349	0,694621	2,113	0,4195	0,722549	3	IPL363	0,337581	2,0114	0,3356	9,08E-05	3
IPL1034	0,646065	2,0552	0,4195	0,009795	1	IPL365	0,337581	2,0114	0,3356	9,08E-05	3
IPL125	0,646065	2,0809	0,4195	0,01696	1	IPL369	0,48476	1,9702	0,3356	1,77E-05	1
IPL349	0,646065	2,0622	0,4195	0,016836	1	IPL398	0,48476	2,0438	0,3356	0,005247	1
IPL377	0,134359	2,0538	0,4195	0,004893	2	IPL461	0,48476	2,0016	0,3356	0,000108	1
IPL964	0,646065	2,0701	0,4195	0,002447	1	IPL620	0,48476	2,0628	0,3356	0,016764	1
NB1017	0,496692	2,1392	0,4195	4,82904	2	IPL865	0,48476	2,0648	0,3356	0,011941	1
NB1130	0,243064	2,1392	0,4195	4,895196	3	NB1015	0,173448	2,1391	0,3356	4,839811	2
NB1267	0,001409	0,0842	0,4195	0	1	NB1028	1,023237	2,1116	0,3356	0,396344	2
NB584	0,730127	2,0829	0,4195	0,049553	2	NB1040	0,754733	2,1538	0,3356	5,05046	2
NB604	0,544166	2,0864	0,4195	0,023162	2	NB1052	0,173448	2,1391	0,3356	4,839811	2
NB667	0,646065	2,032	0,4195	0,000813	1	NB1059	0,001691	0,0842	0,3356	0	1
NB749	1,341611	2,107	0,4195	0,255804	3	NB1061	4,312395	2,1557	0,3356	5,050476	2
NB772	0,916179	2,1539	0,4195	5,061727	2	NB1070	0,754733	2,1538	0,3356	5,05046	2
NB870	0,916179	2,1539	0,4195	5,061727	2	NB1075	0,754733	2,1538	0,3356	5,05046	2
NB917	0,597702	2,1454	0,4195	4,851392	2	NB1089	0,063319	2,1391	0,3356	4,948808	3

Fonte: autoria própria

A matriz de correlação da rede da UF1 consta da Tabela 23.

Tabela 23

Matriz de Correlação da rede da UF1

APS-Servidor	Frequência	IPL125	IPL168	IPL170	IPL173	IPL175	IPL178	IPL179	IPL185	IPL187
APS357-Servidor669	14	0	0	0	0	0	0	0	0	0
APS360-Servidor669	14	0	0	0	0	0	0	0	0	0
APS363-Servidor588	12	0	0	1	0	1	0	1	1	1
APS357-Servidor116	11	0	0	0	0	0	0	0	0	0
APS284-Servidor698	5	0	0	0	0	0	0	0	0	0
APS285-Servidor129	5	0	0	0	0	0	0	0	0	0
APS287-Servidor449	5	0	0	0	0	0	0	0	0	0
APS344-Servidor492	5	0	0	0	0	0	0	0	0	0
APS344-Servidor428	4	0	0	0	0	0	0	0	0	0
APS351-Automático	4	0	0	0	0	0	0	0	0	0
APS353-Automático	4	1	0	0	0	0	0	0	0	0
APS364-Servidor571	4	0	1	0	1	0	1	0	0	0

APS-Servidor	IPL356	IPL357	IPL360	IPL361	IPL363	IPL364	IPL365	IPL366	IPL368	IPL370
APS357-Servidor669	0	0	0	0	0	0	0	0	0	0
APS360-Servidor669	0	0	0	0	0	0	0	0	0	0
APS363-Servidor588	0	0	0	0	1	0	1	0	0	0
APS357-Servidor116	1	0	1	1	0	1	0	1	1	1
APS284-Servidor698	0	0	0	0	0	0	0	0	0	0
APS285-Servidor129	0	0	0	0	0	0	0	0	0	0
APS287-Servidor449	0	0	0	0	0	0	0	0	0	0
APS344-Servidor492	0	0	0	0	0	0	0	0	0	0
APS344-Servidor428	0	0	0	0	0	0	0	0	0	0
APS351-Automático	0	3	0	0	0	0	0	0	0	0
APS353-Automático	0	0	0	0	0	0	0	0	0	0
APS364-Servidor571	0	0	0	0	0	0	0	0	0	0

Fonte: autoria própria

Apêndice II - Individualização das redes de subgrupos da UF2

Com referência às análises das variáveis para os atores da rede, foram assim divididos: a) a lista com as variáveis dos principais atores da rede consta do Apêndice II; b) a lista dos dez servidores com maior grau de centralidade na rede consta da Tabela 24; c) a lista com as dez Agências da Previdência Social com maior grau de centralidade na rede consta da Tabela 25. Da Tabela 24 não foi incluído o servidor referente aos processos de concessão automática, para melhor observação dos demais atores. Da Tabela 24 é possível ver que os três primeiros são o Servidor76, o Servidor525 e o Servidor77. Os três estão envolvidos em operação de combate a fraudes previdenciárias objeto do IPL1059, que teve também a rede de seu subgrupo mapeada e consta do Apêndice II. Segue a listagem com o Servidor73, que foi objeto de investigação no IPL1047; o Servidor312, que foi investigado no IPL560, seguidos do Servidor298, Servidor347, Servidor295, Servidor35 e Servidor96.

Tabela 24

Servidores com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	<i>Eigenvector</i> %	K-Core
Servidor76	0,61	4,37	4,05	44,03	3
Servidor525	0,01	4,31	1,18	7,24	4
Servidor77	0,06	4,33	0,69	4,13	3
Servidor73	0,13	4,22	0,59	0,001	4
Servidor312	0,02	4,23	0,39	0,003	3
Servidor298	0,26	4,37	0,29	0,58	2
Servidor347	0,0002	4,19	0,19	0,0006	2
Servidor295	0,06	4,34	0,19	0,003	2
Servidor35	0,06	4,40	0,19	0,02	2
Servidor96	0,03	4,38	0,19	0,003	2

Fonte: autoria própria

Da Tabela 25 é possível constatar que a APS com maior grau de centralidade é a APS264, onde foram concedidos vários dos benefícios objeto do IPL1059. Na tabela segue as APS236 que, em razão do grande número de vínculos, foi incluída no mesmo subgrupo que a APS239; após

seguem a APS251, APS263, APS258, APS243, APS237 e APS242. Destas, apenas nas APS237 e APS242 é perceptível concentração de vínculos referente a Operação, sendo observáveis alguns benefícios concedidos pelo Servidor73 e objeto do IPL1047.

Tabela 25

APS com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
APS264	6,35	4,50	4,45	45,22	3
APS236	19,96	4,69	3,06	0,20	2
APS251	14,36	4,65	2,47	2,83	3
APS263	4,93	4,57	2,17	9,05	3
APS239	12,60	4,63	2,17	0,08	2
APS258	6,73	4,60	1,98	8,22	4
APS243	6,09	4,56	1,58	0,04	3
APS237	7,31	4,47	1,38	0,01	4
APS242	7,15	4,50	1,38	0,01	4
APS238	7,22	4,54	1,28	0,02	2

Fonte: autoria própria

Para cada servidor e APS listados nas Tabelas 24 e 25 foi mapeada uma rede para o subgrupo gerado a partir destes. Os dados dos subgrupos foram compilados, conforme consta da Tabela 26, sendo as redes dos subgrupos apresentadas e comentadas individualmente, conforme Tabelas 27 e 28.

Tabela 26

Dados das redes do subgrupo formadas com atores de maior grau de centralidade

Rede do subgrupo do ator:	APS na rede do subgrupo	NBs na rede do subgrupo	IPLs na rede do subgrupo	Servidores na rede do subgrupo	Total de atores na rede do subgrupo	Total de vínculos na rede do subgrupo
---------------------------	-------------------------	-------------------------	--------------------------	--------------------------------	-------------------------------------	---------------------------------------

Servidor76, Servidor525, Servidor77	5	69	2	3	79	213
Servidor73	3	6	2	1	18	34
Servidor312	3	4	1	1	13	18
Servidor298	4	3	3	1	14	14
Servidor347	1	2	1	1	74	8
Servidor295	2	2	2	1	9	9
Servidor35	3	2	2	1	10	10
Servidor96	3	2	2	1	10	10
APS264	2	4	4	3	17	16
APS236	13	31	31	2	108	119
APS251	8	25	21	9	88	99
APS263	2	7	5	1	22	27
APS239	18	49	45	8	166	187
APS258	3	7	6	2	25	27
APS243	5	16	12	4	51	60
APS237 e APS242	8	21	12	11	73	105
APS238	5	13	13	5	49	50

Fonte: autoria própria

A observação da rede e dos dados da Tabela 26 mostrou que, como regra geral, cada inquérito policial está vinculado a apenas um benefício. Contudo, os dados da Tabela 26 mostram que em alguns casos há maior a proporção entre a quantidade de NBs e a quantidade de IPLs. Buscando informações sobre tais IPLs, constatou-se que eram, também regra geral, investigações que serviram de base para operações, mas cujas investigações ainda não haviam sido concluídas, ou seja, houve uma fase ostensiva de deflagração, mas as investigações ainda não foram concluídas. Esse aumento na proporção de NBs por IPL foi observado nas redes dos subgrupos Servidor669, Servidor129 (e outros), Servidor698, APS353, APS357, APS285, APS284 e APS354. De outro lado, foi observado também que alguns conjuntos de Servidor-APS estavam vinculados

a números praticamente idênticos de NBs e IPLs, conforme observável nos subgrupos: Servidor588, Servidor116 e Servidor571. Essa diferença na proporção entre a quantidade de NBs investigados e a quantidade de IPLs é discutida na seção de “discussão e implicações dos resultados”, sendo explicável, de maneira resumida, pela existência de desdobramentos de operações deflagradas, onde era feito um inquérito para investigar o núcleo principal dos grupos criminosos e depois instaurados inquéritos individuais para apurar a conduta dos titulares dos benefícios.

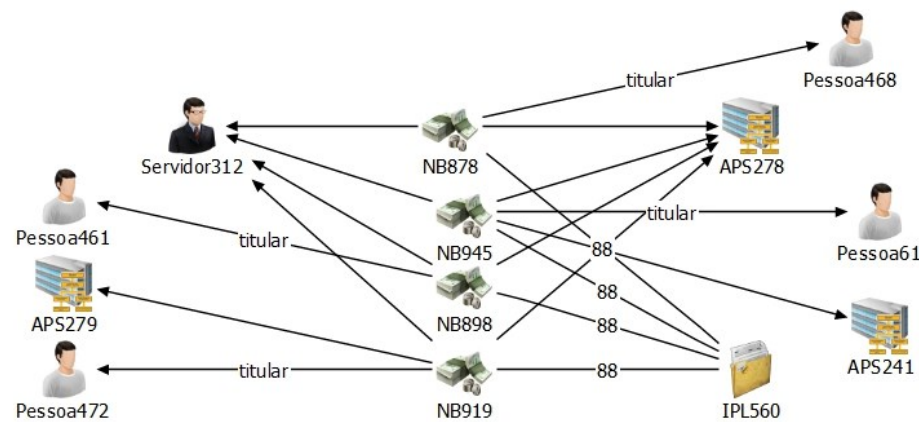
As redes mapeadas a partir dos subgrupos dos servidores de maior grau de centralidade constam do Tabela 27 e as redes dos subgrupos das APS com maior centralidade constam da Tabela 28. Cada rede apresentada é comentada na própria tabela. Foi gerada listagem com análise das variáveis em relação a todos os 1011 atores da rede, sendo apresentados os 50 primeiros resultados por ordem de grau de centralidade na Tabela 29, entendendo-se abrangidos os principais atores da rede.

Tabela 27

Redes de subgrupos formados a partir dos servidores da UF1

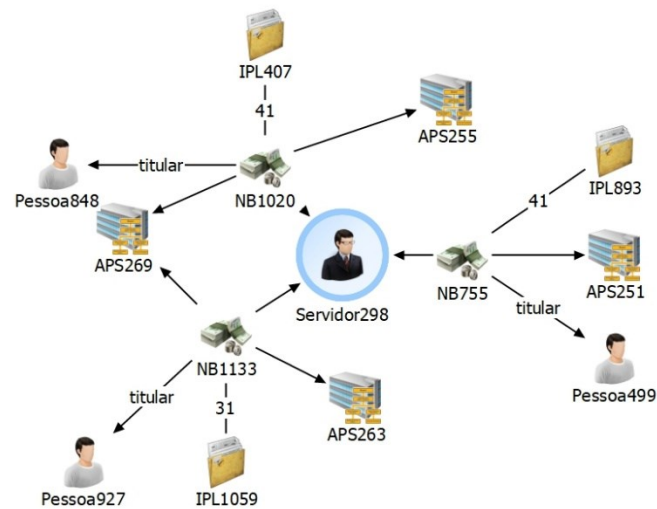
Ator	Rede	Comentários
Servidor73		<p>Os três primeiros servidores da lista com maior grau de centralidades são o Servidor76, o Servidor525 e o Servidor77, responsáveis pela concessão dos benefícios vinculados ao IPL1059.</p> <p>O próximo servidor na lista é o Servidor73, sendo que a rede desenhada a partir deste mostra que foi responsável pelos processos de benefícios vinculados ao IPL1047, concedidos/mantidos nas APS242 e APS237. O mesmo servidor foi responsável pelo processo do NB1420, em investigação no IPL132.</p>

Servidor312



O servidor312 foi responsável pela concessão de 4 NBs vinculados ao IPL560. Todos os NBs são do mesmo grupo 88 (benefícios das LOAS) e foram concedidos na mesma APS, o que reforça a conexão entre os benefícios investigados.

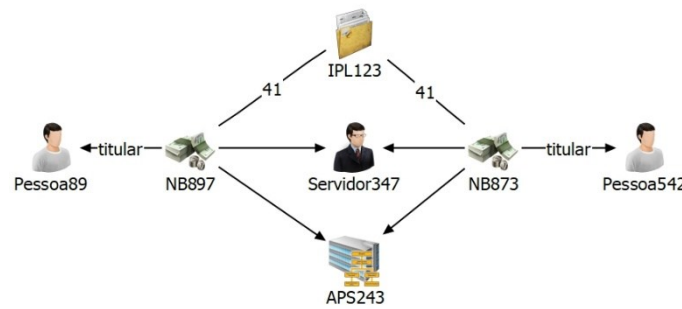
Servidor298



O servidor298 foi o responsável pela concessão de 3 benefícios fraudulentos investigados em 3 inquéritos policiais diferentes, quais sejam, IPL407, IPL893 e IPL1059.

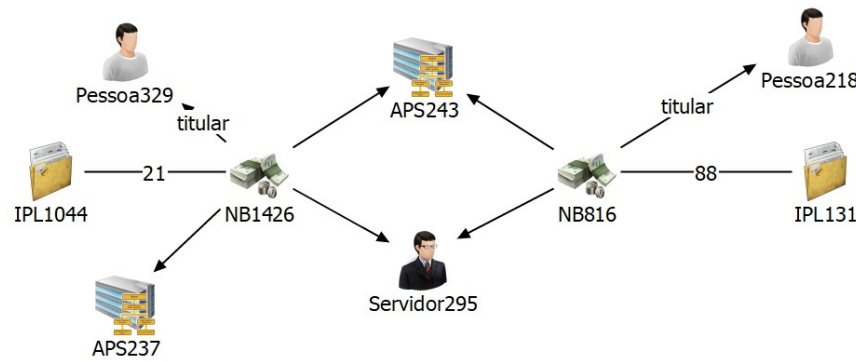
Não foram encontrados elementos que indiquem que os inquéritos foram desdobramentos de uma mesma investigação.

Servidor347



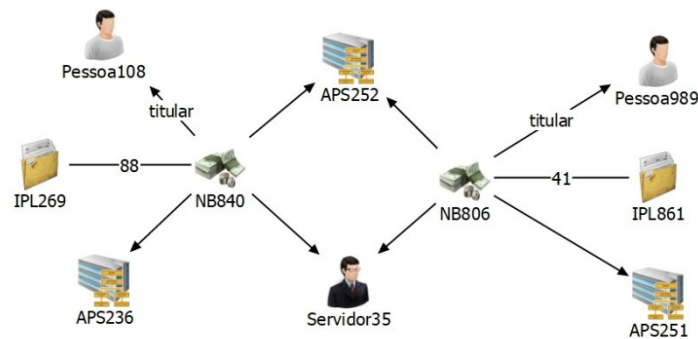
Foi encontrado que o servidor347 foi o responsável pela concessão dos dois NBs investigados no IPL123, sendo o próprio servidor um dos investigados naquele inquérito policial.

Servidor295



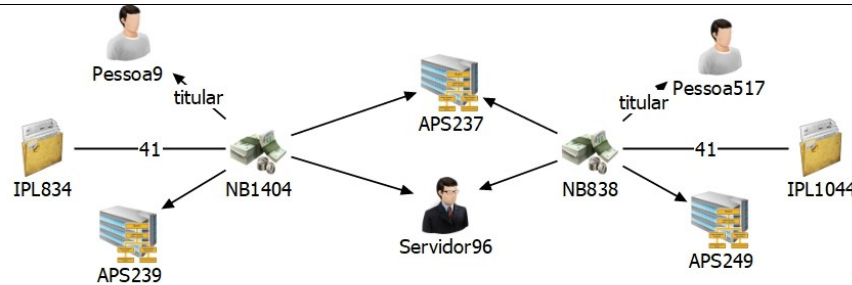
A partir do servidor295 foi identificado possível vínculo entre o IPL1044 e o IPL131, eis que o servidor295 foi responsável pela concessão dos benefícios investigados em ambos inquéritos policiais, na mesma APS243.

Servidor35



Foi identificado possível vínculo entre os inquéritos IPL269 e IPL861, eis que o servidor35 foi responsável pela concessão dos benefícios investigados em ambos inquéritos policiais, na mesma APS252.

Servidor96



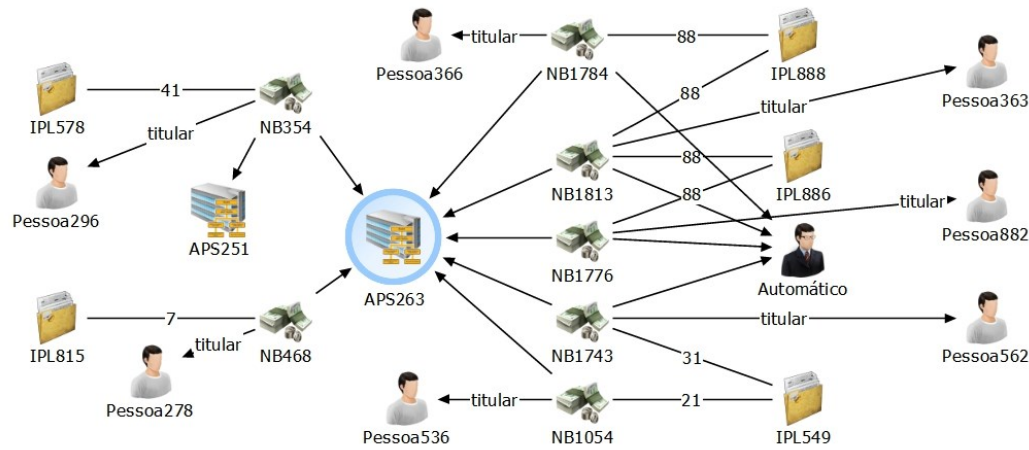
Foi identificado possível vínculo entre os inquéritos policiais IPL834 e IPL1044, eis que o servidor96 foi responsável pela concessão dos benefícios investigados em ambos inquéritos policiais, na mesma APS237.

Fonte: autoria própria

Tabela 28
Redes de subgrupos formados a partir das APSs da UF2

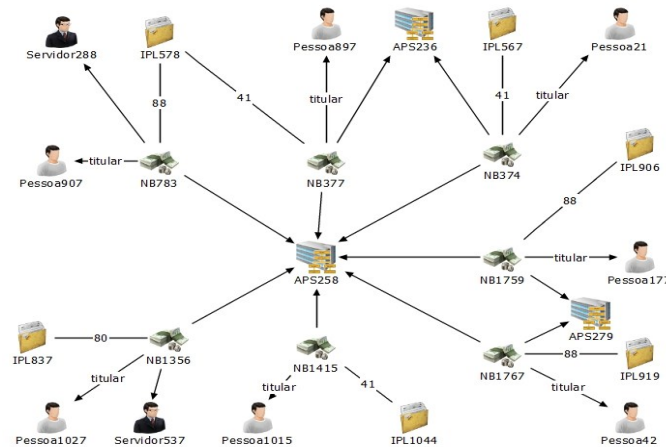
Ator	Rede	Comentários
APS264	<p>The diagram shows a central node APS264 (circled in blue) connected to several other nodes. APS264 is connected to Servidor339, Servidor687, Servidor607, and Pessoa1027. APS264 is also connected to NB738, NB582, and NB1449. NB738 is connected to APS283, Pessoa829 (labeled 'titular'), and IPL541 (labeled '21'). NB582 is connected to Servidor687, Pessoa554 (labeled 'titular'), and IPL809 (labeled '88'). NB1449 is connected to Servidor607, IPL837 (labeled '80'), and Pessoa1027 (labeled 'titular'). Additionally, NB492 is connected to APS264 and Pessoa82 (labeled 'titular'). IPL1044 is connected to NB492 (labeled '41').</p>	<p>As APSs vinculadas aos benefícios fraudulentos do IPL1059, quais sejam, APS264, APS263 e APS258, estão na lista das com maior relevância na rede. Assim, os NBs vinculados ao IPL1059 não serão aqui apresentados e, apesar disso, é possível constatar que foram concedidos naquela mesma APS quatro NBs investigados em quatro inquéritos policiais distintos, o que é visto como possível vínculo oculto entre as investigações.</p>

APS263



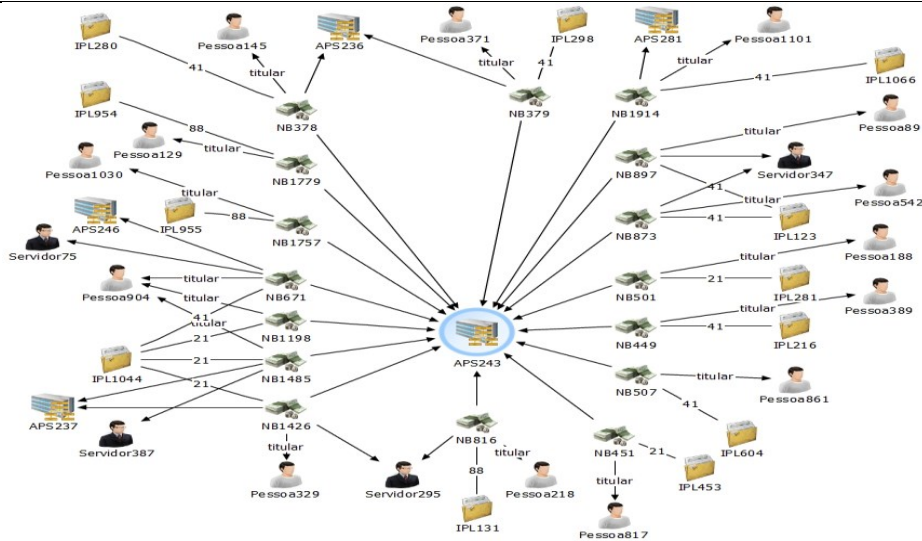
Na APS263 foram concedidos sete NBs que estão sob investigação em cinco diferentes inquéritos policiais. Observa-se que pelo menos quatro dos NBs foram por concessão automática, tratando-se de benefícios da LOAS, sob investigação nos inquéritos policiais IPL549, IPL888 e IPL886.

APS258



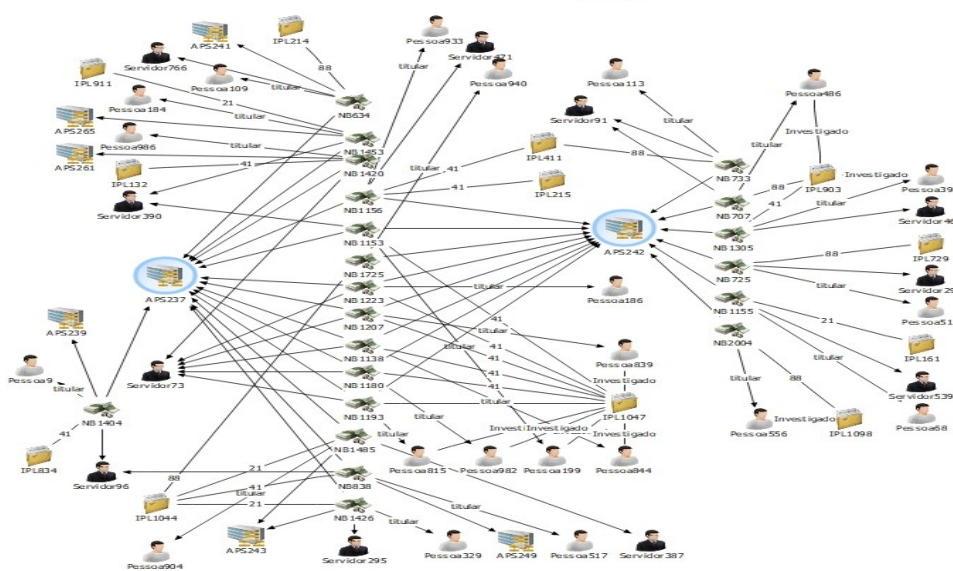
Não foram incluídos no subgrupo os benefícios previdenciários vinculados aos IPL1059 e IPL979. Mesmo excluídos aqueles vínculos, é possível constatar que foram concedidos na APS258 sete NBs, investigados em seis diferentes IPLs.

APS243



Na APS243 estão vinculados 16 NBs, objeto de investigação em 12 diferentes inquéritos policiais, o que é visto como indicativo de possível conexão entre as investigações.

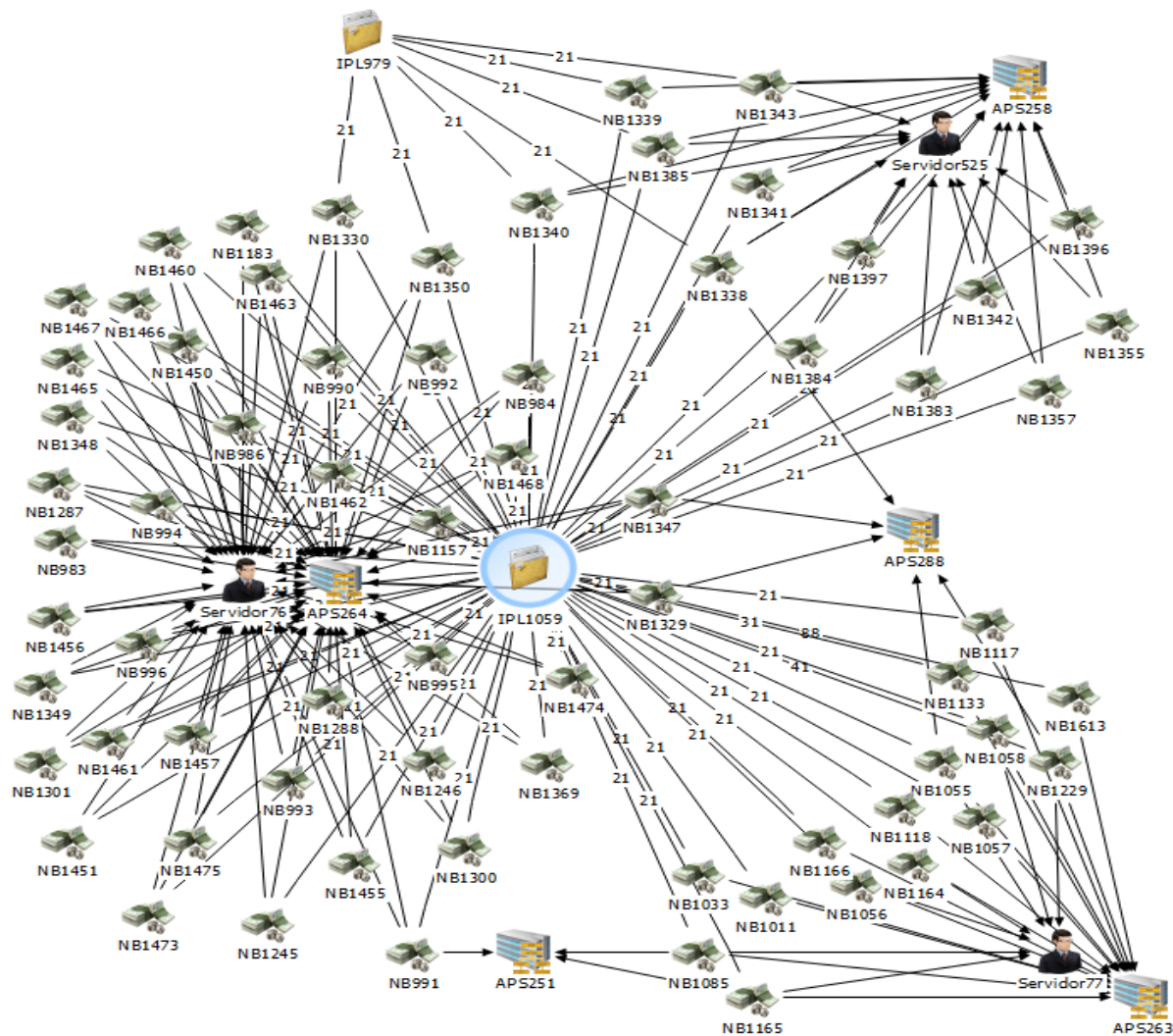
APS237
e
APS242



Na APS237 foram concedidos vários dos NBs que são investigados em inquéritos policiais e que foram concedidos pelo servidor73.

Como as duas APS apresentam vários NBs em comum (foram concedidos em uma APS e são mantidos na outra), foram diagramadas juntas. Da rede do subgrupo é possível ver que estão vinculados a tais APS o total de 21 NBs objeto de 12 diferentes IPLs.

IPL1059



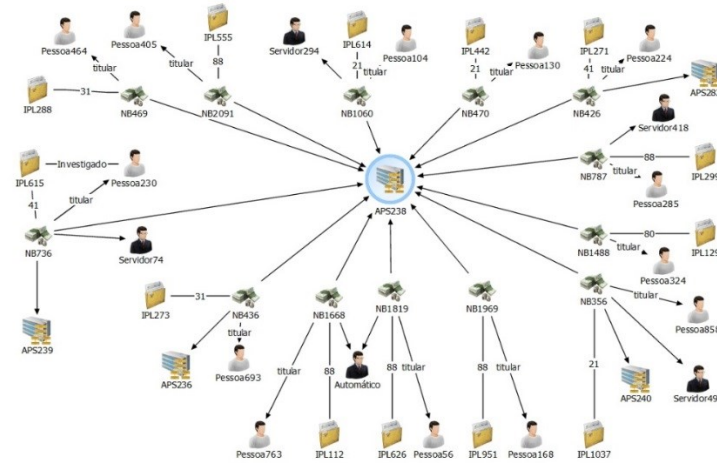
O IPL1059 serviu de base para operação de combate a combate a grupo criminoso organizado atuante na área de fraudes previdenciárias. No caso específico, os benefícios fraudados eram do grupo 21, ou seja, benefícios de pensão por morte (ou congêneres, como a pensão por morte de trabalhador rural).

No caso concreto, a investigação apresentou conexão com os fatos que estavam sendo investigados no IPL979, sendo os casos reunidos para investigação conjunta.

Da rede é possível perceber 3 grupos mais ou menos distintos: a) benefícios concedidos pelo servidor76 na APS264; b) benefícios concedidos pelo Servidor525 na APS258; c) benefícios concedidos pelo Servidor77 na APS263.

No caso concreto, foi comprovada nas investigações o envolvimento dos servidores responsáveis pela concessão dos benefícios, uma vez que ficou comprovado que os mesmos foram concedidos de maneira fraudulenta.

APS238



Na APS238 foram concedidos 13 NBs que estão sob investigação em 13 diferentes inquéritos policiais, sendo que os NBs investigados nos inquéritos policiais IPL112 e IPL626 são de concessão automática, do grupo de benefícios da LOAS.

Fonte: autoria própria

Tabela 29
Medições dos principais atores da rede da UF2

Entidade	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core	Entidade	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
IPL1059	19,37569	4,6273	9,703	75,0396	4	IPL578	2,072116	4,5208	0,6931	0,19503	2
Automático	48,11847	4,8453	4,8515	1,568904	3	IPL979	0,03763	4,3179	0,6931	5,290832	4
APS264	6,351117	4,5017	4,4554	45,22574	3	IPL872	0,768333	4,4799	0,6931	0,094336	3
Servidor76	0,61778	4,3765	4,0594	44,036	3	APS252	2,784075	4,4111	0,6931	0,040607	2
APS236	19,96082	4,6983	3,0693	0,204587	2	Servidor77	0,066783	4,339	0,6931	4,1358	3
APS251	14,36203	4,6529	2,4752	2,836627	3	IPL287	0,971455	4,1703	0,5941	0,000135	1
APS263	4,939212	4,5763	2,1782	9,053347	3	Servidor73	0,137738	4,2281	0,5941	0,001069	4
APS239	12,60248	4,6318	2,1782	0,083078	2	NB1338	0,501886	4,4963	0,5941	8,063991	4
APS258	6,738414	4,603	1,9802	8,227469	4	IPL1004	0,598431	4,4462	0,5941	0,022407	2
IPL1047	1,562284	4,2192	1,8812	0,00128	4	NB1156	1,192662	4,3915	0,5941	0,002143	2
APS243	6,099164	4,5666	1,5842	0,049631	3	NB1330	0,442775	4,4499	0,5941	13,78888	3
APS237	7,318601	4,4766	1,3861	0,011208	4	APS250	2,543784	4,4969	0,5941	0,022915	2
APS242	7,15964	4,5099	1,3861	0,0147	4	APS269	1,434062	4,3863	0,5941	0,595737	2

IPL1044	9,132598	4,6931	1,3861	0,397894	3	APS288	0,018741	4,3249	0,495	4,026022	3
APS238	7,227708	4,5434	1,2871	0,02452	2	IPL135	0,777556	4,305	0,495	0,001369	1
APS255	6,375951	4,5436	1,2871	0,0438	2	IPL770	0,003533	0,0996	0,495	0	1
APS245	5,942718	4,5371	1,1881	0,019862	2	IPL792	0,777556	4,2494	0,495	0,000558	1
Servidor525	0,016742	4,314	1,1881	7,243974	4	IPL801	0,777556	4,3738	0,495	0,001926	1
IPL617	1,266712	4,5164	1,1881	0,038226	2	IPL809	0,777556	4,1397	0,495	0,304968	1
IPL560	1,81018	4,4943	1,0891	0,04924	3	IPL834	0,597267	4,3034	0,495	0,001221	2
APS253	2,511653	4,4835	0,9901	0,096219	3	IPL880	0,80004	4,1793	0,495	0,000235	2
APS278	1,037996	4,4819	0,8911	0,036945	3	IPL888	0,396135	4,4578	0,495	0,168511	2
APS234	3,866781	4,5107	0,8911	0,047747	2	IPL903	0,195992	4,146	0,495	0,000216	2
APS241	3,550179	4,5602	0,8911	0,026695	2	IPL930	0,195338	4,4289	0,495	0,023085	2
APS247	4,797761	3,6506	0,7921	2,73E-06	2						

Fonte: autoria própria

Observando o subgrupo formado a partir do IPL1059, tem-se que naquele inquérito policial foram investigados pelo menos 69 benefícios previdenciários fraudados, tendo sido identificado que muitos dos benefícios foram concedidos pelo Servidor76, na APS264; alguns pelo Servidor525, na APS258; e alguns pelo Servidor77, na APS263. Tais constatações podem ser apresentadas resumidamente conforme rede da Figura 21.

Tabela 30
Matriz de Correlação da UF2

APS-Servidor	Frequência	IPL132	IPL156	IPL544	IPL549	IPL560	IPL579	IPL617	IPL776	IPL872	IPL886	IPL888	IPL920	IPL979	IPL1047	IPL1059	IPL1105	IPL1113
APS264-Servidor76	43	0	0	0	0	0	0	0	0	0	0	0	0	2	0	41	0	0
APS258-Servidor525	16	0	0	0	0	0	0	0	0	0	0	0	0	4	0	12	0	0
APS263-Servidor77	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0
APS237-Servidor73	6	1	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0
APS239-Automático	6	0	0	1	0	2	1	1	1	0	0	0	0	0	0	0	0	0
APS263-Automático	6	0	0	0	1	0	0	0	0	0	2	2	0	0	0	1	0	0
APS242-Servidor73	5	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0
APS251-Automático	5	0	0	0	0	0	0	0	0	3	0	0	1	0	0	0	0	1
APS234-Automático	4	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0
APS278-Servidor312	4	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0

Fonte: autoria própria

Apêndice III - Individualização das redes de subgrupos da UF3

A lista dos dez servidores com maior grau de centralidade na rede consta da Tabela 31 e a lista das dez Agências da Previdência Social com maior grau de centralidade na rede consta da Tabela 32. Da Tabela 31 é possível observar que os processos de concessão automática representam o maior grau de centralidade dentre os servidores. Os servidores com maior grau de centralidade na rede são: Servidor66, Servidor104, Servidor100, Servidor31, Servidor267, Servidor106, Servidor198, Servidor242 e Servidor397. Destes, ressalta-se o Servidor106, que está vinculado a diversos NBs objetos do IPL864.

Tabela 31

Servidores com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
S_Automático	73,86	1,71	10,40	96,31	3
Servidor66	0,05	1,63	0,49	0,06	2
Servidor104	0,01	1,63	0,40	0,18	2
Servidor100	0,01	1,62	0,40	0,11	3
Servidor31	0,30	1,63	0,26	0,06	2
Servidor267	0,01	1,61	0,26	0,01	2
Servidor106 (IPL864)	0,0002	1,57	0,26	0,0005	3
Servidor198	0,03	1,61	0,22	0,004	2
Servidor242	0,01	1,61	0,22	0,009	2
Servidor397	0,002	1,61	0,22	0,11	3

Fonte: autoria própria

Tabela 32

APS com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
APS44	19,44	1,69	3,39	11,90	3

APS114	11,31	1,67	2,85	4,40	2
APS82	7,19	1,67	2,00	4,48	3
APS72	8,51	1,67	1,87	2,29	2
APS97	3,55	1,66	1,83	9,05	4
APS40	4,11	1,67	1,69	6,30	3
APS37	2,27	1,67	1,47	4,18	3
APS38	3,94	1,67	1,42	2,47	3
APS39	3,36	1,67	1,29	6,91	3
APS96 (IPL939)	1,68	1,66	1,16	4,81	3

Fonte: autoria própria

Na Tabela 32 aparece com a maior centralidade na rede a APS44, agência na qual foram concedidos vários dos benefícios fraudulentos objeto do IPL889. Aparecem ainda as APS114, APS82, APS72, APS97, APS40, APS37, APS38, APS39 e APS96. Nesta última APS96 foram concedidos vários dos benefícios objeto de investigação no IPL939, cuja rede está mapeada adiante.

Para cada servidor e APS listados nas Tabelas 31 e 32 foi gerada um subgrupo, cujos dados compilados constam da Tabela 33, sendo as redes apresentadas e comentadas individualmente conforme Tabela 34 e Tabela 35.

Tabela 33

Dados das redes do subgrupo formadas com atores de maior grau de centralidade

Rede do subgrupo do ator:	APS na rede do subgrupo	NBs na rede do subgrupo	IPLs na rede do subgrupo	Servidores na rede do subgrupo	Total de atores na rede do subgrupo	Total de vínculos na rede do subgrupo
Automático	96	233	151	1	481	761
Servidor66	2	11	10	1	24	34
Servidor104	2	9	7	1	19	28
Servidor100	6	9	9	1	25	37
Servidor31	3	6	7	1	17	19
Servidor267	1	6	6	1	14	18
Servidor106	1	19	1	9	30	57

Servidor198	1	5	5	1	12	15
Servidor242	1	5	5	1	12	15
Servidor397	3	5	2	2	12	20
APS44	29	76	69	18	192	238
APS114	6	64	64	37	171	206
APS82	10	45	46	18	119	133
APS72	8	42	40	20	110	125
APS97	5	41	10	16	72	43
APS40	8	38	34	14	94	118
APS37	11	33	14	4	62	97
APS38	13	32	28	13	86	109
APS39	7	29	28	12	76	99
APS96	13	35	1	15	64	110

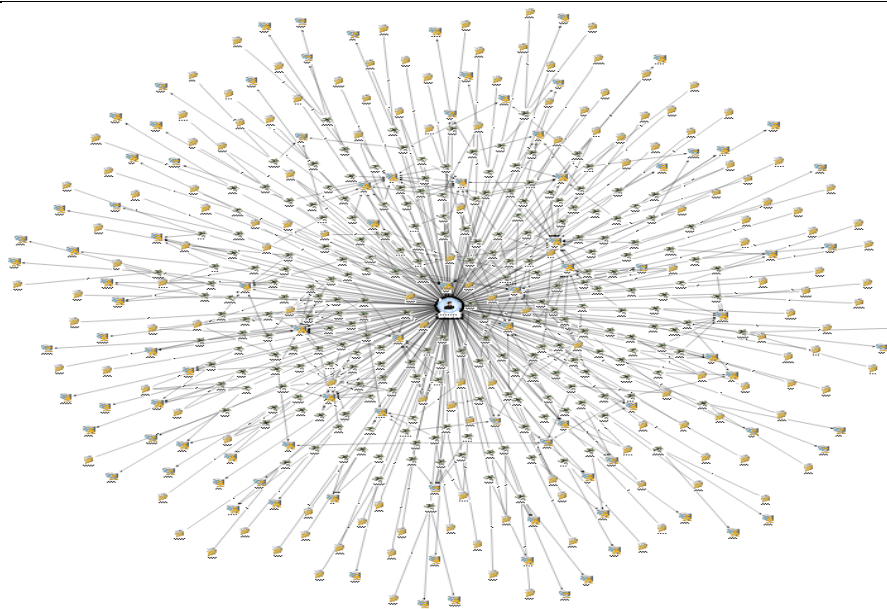
Fonte: autoria própria

Tabela 34

Redes de subgrupos formados a partir dos servidores da UF3

Ator	Rede	Comentários
------	------	-------------

Automático

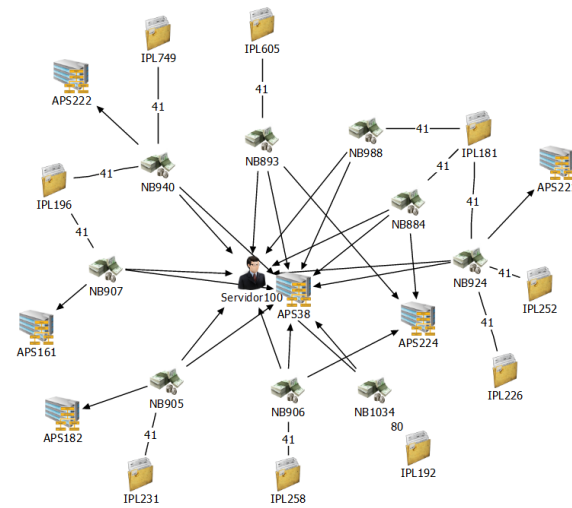


Foram identificados 233 NBs com concessão automática, vinculados a 151 diferentes inquéritos policiais e concedidos em 96 APSs diversas.

A concessão automática do benefício envolve NBs principalmente do grupo 31 (auxílio-doença) e 88 (benefícios da LOAS).

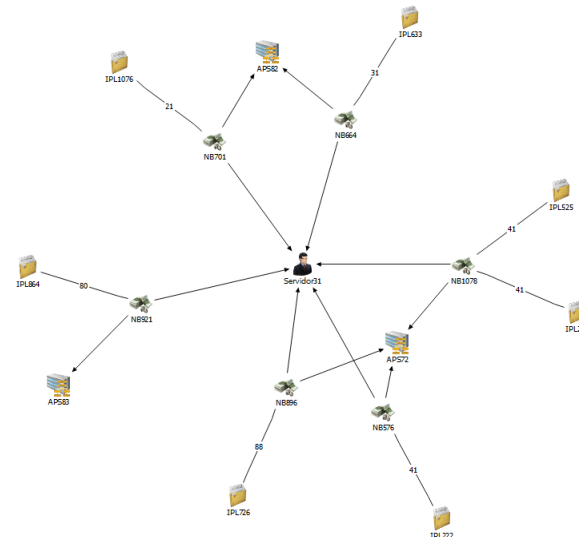
Como não consta um servidor diretamente responsável pela concessão, a comprovação da conexão entre as fraudes precisa ser comprovada por outros meios. Foi observada grande quantidade de benefícios concedidos nas APS44, APS114 e APS72.

Servidor100



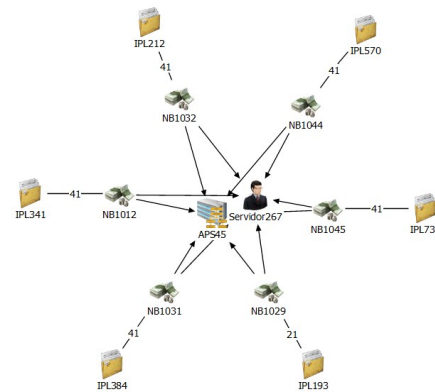
Na rede do subgrupo traçado a partir do Servidor100, é possível constatar a ocorrência de vários NBs concedidos na APS38, objetos de investigação em nove diferentes inquéritos policiais. Aqui é possível perceber maior homogeneidade nas fraudes cometidas, que são principalmente em processos de aposentadoria. Consta do IPL196 que aquele IPL é desdobramento de operação deflagrada na UF3, constatando-se que as fraudes são de natureza heterogênea (pós-óbito: IPL258, IPL605; LOAS: IPL231, IPL749; Aposentadoria por invalidez: IPL181; Aposentadoria IPL226).

Servidor31



Na rede do subgrupo traçado a partir do Servidor31, é possível constatar que atuou em processos de seis NBs, vinculados a 7 diferentes inquéritos policiais. Os benefícios foram concedidos em APSs diferentes e não foi localizada notícia que os inquéritos sejam desdobramentos de alguma operação na UF3, sendo que as fraudes são de natureza heterogênea (Pós-óbito: IPL1076, IPL726, IPL222, IPL525; pensão por morte: IPL633; Salário maternidade: IPL864; Aposentadoria: IPL295)

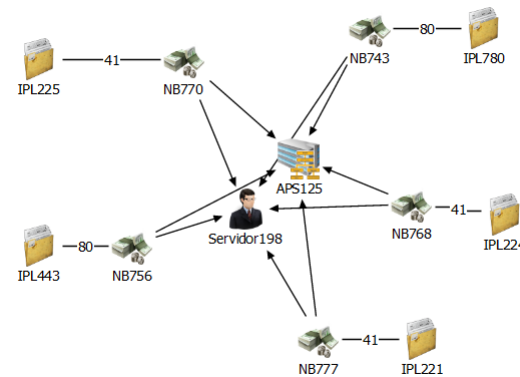
Servidor267



Na rede do subgrupo formado a partir do servidor267 é possível ver que este atuou em seis NBs, todos concedidos na APS45 e investigados em seis diferentes IPLs. Não foi localizada notícia que sejam desdobramento de operação e possuem naturezas diversas (fraude em atestado médico: IPL732, IPL570; saque pós óbito nos IPL193, IPL341 e IPL212; fraude em aposentadoria: IPL384)

Servidor106

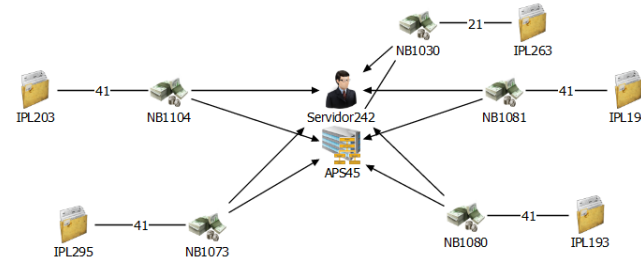
Servidor198



Já diagramado na rede do IPL864

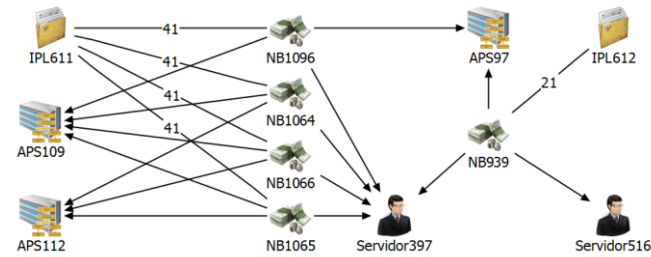
O servidor198 foi responsável pela concessão de cinco NBs, todos concedidos na APS125 e objeto de cinco diferentes inquéritos policiais. A natureza das fraudes também é heterogênea (saques pós-óbito: IPL224, IPL443 e IPL225; fraude em atestado médico: IPL221; fraude em bolsa família: IPL780).

Servidor242



O Servidor242 atuou na concessão de cinco NBs, todos na APS242, sendo as fraudes na maioria de saque pós-óbito (IPL263, IPL194 e IPL193), havendo também fraude em aposentadoria (IPL295) e notícia que o IPL203 é desdobramento de operação da UF3.

Servidor397



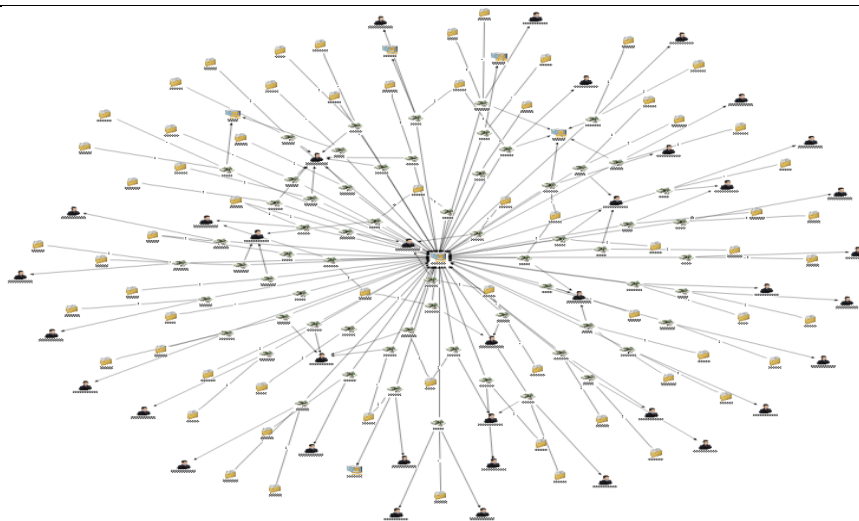
O servidor397 foi responsável pela concessão de cinco benefícios, investigados em dois diferentes IPLs. A maior parte dos benefícios é objeto do IPL611 mas o servidor também atuou no NB939, objeto do IPL612, o que indica possível conexão entre os inquéritos policiais.

Fonte: autoria própria

Tabela 35
Redes de subgrupos formados a partir das APSs da UF2

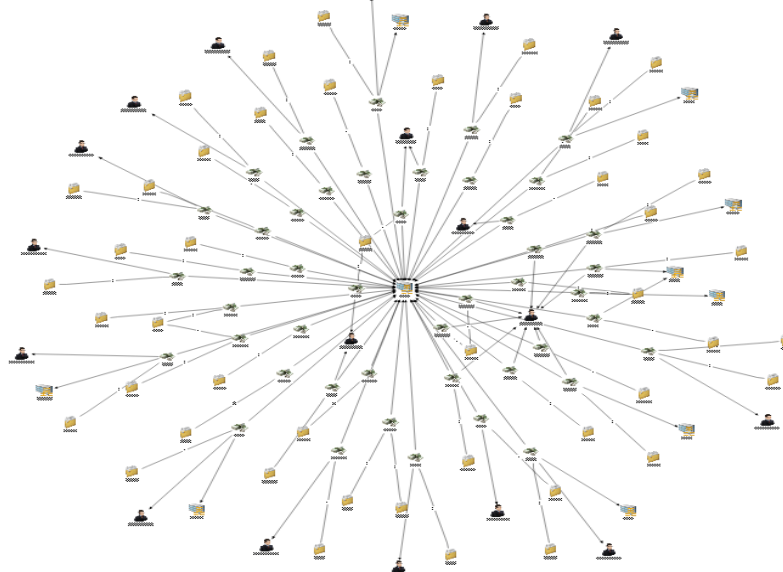
Ator	Rede	Comentários
APS44	<p>A large, complex network diagram with a central node (a square icon) connected to a vast number of peripheral nodes (mostly square icons). The connections are dense and radiate outwards from the center, forming a star-like or hub-and-spoke pattern. The nodes are arranged in a roughly circular pattern around the center.</p>	<p>Na rede formada a partir do subgrupo da APS44, é possível observar que naquela APS foram concedidos 76 NBs investigados em 69 IPLs. É visível que muitos dos NBs foram objeto de concessão automática. Observa-se que 2NBs concedidos na APS44 estão sendo investigados no mesmo IPL889. Não foi observado nenhum servidor com destaque no desenho da rede</p>

APS114



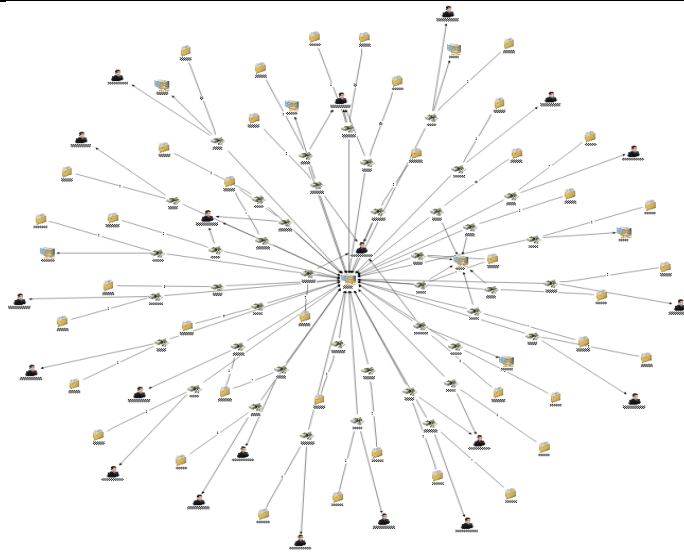
Na rede do subgrupo da APS114 é possível observar que estão vinculados à APS 64 NBs vinculados a 64 IPLs. Na análise da rede aparece também com centralidade os processos de concessão automática. Dentre os servidores, aparece o Servidor414, que atuou em quatro dos NBs investigados em quatro diferentes IPLs e Servidor635, Servidor331, Servidor631 e Servidor573, cada um responsável por três NBs investigados e vinculados à APS114.

APS82



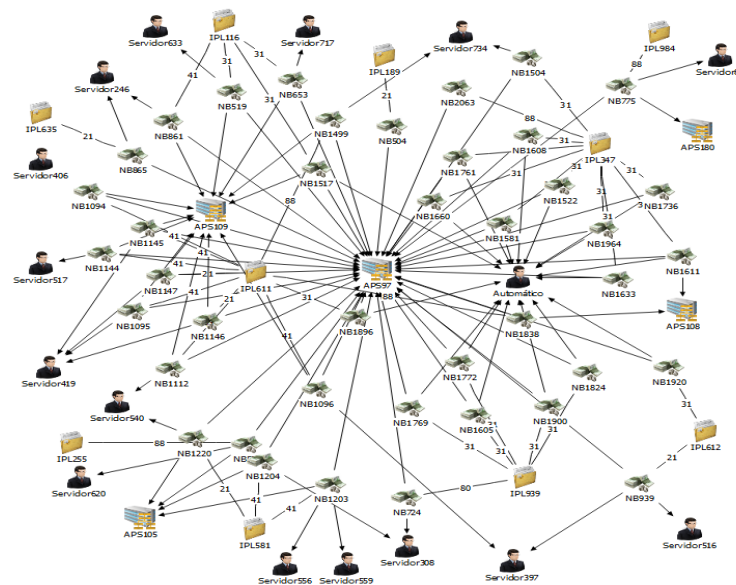
Vinculados à APS82 estão 45 NBs vinculados a 45 IPLs. Os processos de concessão automática aparecem com centralidade à direita do diagrama. Foi identificado apenas um servidor vinculado a mais de um benefício, que foi o Servidor31, vinculado a 2 NBs.

APS72



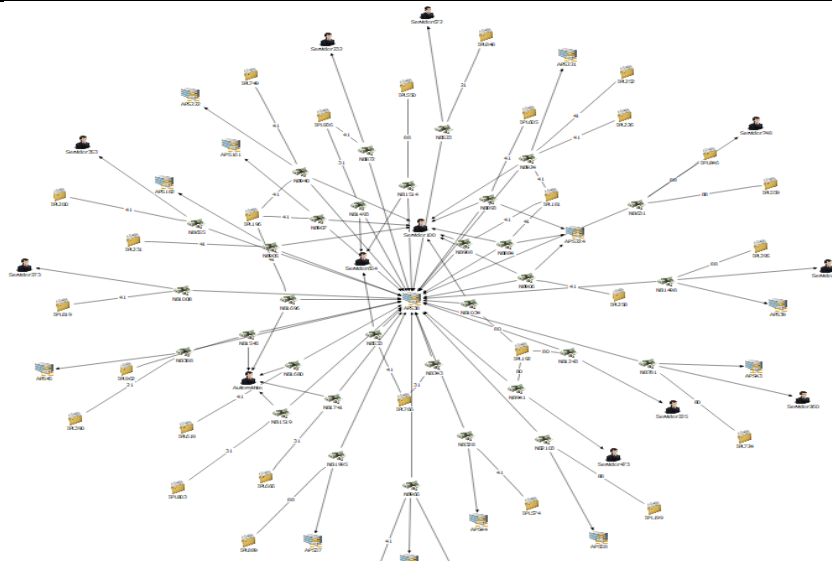
Na rede do subgrupo formado a partir da APS73 podem ser percebidos que estão a esta vinculados 42 NBs, vinculados a 40 IPLs. Foi identificado também aqui que apenas um servidor está vinculado a mais de um benefício, que foi o Servidor31, vinculado a 2 NBs

APS97



Na rede do subgrupo formado a partir da APS97 estão vinculados a esta 41 NBs, investigados em 10 IPLs diferentes. Foi possível observar ainda que vários dos NBs da rede possuem vinculação a uma segunda APS, a APS109 (os NBs foram concedidos em uma e são mantidos na outra). Possui também alta centralidade na rede o IPL611, onde estão sendo investigados 11 NBs sendo quatro deles concedidos pelo Servidor419. Destaca-se também o IPL939, que investiga seis NBs concedidos na APS97 e o IPL347, com onze NBs vinculados à APS

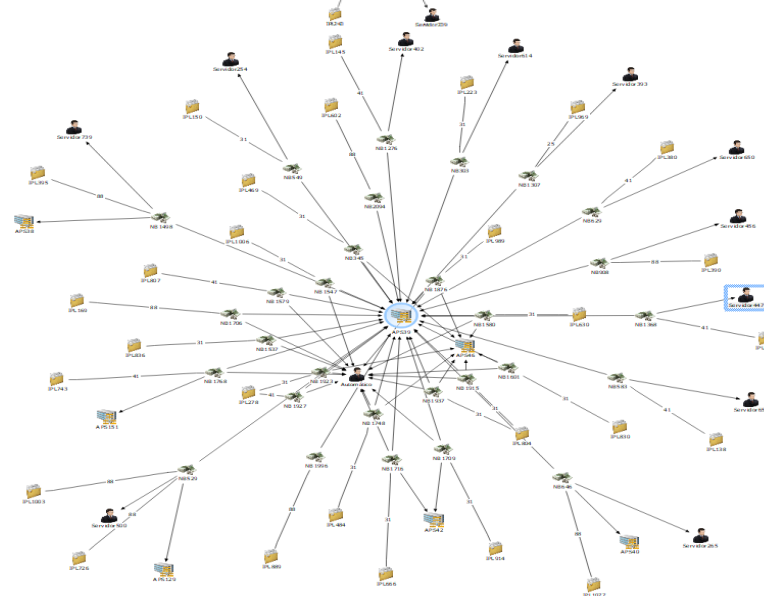
APS38



Na rede do subgrupo da APS38 é possível ver 32 NBs investigados em 28 IPLs. Na rede ganham destaque os NBs concedidos pelo Servidor100, vinculado a nove NBs., vinculados a nove IPLs. Além dele, é observável também o Servidor654 como vinculado a três NBs, vinculados a três IPLs.

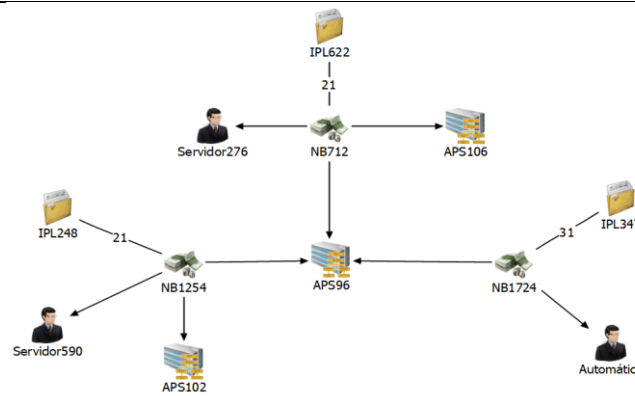
O ponto de concentração à esquerda do centro diz respeito aos processos de concessão automática.

APS39



Ao buscar o subgrupo formado a partir da APS39, constatou-se que vários dos NBs também estão vinculados à APS46 (no centro, à direita). Na rede estão 29 NBs vinculados a 28 IPLs e o único ponto que visualmente se destaca diz respeito aos NBs de concessão automática (no centro, abaixo à esquerda).

APS96



Vários dos NBs analisados no IPL939 foram concedidos na APS96. Assim, foram excluídos os NBs vinculados ao IPL939 e apresentado o subgrupo com os atores restantes, onde é possível ver que também na APS96 forma concedidos NBs investigados em 3 diferentes IPLs.

Fonte: autoria própria

Foi gerada listagem com análise das variáveis em relação a todos os 2240 atores da rede. Na tabela 36, em ordem decrescente pelo grau de centralidade, são colacionados os primeiros 40 resultados da rede formada na UF2, entendendo-se abrangidos os principais atores da rede.

Tabela 36

Medições dos principais atores da rede da UF2

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core	Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
IPL1059	19,37569	4,6273	9,703	75,0396	4	IPL560	1,81018	4,4943	1,0891	0,04924	3
Automático	48,11847	4,8453	4,8515	1,568904	3	APS253	2,511653	4,4835	0,9901	0,096219	3
APS264	6,351117	4,5017	4,4554	45,22574	3	APS278	1,037996	4,4819	0,8911	0,036945	3
Servidor76	0,61778	4,3765	4,0594	44,036	3	APS234	3,866781	4,5107	0,8911	0,047747	2
APS236	19,96082	4,6983	3,0693	0,204587	2	APS241	3,550179	4,5602	0,8911	0,026695	2
APS251	14,36203	4,6529	2,4752	2,836627	3	APS247	4,797761	3,6506	0,7921	2,73E-06	2
APS263	4,939212	4,5763	2,1782	9,053347	3	Servidor77	0,066783	4,339	0,6931	4,1358	3
APS239	12,60248	4,6318	2,1782	0,083078	2	IPL578	2,072116	4,5208	0,6931	0,19503	2
APS258	6,738414	4,603	1,9802	8,227469	4	IPL979	0,03763	4,3179	0,6931	5,290832	4
IPL1047	1,562284	4,2192	1,8812	0,00128	4	IPL872	0,768333	4,4799	0,6931	0,094336	3
APS243	6,099164	4,5666	1,5842	0,049631	3	APS252	2,784075	4,4111	0,6931	0,040607	2
IPL1044	9,132598	4,6931	1,3861	0,397894	3	Servidor73	0,137738	4,2281	0,5941	0,001069	4
APS237	7,318601	4,4766	1,3861	0,011208	4	NB1338	0,501886	4,4963	0,5941	8,063991	4
APS242	7,15964	4,5099	1,3861	0,0147	4	NB1156	1,192662	4,3915	0,5941	0,002143	2

APS238	7,227708	4,5434	1,2871	0,02452	2	NB1330	0,442775	4,4499	0,5941	13,78888	3
APS255	6,375951	4,5436	1,2871	0,0438	2	IPL287	0,971455	4,1703	0,5941	0,000135	1
Servidor525	0,016742	4,314	1,1881	7,243974	4	IPL1004	0,598431	4,4462	0,5941	0,022407	2
IPL617	1,266712	4,5164	1,1881	0,038226	2	APS250	2,543784	4,4969	0,5941	0,022915	2
APS245	5,942718	4,5371	1,1881	0,019862	2	APS269	1,434062	4,3863	0,5941	0,595737	2

Fonte: autoria própria

Para melhor visualização, foram geradas as redes dos subgrupos com base nos inquiridos policiais citados. Começando pela rede do subgrupo observado a partir do IPL889, que é apresentada na Figura 22, observa-se que vinculados ao IPL889 estão 44 NBs, concedidos em 13 diferentes APS, sendo boa parte dos benefícios de concessão automática.

centralidade na rede. Foi observado ainda que vários benefícios que tiveram concessão automática, ganhando destaque também os benefícios concedidos pelo Servidor590 (3 NBs), anotando-se também que o IPL939 deu origem a operação deflagrada na UF3.

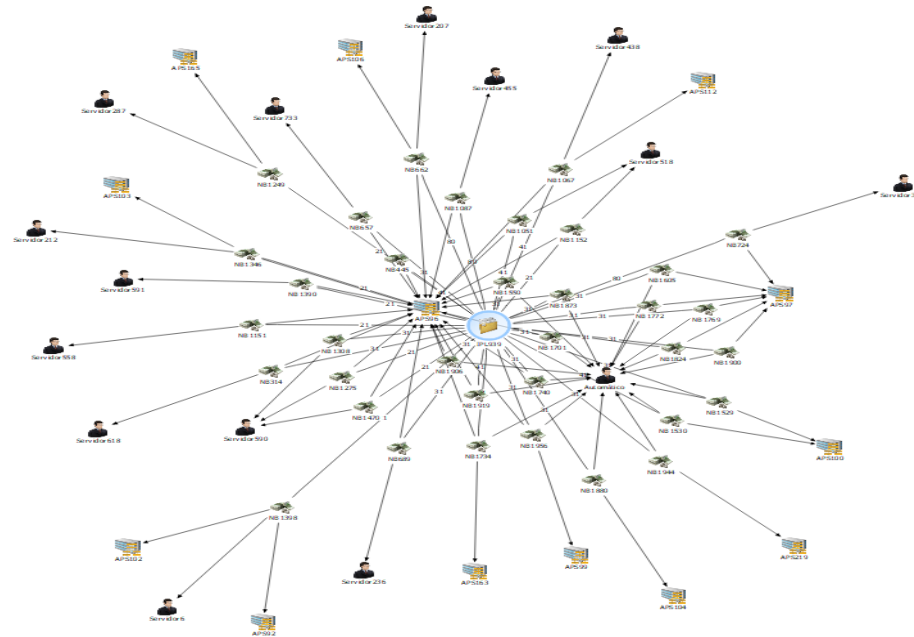


Figura 23. Rede formada a partir do IPL939

Foi ainda diagramada a rede do subgrupo do IPL864, conforme Figura 24. Na visão da rede, é possível perceber que estão vinculados ao IPL864 um total de 19 NBs, todos eles concedidos na APS83. Da rede é possível perceber ainda que vários dos benefícios foram concedidos pelos atores Servidor106 e Servidor501, sendo a maior parte dos benefícios investigados do grupo 80, ou seja, benefícios referentes ao salário-maternidade. Observando o caso real, constatou-se que de fato houve operação deflagrada sobre as fraudes investigadas, tendo sido responsabilizados o Servidor106 e o Servidor501, dentre outras pessoas.

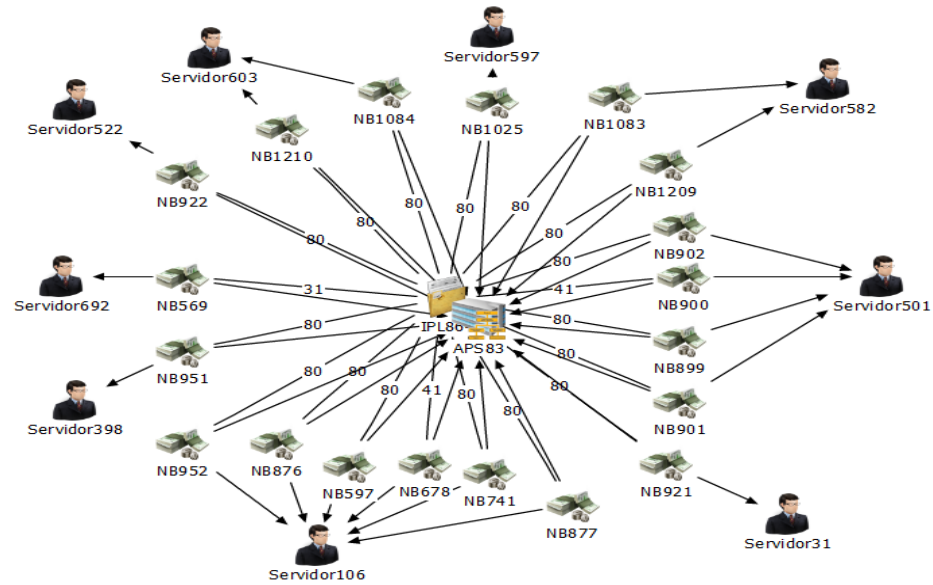


Figura 24. Rede formada a partir do IPL864

A matriz de correlação da rede da UF4 consta da Tabela 37

Tabela 37

Matriz de Correlação da UF3

APS-Servidor	Frequência	IFL124	IFL181	IFL184	IFL192	IFL193	IFL194	IFL196	IFL202	IFL203	IFL212	IFL220	IFL221	IFL224	IFL225	IFL230	IFL231	IFL247	IFL248	IFL258	IFL263	IFL274	IFL295	IFL297	IFL302	IFL341	IFL381	IFL384	IFL389	IFL408	IFL409
APS49-Servidor66	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
APS37-Servidor104	9	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
APS38-Servidor100	9	0	3	0	1	0	0	2	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	
APS45-Servidor267	6	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0		
APS83-Servidor106	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS116-Servidor432	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS123-Servidor198	5	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS45-Servidor242	5	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	
APS95-Servidor531	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	
APS109-Servidor397	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS109-Servidor419	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS114-Servidor414	4	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS117-Servidor216	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0	
APS123-Servidor108	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS129-Servidor264	4	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	
APS40-Servidor652	4	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	
APS83-Servidor501	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS96-Servidor390	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
APS97-Servidor419	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

APS-Servidor	IFL417	IFL421	IFL428	IFL431	IFL443	IFL470	IFL501	IFL566	IFL570	IFL590	IFL603	IFL605	IFL611	IFL673	IFL677	IFL705	IFL712	IFL732	IFL737	IFL744	IFL748	IFL778	IFL780	IFL808	IFL864	IFL889	IFL939	IFL993	IFL1019	IFL1042	IFL1110	
APS49-Servidor66	0	0	0	0	0	1	0	0	0	0	0	0	0	1	2	1	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	
APS37-Servidor104	2	0	0	0	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	
APS38-Servidor100	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS45-Servidor267	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS83-Servidor106	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	
APS116-Servidor432	0	0	0	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
APS123-Servidor198	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
APS45-Servidor242	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS95-Servidor531	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS109-Servidor397	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS109-Servidor419	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS114-Servidor414	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		
APS117-Servidor216	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS123-Servidor108	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	
APS129-Servidor264	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
APS40-Servidor652	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	
APS83-Servidor501	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	
APS96-Servidor390	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	
APS97-Servidor419	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fonte: autoria própria

Apêndice IV - Individualização das redes de subgrupos da UF4

A lista dos dez servidores com maior grau de centralidade na rede consta da Tabela 38 e a lista das dez Agências da Previdência Social com maior grau de centralidade na rede consta da Tabela 39.

Tabela 38

Servidores com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
Serv_Automático	56,40	3,43	8,92	17,31	4
Servidor668	0,83	3,25	2,76	31,07	4
Servidor157	1,39	3,25	2,15	21,42	4
Servidor183	0,77	3,26	0,76	0,56	3
Servidor190	0,34	3,20	0,76	0,13	3
Servidor601	0,002	3,13	0,61	0,16	4
Servidor565	0,002	3,13	0,61	0,16	4
Servidor709	0,46	3,22	0,46	0,12	2
Servidor644	0,11	3,18	0,46	0,03	2
Servidor171	0,04	3,24	0,46	0,38	3

Fonte: autoria própria

Tabela 39

APS com maior grau de centralidade na rede da UF1

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
APS2	23,21	3,33	6,61	3,10	4
APS5	21,36	3,33	6,30	7,07	3
APS21	7,48	3,27	5,07	51,28	4
APS10	5,83	3,26	5,07	53,47	4
APS3	13,91	3,33	3,07	1,14	3

APS15	0,45	3,14	2,30	0,57	4
APS1	11,24	3,23	2,15	0,08	2
APS4	10,10	3,32	2	0,38	2
APS6	7,82	3,24	1,84	0,40	3
APS7	2,46	3,28	1,23	0,63	2

Fonte: autoria própria

Para cada servidor e APS das Tabelas 38 e 39 foi gerado um subgrupo. Os dados dos subgrupos foram compilados e reunidos na Tabela 40, sendo as redes dos subgrupos apresentadas e comentadas individualmente, conforme Tabela 41 e Tabela 42.

Tabela 40

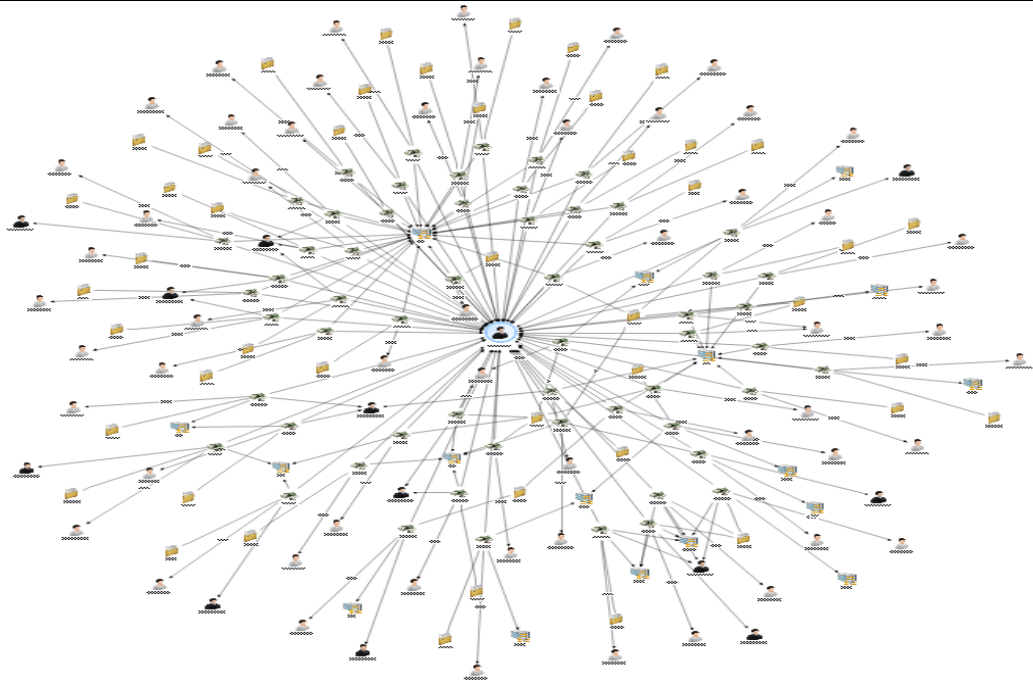
Dados das redes do subgrupo formadas com atores de maior grau de centralidade

Rede do subgrupo do ator:	APS na rede do subgrupo	NBs na rede do subgrupo	IPLs na rede do subgrupo	Servidores na rede do subgrupo	Total de atores na rede do subgrupo	Total de vínculos na rede do subgrupo
Automático	17	58	46	13	190	260
Servidor668, Servidor157	2	96	1	3	31	96
Servidor183	2	5	5	3	20	24
Servidor190	2	5	2	2	15	21
Servidor601, Servidor565	2	14	1	4	20	42
Servidor709	3	3	4	1	14	14
Servidor644	2	3	3	1	12	13
Servidor171	1	3	2	2	11	14
APS2	6	43	22	18	127	193
APS5	6	41	42	11	141	170
APS21, APS10	4	5	5	6	25	25
APS3	7	20	19	12	79	90

APS15 (IPL1023)	3	15	2	5	39	75
APS1	3	14	14	8	53	52
APS4	6	13	11	13	55	58
APS6	1	12	12	11	48	52
APS7	3	8	8	6	33	36

Fonte: autoria própria

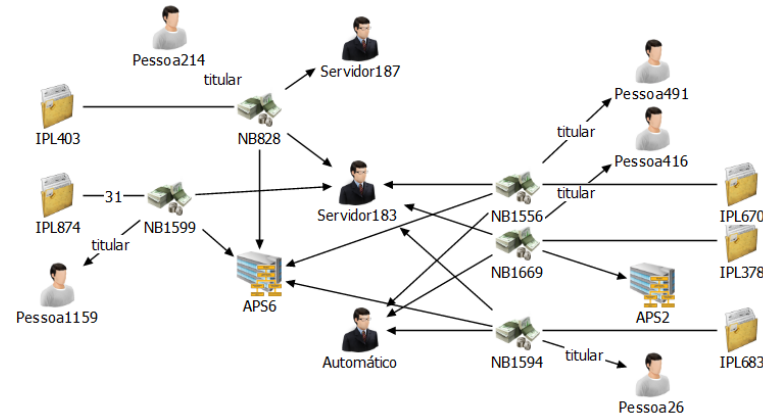
Tabela 41
Redes de subgrupos formados a partir dos servidores da UF4

Ator	Rede	Comentário
Automático		<p>Na rede formada a partir do subgrupo dos NBs com concessão automática aparecem 58NBs vinculados a 46 IPLs.</p> <p>Na rede destacam-se os NBs vinculados à APS2, com 10 NBs vinculados e a APS5, com 27 NBs vinculados. Dentre os servidores, o Servidor157 aparece vinculado a três NBs (investigados em dois IPLs) e o Servidor183, que será detalhado abaixo.</p>
Servidor668		Faz parte da rede do IPL720. Não foram identificados outros benefícios concedidos pelo servidor e investigados em outros inquéritos policiais.

Servidor157

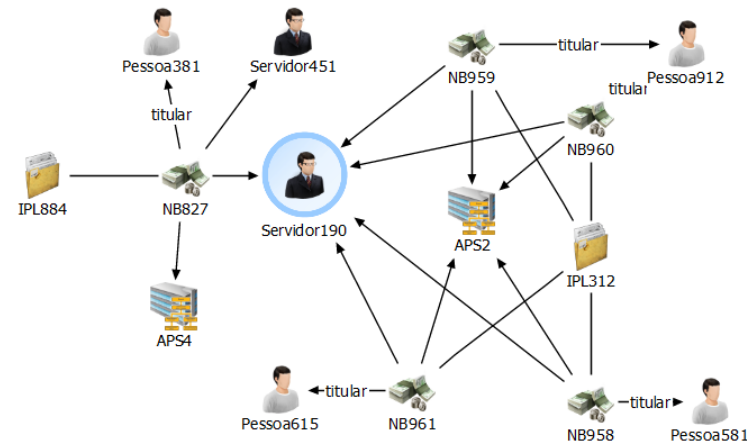
Também relacionado na rede do IPL720. Contudo, foi identificado que também foi o servidor responsável pela concessão do NB1569, investigado no IPL706. Não foram identificados outros benefícios investigados em inquéritos policiais da UF4 com vinculação ao Servidor157.

Servidor183



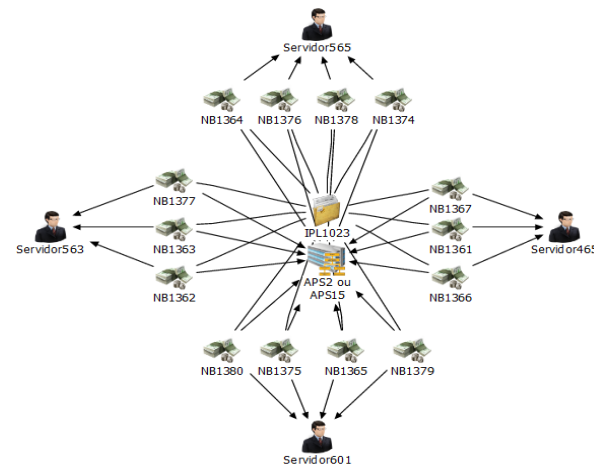
Na rede do subgrupo formado a partir do Servidor183, é possível observar que o servidor foi responsável pela concessão de cinco NBs, vinculados a cinco diferentes IPLs. É possível observar ainda que quatro dos cinco NBs estão vinculados à APS6

Servidor190



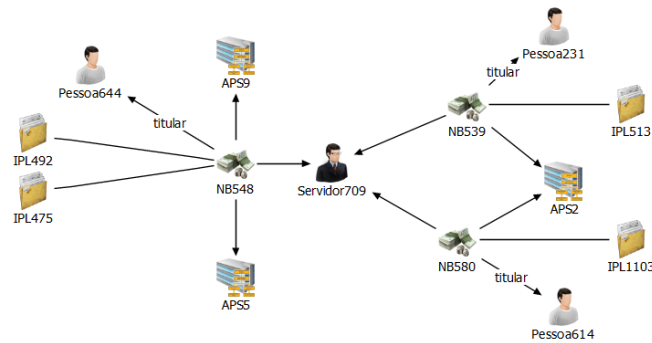
Na rede do subgrupo formado a partir do Servidor190 é possível observar que o servidor foi responsável pela concessão de cinco NBs investigados em dois IPLs. Os NBs vinculados ao IPL312 foram concedidos na mesma APS2. Essa conformação segue o mesmo modelo-base delineado na seção 4.2.

Servidor601 e
Servidor565



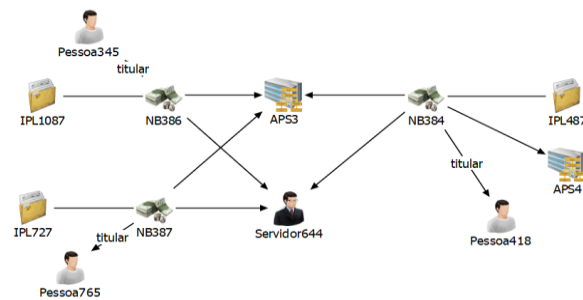
Na rede do subgrupo formado a partir do IPL1023 é possível observar a vinculação de pelo menos quatro servidores: os Servidor601 e Servidor565, vinculados a quatro NBs; os servidores Servidor563 e Servidor465, vinculados a três NBs. Todos os benefícios estão vinculados à APS2 ou à APS5.

Servidor709



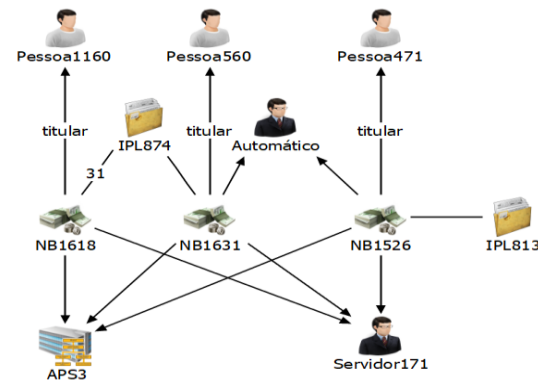
Na rede formada a partir do Servidor709 é possível ver que este é vinculado a três NBs, citados/investigados em quatro IPLs (o NB548 aparece vinculado a dois IPLs diferentes)

Servidor644



Na rede formada a partir do Servidor644, é possível ver que está vinculado a três NBs, investigados em três diferentes IPLs.

Servidor171



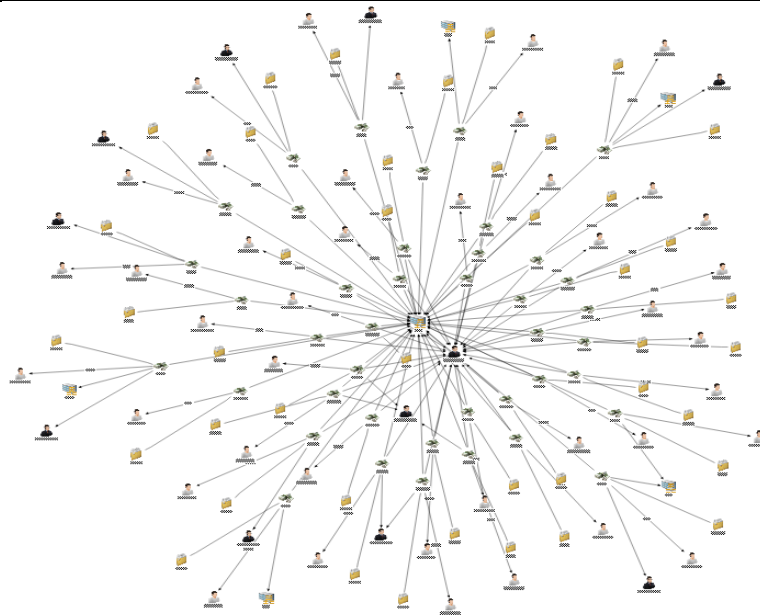
Na rede formada a partir do Servidor171, é possível ver que está vinculado a três diferentes NBs, investigados em dois IPLs.

Tabela 42

Redes de subgrupos formados a partir das APSs da UF4

Ator	Rede	Comentário
APS2	<p>The diagram shows a complex network with a central hub. Numerous nodes are connected to this hub, representing a dense web of relationships between different entities in the network.</p>	<p>Na rede do subgrupo formado a partir da APS2 estão 43 NBs vinculados a 22 IPLs. No centro à esquerda é visível a concentração dos NBs de concessão automática. No centro à direita, concentrados os vínculos referentes ao IPL1023 e vinculados também à APS15. Na APS2 foram concedidos também os quatro NBs vinculados ao IPL884, os dois NBs vinculados ao IPL609, os dois NBs vinculados ao IPL874, os quatro NBs vinculados ao IPL312. Os servidores com maior centralidade são os vinculados ao IPL1023 e serão destacados ao falar da APS15 adiante.</p>

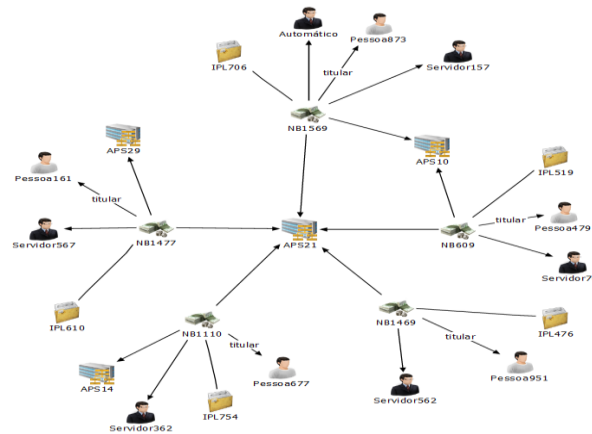
APS5



Na rede do subgrupo formado a partir da APS15 estão 42 NBs investigados em 41 IPLs. No centro à direita estão vinculados os NBs de concessão automática.

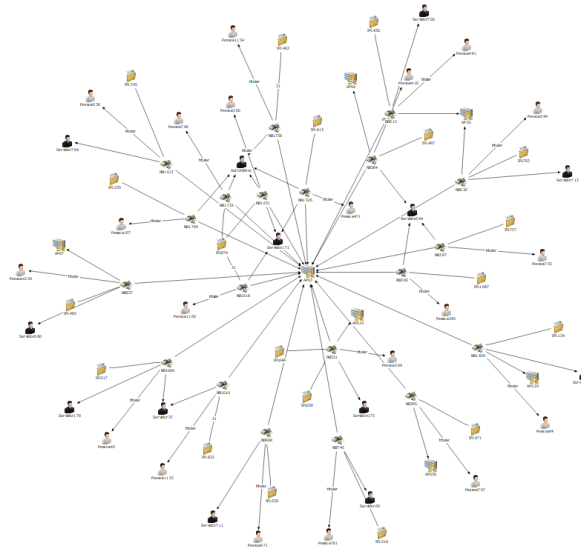
Na rede o servidor de maior centralidade é o Servidor158, responsável pela concessão de três NBs, investigados em três IPLs diferentes.

APS21
e
IAPS10



Analisada junto com o IPL720. Excluídos os benefícios ligados ao IPL720, foram identificados outros 5 benefícios concedidos na APS21, investigados em 5 inquéritos policiais distintos. Os benefícios vinculados à APS10 também estão apontados na diagramação referente ao IPL720. Contudo, não foram identificados outros benefícios concedidos na APS10 em investigação em outros inquéritos policiais (que não os já citados no IPL720).

APS3

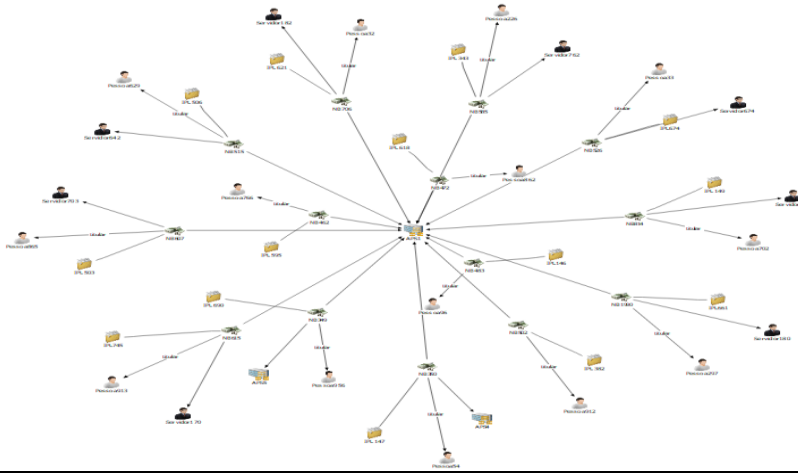


Na rede do subgrupo formado a partir da APS3 estão 20 NBs investigados em 19IPLs. Da rede é possível observar que o Servidor171 está vinculado a três NBs, investigados em dois IPLs. O Servidor644 também está vinculado a três NBs, mas investigados em três diferentes IPLs. A pequena concentração acima e à esquerda do centro diz respeito aos NBs de concessão automática.

APS15

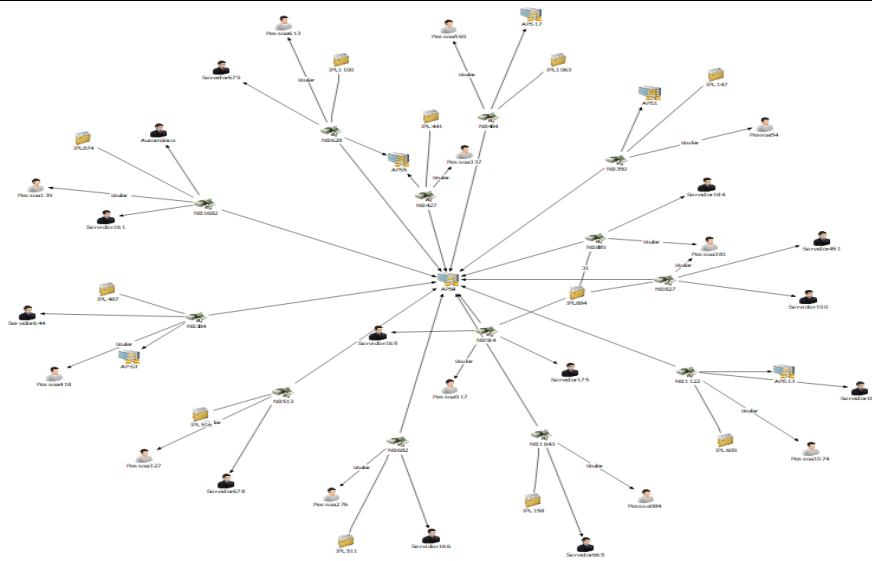
Os benefícios vinculados à APS15 estão vinculados ao IPL1023, descrito junto com os servidor Servidor601 e Servidor565 acima. Excluídos da rede do subgrupo os benefícios vinculados ao IPL1023, identificou-se apenas um benefício vinculado à APS15, em investigação no IPL679.

APS1



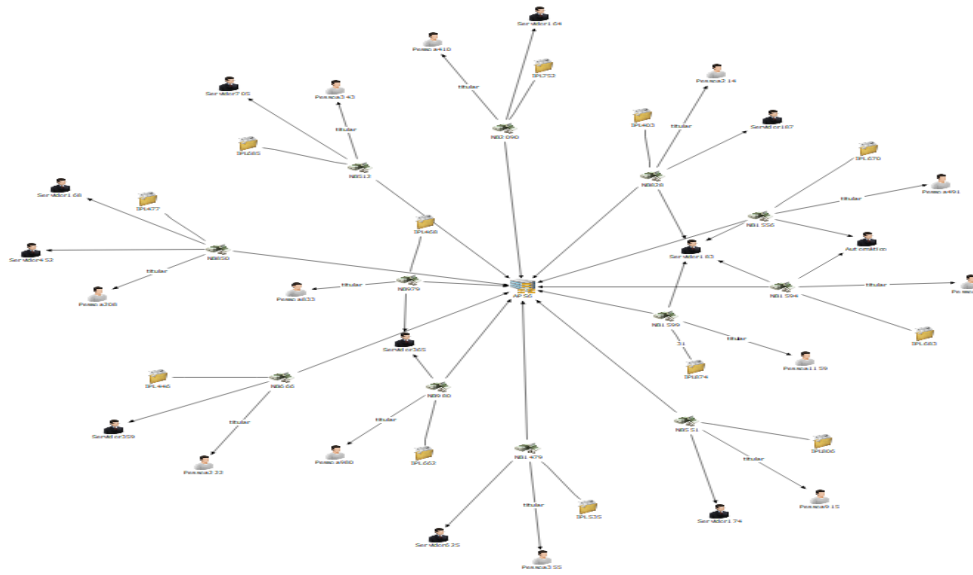
Na rede do subgrupo formado a partir da APS1 estão 14 NBs vinculados a 14 IPLs. Não foram observados na rede outros vínculos entre diferentes NBs ou IPLs.

APS4



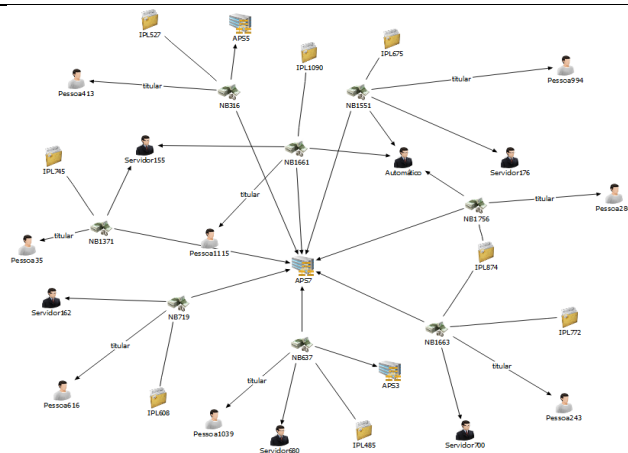
Na rede do subgrupo formado a partir da APS4 estão 13 NBs investigados em 11 IPLs. Na rede é observável o IPL884, ao qual estão vinculados três NBs concedidos a APS4, não tendo sido observados outros vínculos que reúnam diferentes NBs ou IPLs.

APS6



Na rede do subgrupo formado a partir da APS6 estão 12 NBs investigados em 12 diferentes IPLs. Na rede aparece o Servidor365, vinculado a dois NBs investigados em dois diferentes IPLs. Aparece também o Servidor183, vinculado a quatro NBs em investigação em quatro diferentes IPLs.

APS7



Na rede do subgrupo formado a partir da APS7 estão oito NBs vinculados a oito diferentes IPLs. Na rede, o Servidor155 aparece vinculado a dois NBs vinculados a dois IPLs diferentes, e os NBs de concessão automática aparecem à direita acima do centro.

Fonte: autoria própria

Foi gerada listagem com análise das variáveis em relação a todos os 651 atores da rede. Na Tabela 43, em ordem decrescente pelo grau de centralidade, são colacionados os primeiros 40 resultados da rede formada na UF2, entendendo-se abrangidos os principais atores da rede.

Tabela 43

Medições dos principais atores da rede da UF4

Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core	Ator	Intermediação%	Proximidade%	Grau%	Eigenvector%	K-Core
Automático	73,86257	1,7153	10,4064	96,31807	3	APS39	3,36719	1,6704	1,2952	6,919327	3
APS44	19,44671	1,6924	3,3944	11,90408	3	APS96	1,687915	1,6627	1,1612	4,816252	3
APS114	11,31933	1,6758	2,8584	4,404227	2	APS41	2,906601	1,6458	0,9379	0,154964	2
APS82	7,191728	1,6782	2,0098	4,485378	3	APS48	2,649467	1,6699	0,9379	1,418262	3
IPL889	2,168654	1,6758	1,9652	5,984801	3	APS83	2,407545	1,6265	0,9379	0,011196	3
APS72	8,513368	1,678	1,8758	2,298121	2	APS70	2,0881	1,6704	0,8933	2,38461	3
APS97	3,557419	1,6641	1,8312	9,059333	4	APS80	2,651793	1,6423	0,8486	0,111672	2
APS40	4,11663	1,6756	1,6972	6,300932	3	IPL864	0,078367	1,5861	0,8486	0,001747	3
IPL939	2,606727	1,6645	1,5632	8,491886	3	APS45	2,508293	1,6656	0,8039	0,435208	2
APS37	2,270352	1,6714	1,4739	4,182294	3	APS75	1,951963	1,6642	0,8039	3,439865	3

APS38	3,942552	1,6754	1,4292	2,473015	3	APS125	1,84336	1,6351	0,8039	0,022934	2
APS42	1,76979	1,671	0,8039	2,700366	3	APS74	2,634469	1,669	0,6699	0,473564	2
APS109	0,269338	1,662	0,8039	1,029879	4	APS116	2,070864	1,6639	0,6253	0,8432	3
APS122	2,828207	1,6692	0,7593	0,477646	2	APS129	1,204946	1,626	0,5806	0,040755	2
APS117	2,302305	1,6416	0,7593	0,111204	3	APS47	1,193211	1,6636	0,5806	1,29289	3
APS49	1,831893	1,663	0,7593	0,879208	2	APS58	1,00611	1,6729	0,5806	1,853966	3
APS46	1,233323	1,6746	0,7593	4,7332	3	APS55	0,580799	1,6628	0,5806	2,637706	3
APS95	2,441956	1,6619	0,7146	0,423262	3	IPL347	0,0862	1,6624	0,5806	4,956052	3
APS137	1,941562	1,6631	0,7146	2,114212	3	APS94	2,535269	1,6622	0,536	1,657888	2
IPL611	0,472305	1,6619	0,7146	1,333346	4	APS56	0,880039	1,6644	0,536	1,317846	3

Fonte: autoria própria

Foi gerada a rede do subgrupo dos vínculos do IPL720, rediagramada para melhor visualização, conforme consta da Figura 25. Na figura, é possível perceber que vinculados ao IPL720 estão 31 NBs, concedidos principalmente pelos servidores Servidor 668 e Servidor157, na APS10 ou na APS21. É possível constatar ainda que todos os benefícios são do grupo 88, ou seja, benefícios da LOAS. Confrontando a rede com o caso concreto, constatou-se que o IPL720 serviu de base para operação que resultou na responsabilização do Servidor668 e do Servidor157, além de outras pessoas.

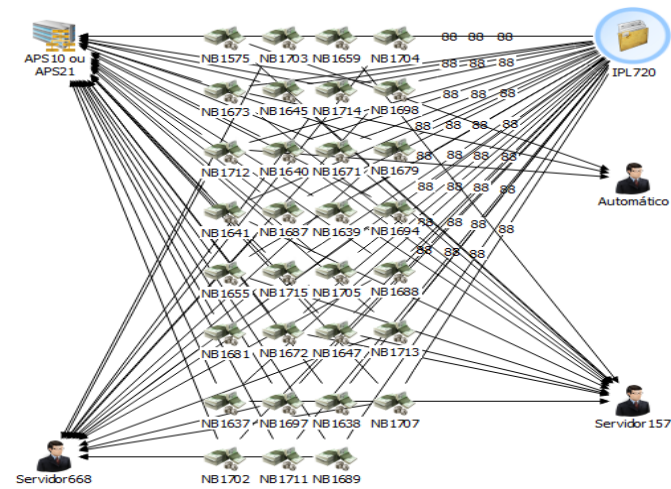


Figura 25. Rede da rede do subgrupo do IPL720

A matriz de correlação da UF4 consta da Tabela 44.

Tabela 44

Matriz de correlação da UF4

APS-Servidor	Frequência	IPL312	IPL378	IPL403	IPL462	IPL495	IPL535	IPL561	IPL569	IPL575
APS5-Automático	27	0	0	0	1	1	0	1	1	1
APS10-Servidor668	18	0	0	0	0	0	0	0	0	0
APS21-Servidor668	17	0	0	0	0	0	0	0	0	0
APS10-Servidor157	14	0	0	0	0	0	0	0	0	0
APS2-Automático	10	0	1	0	0	0	0	0	0	0
APS21-Servidor157	9	0	0	0	0	0	0	0	0	0
APS3-Automático	5	0	0	0	1	0	1	0	0	0
APS6-Servidor183	4	0	0	1	0	0	0	0	0	0
APS2-Servidor601	4	0	0	0	0	0	0	0	0	0
APS2-Servidor565	4	0	0	0	0	0	0	0	0	0
APS2-Servidor190	4	4	0	0	0	0	0	0	0	0
APS15-Servidor601	4	0	0	0	0	0	0	0	0	0
APS15-Servidor565	4	0	0	0	0	0	0	0	0	0
APS10-Automático	4	0	0	0	0	0	0	0	0	0

APS-Servidor	IPL653	IPL664	IPL665	IPL668	IPL670	IPL672	IPL681	IPL683	IPL693	IPL694
APS5-Automático	1	1	1	1	0	1	0	0	1	1
APS10-Servidor668	0	0	0	0	0	0	0	0	0	0
APS21-Servidor668	0	0	0	0	0	0	0	0	0	0
APS10-Servidor157	0	0	0	0	0	0	0	0	0	0
APS2-Automático	0	0	0	0	0	0	1	0	0	0
APS21-Servidor157	0	0	0	0	0	0	0	0	0	0
APS3-Automático	0	0	0	0	0	0	0	0	0	0
APS6-Servidor183	0	0	0	0	1	0	0	1	0	0
APS2-Servidor601	0	0	0	0	0	0	0	0	0	0
APS2-Servidor565	0	0	0	0	0	0	0	0	0	0
APS2-Servidor190	0	0	0	0	0	0	0	0	0	0
APS15-Servidor601	0	0	0	0	0	0	0	0	0	0
APS15-Servidor565	0	0	0	0	0	0	0	0	0	0
APS10-Automático	0	0	0	0	0	0	0	0	0	0

Fonte: autoria própria

Apêndice V – Memória de cálculo

Foram colhidos os dados referentes à quantidade de servidores indiciados, outros indiciados, número de processos de benefícios fraudados e prejuízo total apurado, organizados conforme Tabela 45. Os dados referentes a duas operações consecutivas foram agrupados, como nos casos das operações Casa Cheia e Intervenção. Os dados foram então tratados com o software Microsoft Excel versão 2013, sendo utilizada a função “Análise de dados” - “regressão”, utilizando como variável dependente o valor do prejuízo apurado, gerando os dados da Tabela 46, gerando R^2 de 0,9956.

Tabela 45

Dados gerais e estatísticas de regressão das Operações

Operação	Prejuízo	Não-Servidores indiciados	Servidores indiciados	NBs fraudados
Fim de Linha	R\$ 897.145,90	5	1	64
Casa Chaeia I e II	R\$ 3.270.000,00	11	3	177
Intervenção I e II	R\$ 3.066.158,99	2	1	107
Aquestos	R\$ 1.694.389,61	10	5	9
Duo Fratres II	R\$ 1.150.000,00	5	0	107

Tabela 46

Estatística de regressão

<i>Estatística de regressão</i>	
R múltiplo	0,9978
R-Quadrado	0,9956
R-quadrado ajustado	0,9825
Erro padrão	144592,5367
Observações	5,0000

ANOVA

	<i>Gl</i>	<i>SQ</i>	<i>MQ</i>	<i>F</i>	<i>F de significação</i>
Regressão	3	4,76E+12	1,59E+12	75,8863	0,08413
Resíduo	1	2,09E+10	2,09E+10		
Total	4	4,78E+12			

	<i>Coefficientes</i>	<i>Erro padrão</i>	<i>Stat t</i>	<i>valor-P</i>	<i>95% inferiores</i>	<i>95% superiores</i>	<i>Inferior 95,0%</i>	<i>Superior 95,0%</i>
Interseção	404272,10	177465,87	2,28	0,26	-1850645,6	2659189,79	-1850645,6	2659189,79
Não_servidores Indiciados	-356225,34	39017,57	-9,13	0,07	-851990,60	139539,92	-851990,60	139539,92
Servidores Indiciados	922953,51	79163,93	11,66	0,05	-82919,63	1928826,64	-82919,63	1928826,64
NBs fraudados	22806,54	1557,93	14,64	0,04	3011,19	42601,90	3011,19	42601,90

Fonte: autoria própria