12607051 08027.000761/2020-27

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
GABINETE DO MINISTRO

OFÍCIO Nº 2117/2020/AFEPAR/MJ

Brasília, 14 de setembro de 2020.

A Sua Excelência a Senhora
Deputada Federal SORAYA SANTOS
Primeira Secretária
Câmara dos Deputados
70160-900 - Brasília - DF

Assunto: **Requerimento de Informação Parlamentar (RIC) nº 869/2020, de autoria do Deputado Federal Capitão Alberto Neto - REPUBLIC/AM.**

Referência: **Ofício 1aSec/RI/E/nº 1388**

Senhora Primeira Secretária,

1. Com meus cordiais cumprimentos, reporto-me ao Requerimento de Informação Parlamentar (RIC) nº 869/2020, de autoria do Deputado Federal Capitão Alberto Neto (REPUBLIC/AM) para encaminhar a Vossa Excelência informações *"sobre fraudes realizadas em ambientes virtuais"*, nos termos da documentação anexa.

Atenciosamente,

(documento assinado eletronicamente)

ANDRÉ LUIZ DE ALMEIDA MENDONÇA
Ministro de Estado da Justiça e Segurança Pública

ANEXOS

1. OFÍCIO Nº 877/2020/SEAPRO/GAB/PF (12444902);
2. Relatório - Crimes Cibernéticos (12444864).

Esplanada dos Ministérios, Bloco T, Ed. Sede, 4º Andar, Sala 408 - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-9001 Site: - www.justica.gov.br

Ministério da Justiça e Segurança Pública
Polícia Federal

OFÍCIO Nº 877/2020/SEAPRO/GAB/PF

Brasília, 19 de agosto de 2020.

Ao Senhor
LUCAS ALVES DE LIMA BARROS DE GÓES
Chefe da Assessoria Especial de Assuntos Federativos e Parlamentares
Ministério da Justiça e Segurança Pública
Brasília - DF

Assunto: **Requerimento de Informação Parlamentar (RIC) nº 869/2020, de autoria do Deputado Federal Capitão Alberto Neto - REPUBLIC/AM.**□
Referência: Ofício nº 1904/2020/AFEPAR/MJ

Senhor Chefe,

Em atenção ao documento em referência, encaminho o Despacho SIC/DOV/GAB/PF15754122 e o Relatório - Crimes Cibernéticos (15733447), aprovados pelo Diretor-Geral, contendo as informações quanto ao assunto.

Atenciosamente,

MILTON RODRIGUES NEVES
Delegado de Polícia Federal
Chefe de Gabinete da Direção-Geral

Documento assinado eletronicamente por **MILTON RODRIGUES NEVES**, **Chefe de Gabinete**, em 20/08/2020, às 16:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15766107** e o código CRC **E895534A**.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

POLÍCIA FEDERAL

RELATÓRIO
CRIMES CIBERNÉTICOS
(FRAUDES BANCÁRIAS ELETRÔNICAS)

Autor: **Erik Pereira de Siqueira / Agente de Polícia Federal**

Divisão de Repressão aos Crimes Cibernéticos – DRCC/CGPFAZ

Sumário

1- INTRODUÇÃO

Durante a crise sanitária provocada pelo Covid-19, a Polícia Federal detectou um aumento significativo de ameaças cibernéticas, principalmente relacionadas às fraudes bancárias eletrônicas e com foco ao Auxílio Financeiro do Governo Federal.

Esta ajuda financeira tem sido objeto de interesse e ataques por parte de organizações criminosas tradicionais.

Ainda, os crimes cibernéticos (especialmente as fraudes bancárias eletrônicas) passaram a ser utilizadas, de forma global, como financiadoras de outras condutas criminosas, cibernéticas ou não.

Atualmente há um forte componente cibernético utilizado para o cometimento das mais variadas condutas criminosas, esse componente sendo utilizado muitas vezes como suporte financeiro e/ou material pela criminalidade organizada.

Com a evolução dos ataques cibernéticos criou-se também a necessidade de desenvolvimento de novas técnicas investigativas por parte da Polícia Federal, como o Projeto Tentáculos e mais recentemente a Base Nacional de Fraudes no Auxílio Emergencial, além da necessidade ímpar do trabalho em parceria com a iniciativa privada.

Neste contexto, esse relatório irá abordar, de forma resumida, o contexto geral dos crimes cibernéticos (especificamente as fraudes bancárias eletrônicas) e a forma de atuação da Polícia Federal na repressão a esses crimes.

2- CENÁRIO GLOBAL E BRASILEIRO DAS AMEAÇAS CIBERNÉTICAS

A crescente dependência da internet nos modelos de negócios privados e governamentais tornou a economia mundial mais vulnerável aos ataques cibernéticos. **Estimam-se, por ano, perdas globais de US$ 600.000.000.000,00 (seiscentos bilhões de dólares)**[1].

Nesse sentido, o risco cibernético passou a ser item relevante nos mais diversos índices de apuração e projeção da atividade econômica global. O **Relatório de 2019 do Fundo Monetário Internacional (FMI) destaca os riscos cibernéticos ao lado de fatores como as mudanças climáticas, incertezas políticas e perda da credibilidade das instituições**[2], dentre aqueles que podem afetar o cenário econômico no médio prazo.

> Over the medium term, many Directors noted risks from rising inequality, climate change, cyber risks, political uncertainty, and declining trust in institutions.

Fonte: https://www.imf.org/en/Publications/WEO/Issues/2019/03/28/world-economic-outlook-april-2019

Ainda no cenário internacional, **o relatório INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018** - EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, EUROPOL - **cita a falta de legislação adequada aos crimes cibernéticos como um dos fatores do Brasil ser o líder de fontes de ataques cibernéticos na América Latina**.

Além disso, o relatório IOCTA 2018, informa que 54 % dos ataques cibernéticos reportados no Brasil tem origem interna. Similarmente aos EUA, o Brasil também está no topo dos países que hospedam *phishing*, colocando o Brasil entre os dez maiores países originários de ataques cibernéticos.

Destaca-se que recentemente o Governo Federal publicou o DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 **no qual aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber).**

---

1 THE COST OF CYBERCRIME. INTERNET SOCIETY. Fonte: https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime

2 The following remarks were made by the Chair at the conclusion of the Executive Board's discussion of the Fiscal Monitor, Global Financial Stability Report, and World Economic Outlook on March 21, 2019. Fonte: https://www.imf.org/en/Publications/WEO/Issues/2019/03/28/world-economic-outlook-april-2019

A E-Ciber é a *orientação manifesta do Governo Federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.*

Destaca-se **também alguns dados do diagnóstico do risco cibernético para a economia brasileira publicada na E-CIBER**[3]:

> *O risco para a economia brasileira, gerado pela intrusão em computadores e pela disseminação de códigos maliciosos praticados pelo crime organizado já é uma realidade, conforme se vê pelos dados a seguir, referentes à conectividade do Governo, do setor privado e dos cidadãos, aos índices globais e aos crimes cibernéticos:*
>
> *- O Brasil ocupa o 66º lugar no **ranking** da Organização das Nações Unidas - ONU de tecnologia da informação e comunicação;*
>
> *- Apenas 11% dos órgãos federais têm bom nível em governança de TI;*
>
> *- O Brasil ocupa o 70º lugar no **Global Security Index**, da UIT;*
>
> *- 74,9% dos domicílios (116 milhões de pessoas) com acesso à internet;*
>
> *- 98% das empresas utilizam a internet;*
>
> *- 100% dos órgãos federais e estaduais utilizam a internet;*
>
> *- Em 2018, 89% dos executivos foram vítimas de fraudes cibernéticas;*
>
> *- As questões de segurança desestimulam o comércio eletrônico;*
>
> *- O Brasil é o 2º com maior prejuízo com ataques cibernéticos.*

Ainda no cenário nacional, os números das ameaças são alarmantes como pode ser verificado **no Relatório de Ameaças à Segurança na Internet 2018 para o Brasil,** alguns dados relevantes:

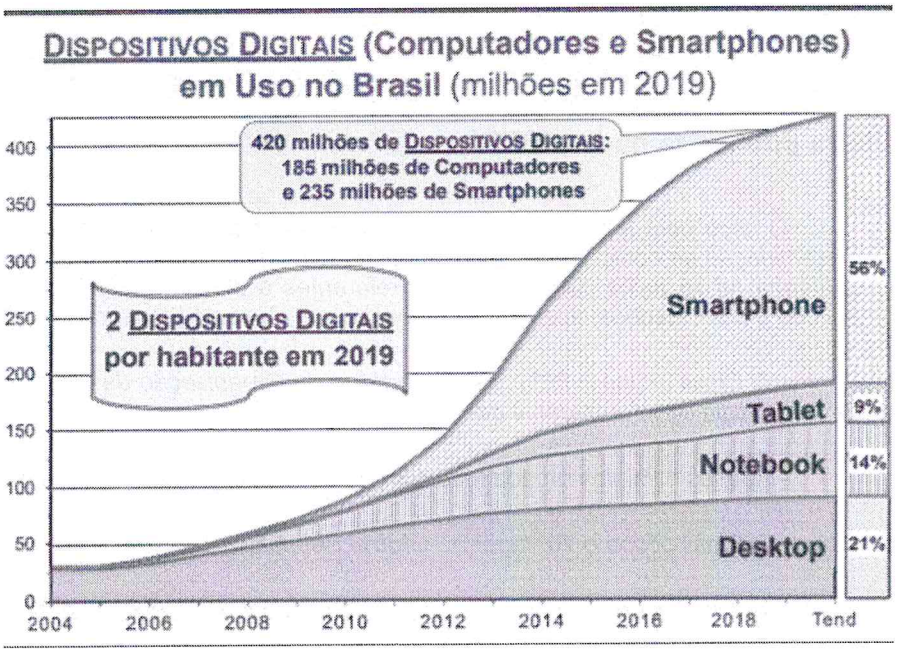
- *62 milhões de brasileiros foram vítimas de crime cibernético;*
- *45% dos adultos no país tiveram uma experiência de crime virtual e comportamento de risco nos últimos 12 meses;*
- *Custo líquido do crime cibernético, nos últimos 12 meses, foi superior a R$ 22 bilhões;*

Esse aumento substancial no número de crimes cibernéticos foi fortemente impulsionado pelo crescimento do uso da TI no Brasil (FGV, 2019). **A pesquisa registra o**

---

[3] Decreto 10.222/2020: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

impressionante número de mais de 420 milhões de dispositivos digitais em uso no Brasil - computadores e smartphones (2 dispositivos digitais por habitante) .



Fonte: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2019fgvciappt_2019.pdf

Além disso, **os crimes cibernéticos são cometidos sem o uso da violência.** Esta característica, durante anos, acabou deixando em segundo plano o combate a esse tipo de crime e **afetou até mesmo a construção de um arcabouço legal mais adequado.**

> **"Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Fonte: Artigo 154 do Código Penal Brasileiro

Houve também uma associação/definição, de certo modo equivocada, dos crimes cibernéticos como crimes "virtuais", acabando por se criar uma visão distorcida e minimizada do potencial lesivo e dano dos criminosos cibernéticos à sociedade, como se os crimes não fossem reais.

Soma-se a isso, as dificuldades investigativas inerentes a própria estrutura e funcionamento da internet, ou seja, um crime sem fronteiras com forte atuação transnacional,

no qual o atacante e/ou infraestrutura computacional está quase sempre bem distante da vítima.

Ainda em relação ao cenário interno, a tendência do mercado clandestino dos crimes cibernéticos no Brasil segue a tendência do cenário mundial, ou seja, tem caminhado para uma maior especialização de funções, onde são oferecidos, pelos criminosos, serviços sob demanda, de acordo com a necessidade do contratante.

Esta tendência detectada no Brasil adota um modelo conhecido como *Cybercrime-as-a-Service* (SAMANI & FRANÇOIS, 2013), ou seja, um modelo de negócios fraudulentos que muito se compara aos modelos legais de negócios corporativos: Criminosos cibernéticos utilizam esquemas similares ao legítimo modelo B2B (*business to business*) para a realização de suas operações tais como o altamente sofisticado modelo *Criminal-to-criminal* (C2C).

Resumidamente, no modelo C2C *(Criminal to Criminal)*, há uma verdadeira terceirização de cada função, os serviços técnicos são oferecidos conforme o grau de especialização de cada um: vulnerabilidades *zero day*[4] em *softwares*, *exploits*, *ransomwares*, *spam*, *malware*, *botnets*, hospedagem, serviços *DDoS* e outros.

Esta abordagem conhecida como *as-a-Service* (como um serviço) onde há a oferta, no mercado clandestino, de vários serviços: *Malware-as-a-Service*[5], *Exploit-as-a-Service*[6], *DDoS-as-a-Service, Hacking-as-a-Service* dentre outros, onde o mais importante é obter lucro de acordo com a especialidade do desenvolvedor e serviço criminoso prestado.

Há assim um mercado criminoso organizado com a oferta de dados, informações, serviços, plataformas e artefatos maliciosos.

---

[4] São vulnerabilidades ainda desconhecidas ou que ainda não tenham uma correção disponibilizada pelo desenvolvedor da aplicação ou sistema, mas que já são do conhecimento e explorada por atacantes da aplicação ou sistema.

[5] Serviço de criação de *Malwares* Personalizados.

[6] Manufacturing Compromise: The Emergence of Exploit-as-a-Service (GRIER et al, 2012).

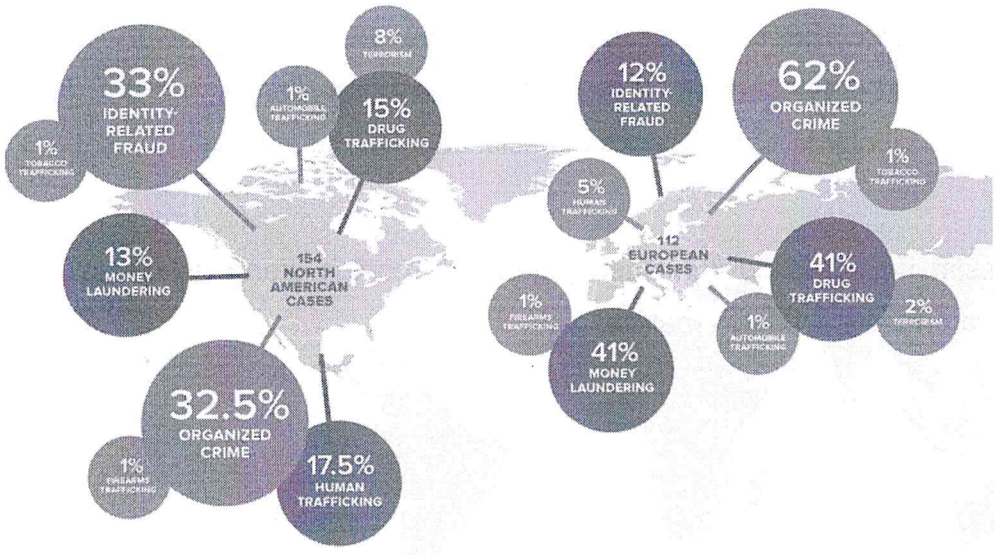
3 – CRIMES CIBERNÉTICOS: A NOVA FORMA DE FINANCIAMENTO DE ORGANIZAÇÕES CRIMINOSAS TRADICIONAIS

É importante destacar que os crimes cibernéticos (especialmente as fraudes bancárias eletrônicas) passaram a ser utilizadas, de forma global, como financiadoras de outras condutas criminosas, cibernéticas ou não.

"*Precisamos entender o verdadeiro impacto das fraudes – não apenas os custos financeiros, mas também os custos para a Segurança Pública e a Segurança Nacional*"[7].

A linha que separa os crimes cibernéticos das atividades criminosas tradicionais desapareceu completamente.

Atualmente há um forte componente cibernético utilizado para o cometimento das mais variadas condutas criminosas, esse componente sendo utilizado muitas vezes como suporte financeiro e/ou material pela criminalidade organizada, conforme dados de recente pesquisa que analisou casos investigados na América do Norte e Europa (TERBIUM LABS RESEARCH) que envolvem fraudes com o uso de dados de pagamentos em meios eletrônicos.



Fonte: WHERE AND HOW IS STOLEN PAYMENT DATA USED IN TRANSNATIONAL CRIME ACROSS THE WORLD? - Vínculos entre as fraudes em meios de pagamento e crimes transnacionais.

7 https://terbiumlabs.com/2019/06/24/new-research-terbium-labs-uncovers-pervasive-links-between-fraud-and-transnational-crime/

3.1– A importância do combate às fraudes bancárias eletrônicas

Dentro do cenário dos Crimes Cibernéticos, as fraudes bancárias via internet representam o crime cibernético clássico e são cometidas sem o uso da violência. Esta característica acabou colocando em segundo plano, durante anos, o combate a esse tipo de crime.

Para se ter uma ideia da importância do combate às fraudes bancárias eletrônicas, no assalto ao Banco Central (maior assalto a banco no Brasil), em agosto de 2005, os criminosos furtaram um montante de R$ 150 milhões.

O ESTADO DE S. PAULO

TERÇA-FEIRA

R$ 150 milhões, o maior assalto a banco no Brasil

Ladrões abriram túnel de 78 metros até o cofre do Banco Central em Fortaleza

Figura: Fonte: acervo.estadao.com.br

De forma silenciosa e sem violência (quase invisível), o montante fraudado em fraude eletrônica no Brasil em 2019 somou o expressivo montante de aproximadamente R$ 4 bilhões, ou seja, o montante é equivalente a mais de 25 assaltos ao Banco Central por ano ou um assalto ao Banco Central aproximadamente a cada 15 dias!

Nesse cenário, nas mais diversas operações policiais desencadeadas pela Polícia **Federal foram encontradas evidências inequívocas de que as fraudes bancárias eletrônicas atualmente são financiadoras de diversas outras condutas criminosas**, cibernéticas ou não, dentre as quais pode-se destacar:

- **Infração à ordem econômica:** diversas investigações detectaram que serviços fraudulentos especializados de quitação de dívidas são frequentemente contratados por empresas a fim de obter vantagem competitiva no mercado e/ou prejudicar a livre concorrência. As dívidas de impostos e a compra de bens de consumo das mais diversas empresas são pagas em contas vítimas de fraude pela internet, gerando um desequilíbrio nas relações de concorrência.

São casos nem sempre fáceis de enquadrar no ordenamento jurídico[8], mas que são condutas que podem se encaixar ao crime contra a economia popular[9].

- **Financiamento de agentes políticos:** As fraudes com cartões de crédito pela internet têm sido utilizadas como suporte ao financiamento de campanhas eleitorais aos mais diversos cargos eletivos, conforme já detectado em investigações internas da Divisão de Repressão aos Crimes Cibernéticos da Polícia Federal:

> Para o cadastramento do EC ZP [redacted] junto à ZOOP TECNOLOGIA E MEIOS DE PAGAMENTO S.A. foi fornecido também o CPF [redacted], de [redacted], com endereço em [redacted]
>
> [redacted] foi candidata a Deputada Estadual em 2018 pelo [redacted], partido pelo qual consta como responsável em sua cidade.

Fonte: Trecho retirado de Relatório Interno do DRCC/CGPFAZ (EC- Estabelecimento Comercial utilizado para recepcionar transações fraudulentas com cartões de crédito pela internet em nome de candidata a Deputada Estadual em 2018).

- **Lavagem de dinheiro e financiamento ao Terrorismo**[10]: Os cibercriminosos especialistas em fraudes bancárias pela *internet* chegam também a oferecer complexas redes para ocultação de ativos, seja por meio de cartões pré-pagos nacionais e internacionais, **contas bancárias de laranjas ou mecanismos extremamente bem elaborados que utilizam criptomoedas (*bitcoin* por exemplo) e cartões pré-pagos.** Nesse sentido, a União

[8] https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet

[9] https://ww2.stj.jus.br/processo/revista/documento/mediado/?compontente=ITA&sequencial=1459186&num_registro=201400940269&data=20151106&formato=PDF

[10] https://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH <acesso em 14/11/2018>

Européia[11] aprovou recente recomendação do fortalecimento da legislação dos Estados-Membros quanto ao uso de cartões pré-pagos e criptomoedas como medida preventiva à lavagem de dinheiro e terrorismo.

RISK MANAGEMENT / FIGHTING FRAUD 2018

How fraud is funding terrorism

In his evidence before the Treasury select committee of MPs, Donald Toon from the National Crime Agency, said: "It would be realistic to say that hundreds of billions are laundered through the UK annually"

Fonte: https://www.raconteur.net/risk-management/fraud-funding-terrorism

Importante destacar também a ocultação/dissimulação da origem de bens/valores por parte das quadrilhas especializadas nos crimes cibernéticos, utilizando-se, principalmente, de negócios de fachada para justificar o alto padrão social.

- **Tráfico Internacional de Drogas:** recentes investigações da DRCC/CGPFAZ identificaram inúmeras compras de passagens aéreas internacionais pela internet, com o uso de cartões de crédito fraudados.

Os bilhetes de passagem são comprados em datas próximas ao embarque, para destinos na Europa, partindo do Brasil com escala em países como a Colômbia, num claro movimento da utilização pelos traficantes internacionais dos serviços fraudulentos *online*, maximizando as vantagens financeiras oriundas do tráfico de drogas, dificultando o rastreamento da origem e reduzindo os custos operacionais das passagens aéreas para os tradicionais "mulas".

- Outras condutas: diversas outras condutas criminosas já foram detectadas como diretamente associadas ao financiamento realizado pelas fraudes bancárias eletrônicas: **compra ilegal de armas, tráfico de drogas**, **pornografia infantil,** (diversos *marketplaces* na *darkweb* tem sua infraestrutura computacional totalmente financiada por meio de fraudes bancárias eletrônicas), **espionagem industrial, invasão de dispositivos computacionais e**

[11] https://finance.yahoo.com/news/european-union-votes-closer-regulation-181146774.html <acesso em 20/11/2018>

base de dados governamentais, pirataria de audiovisual, aprovação em concursos públicos, dentre outras.

Operação Singular

PF derruba organização que cobrava para 'aprovar' candidatos a exame da OAB

A Polícia Federal (PF) em São Paulo deflagrou na manhã desta terça-feira, 4, a Operação Singular, para desarticular uma organização que praticava crimes cibernéticos. Os federais descobriram que um dos líderes do grupo invadiu o sistema de uma empresa responsável pela realização de concursos e cobrou valores em criptomoedas para "aprovar" candidatos que alcançassem a [...]

04/06/2019 13:43

Operação Singular da PF mira em roubo de dados de cartões de crédito

A Polícia Federal (PF) deflagrou na manhã desta terça-feira, 4, a Operação Singular, para desarticular uma organização que praticava crimes cibernéticos, principalmente fraudes bancárias eletrônicas, roubando e revendendo dados de cartões de crédito. Agentes cumpriram cinco mandados de busca e apreensão e cinco de prisão preventiva nos Estados de São Paulo, Rio Grande do Sul [...]

04/06/2019 10:12

Fonte:https://odia.ig.com.br/brasil/2019/06/5649557-pf-derruba-organizacao-que-cobrava-para--aprovar--candidatos-a-exame-da-oab.html

4 POLÍCIA FEDERAL E OS ACORDOS DE COOPERAÇÃO TÉCNICA NO COMBATE AOS CRIMES CIBERNÉTICOS

Idealizado no ano de 2007 e implementado em virtude da assinatura do termo de Cooperação Técnica com a CAIXA em 2008, o projeto TENTÁCULOS **centraliza todas as notícias-crime de fraudes recebidas diretamente do órgão central da CAIXA (CESEG), em um repositório único de dados, a denominada Base Nacional de Fraudes Bancárias e Eletrônicas (BNFBE).**

De forma simplificada, a BNFBE organiza as fraudes em um banco de dados para a verificação de pontos em comum e assim diminuir o número de procedimentos investigatórios (evita o modelo de uma fraude = um Inquérito Policial), impedindo também o retrabalho e otimizando os recursos materiais e humanos nas investigações.

A Figura 1 demonstra os tipos de vínculos e correlacionamentos criados a partir da BNFBE onde, ao final, sugere a instauração de apenas um procedimento investigativo para todas as fraudes relacionadas.

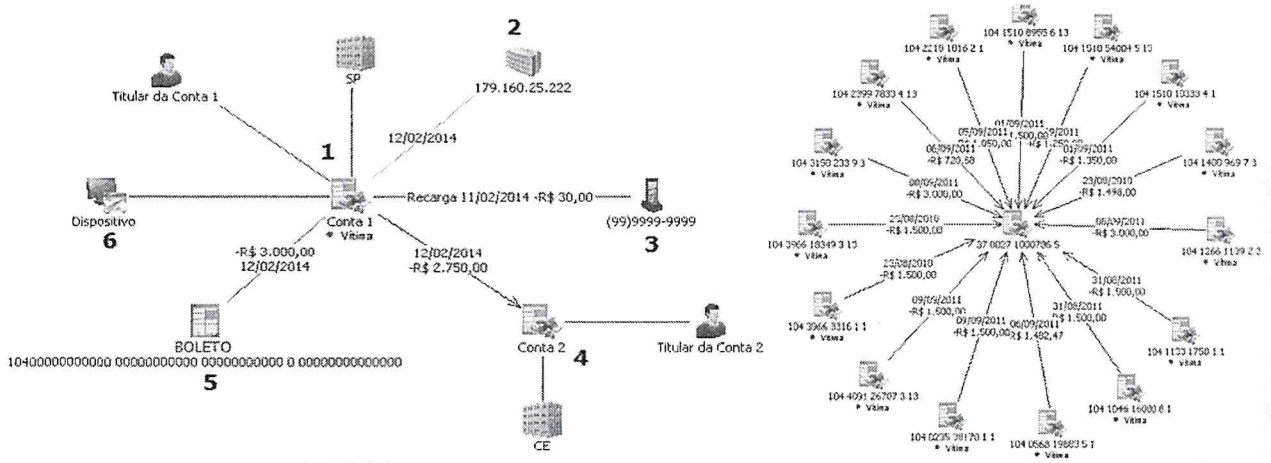


Figura 1: Entidades e Relacionamentos – Fonte: BNFBE.

Com a nova abordagem do Projeto Tentáculos a Polícia Federal deixou de instaurar mais de 790.793 inquéritos policiais desde o ano de 2009.

4.1 Acordo de Cooperação Técnica PF X FEBRABAN

Uma das consequências imediatas do sucesso da parceria PF X CAIXA (Projeto Tentáculos), foi a manifestação do interesse demonstrado pela FEBRABAN (Federação Brasileira de Bancos) em fazer parte do projeto.

Apesar de não ser uma atribuição constitucional da Polícia Federal a fraude cometida em desfavor de bancos privados, a experiência das operações desencadeadas frequentemente demonstrou que, nos casos de fraudes no canal internet banking, um único fraudador ataca os mais diversos bancos com atuação em âmbito interestadual.

Surgiu assim, em tempos de vertiginoso crescimento das ameaças pela internet, a necessidade de se trabalhar em uma ampla parceria, PF X CAIXA e as demais instituições bancárias.

Assim, em Setembro de 2017**, o Exmo Diretor-Geral da Polícia Federal, assinou o Acordo de Cooperação Técnica (ACT) PF X FEBRABAN**, ampliando a capacidade investigativa da Polícia Federal, e proporcionando um aperfeiçoamento constante do modelo.

Desta forma a Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE) passou a contar com dados das fraudes comunicadas pelos bancos aderentes ao ACT, atualmente num total de 22 (vinte e duas) instituições bancárias, potencializando o alcance das investigações relacionadas ás fraudes bancárias eletrônicas.

Bancos Aderentes ao ACT PF X FEBRABAN (TOTAL 22 BANCOS):

Caixa
Bradesco
Banco do Brasil
Inter
Itaú Unibanco
Santander
Agiplan
Banco do Estado de Sergipe S.A
Banrisul
Banco da Amazônia S.A.
Banco de Brasília
Banco Neon S.A.
Banco Cooperativo Sicredi S.A
Banco Original
Banco BS2
Banco BMG
PAN
Sicoob
Carrefour
Votorantim
Banco do Nordeste
Banco do Pará

22 Instituições bancárias aderentes ao ACT PF X FEBRABAN.

Atualmente a BNFBE possui mais de 1.000.000 (hum milhão) de registros de ocorrências de fraude dos mais diversos bancos.

5 OPERAÇÕES POLICIAIS

Em relação às operações referentes às fraudes bancárias eletrônicas, dentro do escopo do Acordo de Cooperação Técnica PF X CAIXA e PF e FEBRABAN, a Polícia Federal deflagrou as seguintes operações classificadas como especiais (de 2015 a 2019) com os números de mandados cumpridos:

Operação	MBA	MPP	MPT
LAMMER	14	9	0
OPERAÇÃO VALENTINA	25	7	6
PATROCÍNIO	13	0	0
DARKODE	4	2	0
PECADO ORIGINAL	8	0	0
SHEIK - FASE II	3	5	0
DARKODE 2	18	6	15
O GRANDE IRMÃO	11	0	9
SAFETY MODE	1	0	0
GATEWAY	5	0	0
VIGILANCIA DIGITAL	7	0	0
STALKER	10	0	3
BR 153	12	2	0
CARTÃO VERMELHO	6	1	0
CARTÃO VERMELHO II	1	1	0
PESCARIA	0	0	0
TENTÀCULOS INGLESES	3	2	2
CTRL C	21	0	17
CAPTURA	22	18	3
FRAUDE POSTAL II	5	0	4
CHARGEBACK	12	12	0
SPURIUS 2	20	12	6
SPURIUS 3	15	0	0
CÓDIGO REVERSO	23	7	3
BACKDOOR	16	6	0
CRÉDITO FÁCIL	7	0	0
DR. CROSS	11	11	0
ALMAS PERDIDAS	4	0	0
CRACKER	12	3	0
CÂMERA 1	3	2	0
AMERICAN DREAM 2	5	0	0
DEEP DOT DOWN	1	0	0
CÂMERA 1	3	2	0
OPERAÇO LAS VEGAS	20	7	1
OPERAÇÃO SINGULAR	10	5	1
TOTAL	351	120	70

Legenda: MBA (Mandado de Busca e Apreensão), MPP (Mandado de Prisão Preventiva) , MPT (Mandado de Prisão Temporária)

É importante destacar que, além das operações classificadas como Especiais, nos últimos anos foram produzidos 620 Relatórios de Análises de Fraudes Bancárias, que dão causa à instauração dos respectivos Inquéritos Policiais nas Superintendências Regionais e nas delegacias descentralizadas, produzidos diretamente dos dados extraídos da Base Nacional de Fraudes Bancárias Eletrônicas, resultando em investigações de ocorrências de fraudes bancárias eletrônicas que resultaram em prejuízo de mais de R$ 300 milhões de reais.

Os relatórios fazem parte do modelo investigativo criado por meio do Projeto Tentáculos da Polícia Federal.

6 A BASE NACIONAL DE FRAUDES NO AUXÍLIO EMERGENCIAL

Considerando que o artigo 2º da Lei nº 13.982/2020 criou o auxílio emergencial como medida excepcional de proteção social para o período da pandemia de Covid-19, na área repressiva, visando a necessidade de otimização das investigações e centralização das informações referente às ocorrências de fraude, a Polícia Federal implementou a denominada Base Nacional de Fraudes no Auxílio Emergencial (BNFAE).

A BNFAE faz parte da Estratégia Integrada contra a Fraude ao Auxílio Emergencial da Polícia Federal com o Ministério Público Federal e demais órgãos governamentais participantes.

De forma simplificada, a BNFAE utiliza a mesma metodologia de investigação baseada no Projeto Tentáculos onde organiza as fraudes em um banco de dados para a verificação de pontos em comum e assim diminuir o número de procedimentos investigatórios (evita o modelo de uma fraude = um Inquérito Policial), impedindo também o retrabalho e otimizando os recursos materiais e humanos nas investigações. O foco é o combate à criminalidade organizada.

Dessa forma, buscou-se centralizar em um banco de dados, todas as informações relacionadas aos processos de contestação resultantes da análise e da confirmação, por parte da CAIXA, das comunicações de irregularidades envolvendo o recebimento do benefício do Auxílio Emergencial.

Assim, com base nos dados de contestação encaminhados pela CAIXA à Polícia Federal, bem como as informações complementares obtidas junto aos outros atores (instituições financeiras, provedores de internet etc), busca-se a produção de investigações com base nas correlações encontradas entre as fraudes, conforme exemplo gráfico abaixo:

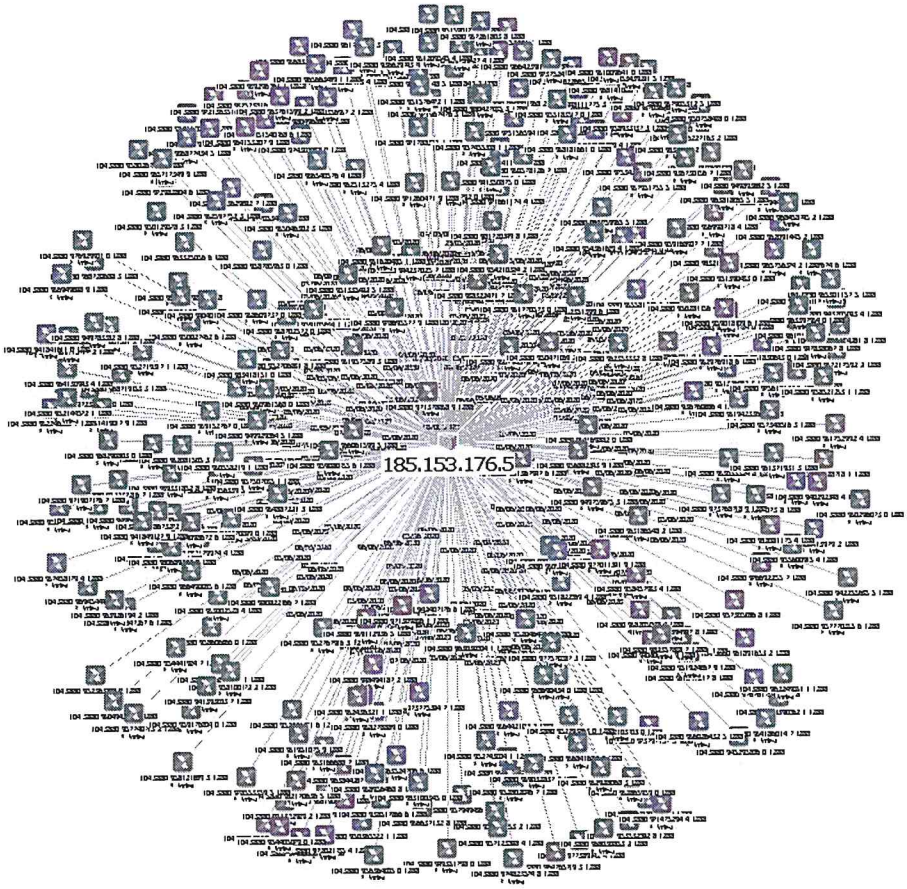


Gráfico extraído da BNFAE no qual demonstra o acesso pelo mesmo IP a 292 contas bancárias fraudadas no Auxílio Emergencial.

7 CONCLUSÃO.

Os crimes cibernéticos têm aumentado numa escala global por meio de elaborados esquemas criminosos e como financiadores de organizações criminosas tradicionais nos mais diversos países.

O atual arcabouço legal de combate aos crimes cibernéticos, notadamente em relação às fraudes bancárias eletrônicas, infelizmente tem estimulado o aumento e migração para esta prática criminosa no Brasil.

A Polícia Federal por meio dos Acordos de Cooperação com as instituições bancárias, além de propor uma quebra de paradigma no combate ao crime e conforme demonstrado, reduziu fortemente o número de inquéritos policiais instaurados nos últimos anos, ampliando a capacidade investigativa, mapeando os grandes grupos criminosos e selecionando o melhor local para a atuação policial, com reflexos diretos nos outros atores da persecução penal (Ministério Público e Justiça Federal).

Além disso, as mais diversas operações desencadeadas pela Polícia Federal nos últimos anos, demonstram o alcance ilimitado e o enorme potencial lesivo das fraudes bancárias eletrônicas para a sociedade e de como tradicionais organizações criminosas tem utilizado essa conduta criminosa como suporte financeiro e material para cometimento dos mais diversos crimes.

Por fim, conforme demonstrado neste relatório, principalmente durante o período da pandemia do covid-19, houve aumento considerável dos crimes cibernéticos tornando-se um atual problema de segurança pública e demonstrando a necessidade de cooperação e coordenação Policial interestadual e transnacional no sentido de reprimir as ações das organizações criminosas.