FRAUDES COMETIDAS NA INTERNET – USO DE FONTES ABERTAS NA INVESTIGAÇÃO POLICIAL E NA INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Alesandro Gonçalves Barreto[1]

RESUMO

Os criminosos têm se valido dos avanços tecnológicos para potencializar suas ações, especialmente no que diz respeito às fraudes cometidas em ambiente virtual. Muito embora, exista legislação determinando aos entes federativos a estruturação de setores ou delegacias especializadas na repressão dos crimes de *Internet*, o que vemos, ainda são estruturas deficientes na investigação criminal dessas infrações. É nesse contexto que surge a utilização de fontes abertas para obtenção de informações atualizadas sobre as fraudes praticadas. Por fim, as informações livremente disponíveis na *Internet* podem auxiliar na tarefa de investigar crimes cibernéticos.

Palavras-chave*:* Crime;Fontes Abertas;Fraudes; Eletrônica.

INTRODUÇÃO

A *Internet* tem se tornado um terreno fácil para a prática dos mais diversos crimes. A cada dia surgem novos golpes, dificultando, de sobremaneira, a atuação da polícia judiciária. Quando tomam conhecimento de determinada prática, vários usuários desavisados tornam-se vítimas, com valores ou informações pessoais subtraídos.

A investigação de delitos contra o patrimônio cometidos na *Internet* necessita, pois, de especialização da polícia judiciária. É nesse contexto que foi sancionada a Lei Azeredo[i], determinando aos órgãos de polícia judiciária a estruturação de "setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado".

Desde o sancionamento da lei em questão, transcorreram-se 05 (cinco) anos sem nenhum avanço significativo na criação de delegacias especializadas na repressão dos crimes

1 Delegado de Polícia Civil do Estado do Piauí e coautor dos livros Investigação Digital em Fontes Abertas e Manual de Investigação Cibernética à Luz do Marco Civil da *Internet*, ambos da Editora Brasport. Coordenador do Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos nos Jogos Olímpicos e Paralímpicos Rio 2016. Colaborador Eventual da Secretaria Nacional de Segurança Pública. delbarreto@gmail.com.

cibernéticos. Muito embora alguns Estados tenham avançado, criando centros de excelência na investigação dos delitos informáticos, alguns ainda deixam a desejar nessa seara, resultando, assim, num atendimento inadequado às vítimas e na impunidade dos infratores.

Sem embargo, não nos cabe apenas esperar pela criação de estruturas de repressão, mas também, engendrar mecanismos e utilizar de fontes para tomar conhecimento dos golpes cometidos por meio da *Internet*, tão logo eles ocorram.

1. USO DE FONTES ABERTAS PARA ACOMPANHAMENTO DE FRAUDES ONLINE.

A investigação policial deve se adequar à nova realidade dos avanços tecnológicos. Um dos caminhos para isso é a utilização de informações disponíveis em fontes abertas.

BARRETO, CASELLI e WENDT[ii] ressaltam a importância da coleta em fonte aberta tanto para a atividade de inteligência quanto para a investigação policial ao definir como:

> Qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).

Não há como desprezar essas informações disponíveis para agregar valor à investigação de fraudes cometidas via *Internet*. É nesse contexto que se insere o Catálogo de Fraudes da RNP –Rede Nacional de Ensino e Pesquisa[iii]. Através do CAIS – Centro de Atendimento a Incidentes de Segurança – disponibiliza, desde o ano de 2008, informações sobre os principais golpes praticados na rede mundial de computadores.

A consulta às fraudes praticadas deve ser feita no link https://www.rnp.br/servicos/seguranca/catalogo-fraudes, podendo ser encontradas informações sobre *phishingscam*[iv] ou *malwares*[v] disseminados através de *scam*[vi]. As fraudes são catalogadas a partir de sua detecção, com dados atinentes às imagens, data, assunto, tipo de arquivo malicioso e *modus operandi*.

À vista disso, o investigador deve utilizar o supracitado serviço fornecido como ferramenta para acompanhamento dos golpes online, seja para consulta no momento da lavratura do boletim de ocorrência, seja para agregar *expertise* na sua atividade investigativa.

Ressalte-se, todavia, que esses dados obtidos em fontes abertas devem ser confrontados com outras fontes de consulta para agregar valor na produção de provas ou de conhecimento de inteligência de segurança pública. Ademais, o catálogo de fraudes pode ser acessado por qualquer usuário antes de realizar qualquer compra na *Internet*.

Acrescente-se ainda, a existência de outras ferramentas de busca que podem ser utilizadas para obter informações de fraudes online, a exemplo da opção de criar alertas de palavras-chave, recebendo a notificação por *e-mail* quando aquele assunto é indexado pela *Internet*. Nesse caso, facilita-se, de sobremodo, a atividade policial, eis que as informações sobre fraudes serão encaminhadas rotineiramente para o investigador policial. Os principais serviços de alertas disponíveis são Google *Alerts*, Talkwalker *Alerts* e Bing *Alerts*.

CONSIDERAÇÕES FINAIS

A atividade investigativa e/ou produção de conhecimentos na inteligência de segurança pública não podem desprezar os dados de livre acesso em razão dos avanços tecnológicos. Nesse contexto, inserem-se as fontes abertas como mecanismos para agregar valor na produção de conhecimento e/ou elementos informativos.

Os dados fornecidos pela plataforma da RNP são de extrema importância na obtenção de conteúdo relacionado ao cometimento de fraudes eletrônicas na rede mundial de computadores. Os criminosos aproveitam-se dessa interconectividade e do alcance da *Internet* para aperfeiçoar suas ações. Portanto, para que a atividade investigativa acompanhe o "*modus operandi*" dos criminosos, não deve, de maneira nenhuma, abrir mão de recursos disponíveis como os citados.

Por fim, a investigação policial ou a atividade de inteligência não devem ficar adstritas ao secreto ou dado negado. De quando em vez, o conteúdo disponível poderá apontar um melhor caminho na obtenção do dado ou elemento informativo.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. BRASIL,Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da *Internet*. BRASPORT Editora. Rio de Janeiro. 2016.

BARRETO, Alesandro Gonçalves; WENDT, Emerson. CASELLI, Guilherme. Investigação Digital em Fontes Abertas. BRASPORT Editora. Rio de Janeiro. 2017.

BARRETO, Alesandro Gonçalves. Utilização de fontes abertas na investigação policial. **Direito e TI**, Porto Alegre, nov. 2015. Disponível em: <http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>. Acesso em: 01 mar. 2017.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 01. mar. 2017.

_____. Lei 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 01. mar. 2017.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01. mar. 2017.

[i] Lei Nº 12.735/2012. Em seu art. 4º determina: "Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado".
[ii] BARRETO, Alessandro Gonçalves; CASELLI, Guilherme; WENDT, Emerson. Investigação Digital em Fontes Abertas. Rio de Janeiro: Brasport, 2017.
[iii] A Rede Nacional de Ensino e Pesquisa (RNP) provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa.
[iv] Fraude aplicada, utilizando engenharia social ou de outros artifícios para obtenção de dados pessoais e financeiros das vítimas.
[v] Softwares que executam atividades maliciosas dentro de um dispositivo informático.
[vi] Ação enganosa ou fraudulenta que têm como objetivo a obtenção de vantagem financeira.