ISSN 2447-1097

Direito & TI–Porto Alegre / RS www.direitoeti.com.br

BUSCA DE ELEMENTOS INFORMATIVOS DE CRIMES COMETIDOS EM SITES – EMPREGO DE FONTES ABERTAS

Alesandro Gonçalves Barreto[1]

RESUMO

O presente artigo examina a busca de elementos informativos por meio do emprego de fontes abertas na investigação de crimes cometidos em sites de *Internet*. A preservação da evidência é de suma importância nessa seara, entretanto, não é o caminho único a ser seguido pelo investigador. Nesse âmbito, as informações livremente disponíveis na *Internet* podem auxiliar nesse mister.

Palavras-chave*:* Cache; Crime; Investigação; Site.

INTRODUÇÃO

A coleta de evidências é uma tarefa bastante árdua para o investigador de polícia nos fatos envolvendo crimes cibernéticos.

O Código de Processo Penal[i] estipula que, após ter conhecimento do cometimento do crime, "a autoridade policial deverá dirigir-se ao local, providenciando que não se alterem o estado e a conservação das coisas, até a chegada dos peritos criminais". Na prática, essa preservação do local do crime encontra dificuldades em locais reais, quanto mais em ambientes virtuais, caracterizados pela volatilidade da evidência.

Neste cenário, será realizada uma análise com o objetivo de buscar evidências relacionadas a sites, com a aplicação de ferramentas disponíveis em fontes abertas para o atingimento de informações úteis à investigação.

1. DA BUSCA DA EVIDÊNCIA CIBERNÉTICA

A investigação de um delito cometido em sites deve ser pontuada pela celeridade e oportunidade na coleta de elementos informativos. As evidências são bastante voláteis e, caso não

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. delbarreto@gmail.com.

preservadas da maneira ágil e adequada, serão perdidas ou questionadas posteriormente. Essa preservação pode ser feita por meio de certidão do escrivão de polícia, ata notarial[ii], dentre outras possibilidades.

BARRETO e SILVEIRA[iii]relatam a importância dessa preservação ao mencionar que:

> A evidência digital é de grande valia e deve ser tratada da mesma forma que a de outro local de crime. Caracteriza-se por ser volátil, anônima (em princípio), alterável e/ou modificável, bem como pode ser eliminada a qualquer instante. A preservação da evidência em crimes praticados na *internet* é uma das grandes dificuldades com que a investigação se depara. O caminho é bem longo desde a procura da vítima na delegacia até a expedição da ordem judicial determinando ao provedor a disponibilização dos registros de conexão e acesso a aplicações de internet. Nesse ínterim, o usuário responsável pela postagem de conteúdo ofensivo poderá modificar ou excluir o conteúdo, dificultando a individualização da autoria e materialidade delitiva.

Nesse diapasão, o emprego de fontes abertas tem agregado valor à procura, mesmo quando a evidência não tenha sido preservada. A popularização da *Internet* traz consigo inúmeras possibilidades de incremento à investigação policial, especialmente na seara dos delitos informáticos. Na busca por elementos informativos desse tipo de crime, há a impressão de que este conteúdo se encontra inacessível ou que são necessários softwares caríssimos para a solução do caso. Não se pode perder tempo com o que está disponível. As fontes abertas, desde que agregadas a outros elementos colhidos durante a investigação, devem ser utilizadas como ferramenta de investigação criminal.

Muito embora a evidência tenha sido perdida, o investigador ainda poderá alcançar outros elementos informativos individualizadores da autoria e materialidade delitiva. Dentre os caminhos a serem seguidos, serão analisados os aspectos atinentes ao registro de domínio e ao *cache* do servidor, conforme se verifica a seguir.

1.1 Registro de Domínio e Hospedagem do Site

O registro do domínio de um site e a hospedagem do conteúdo são dois requisitos necessários para se disponibilizar conteúdo na *Internet*. O domínio representa o endereço do site na *Internet*, por exemplo, www.meudominio.com.br. São inúmeras as informações que podem ser obtidas com essa consulta: CPF, CNPJ, dados cadastrais, e-mail de contato, dentre outras.

Esta verificação pode ser feita utilizando várias ferramentas disponíveis na *Internet*:

- Whois Registro Br – disponível em https://registro.br/cgi-bin/whois/. Em uma consulta a determinado domínio, podem ser encontradas informações sobre o titular, contatos

administrativos e técnicos, servidor DNS no qual está hospedado o conteúdo do site e datas de criação, modificação e expiração do domínio.

- ARIN - https://www.arin.net/
- DNS Stuff- http://www.dnsstuff.com/
- Geek Tools - http://geektools.com/whois.php
- Who.is- https://who.is/.
- Whois Lookup- http://whois.domaintools.com/

Diferentemente do domínio, a hospedagem é o espaço pago ou gratuito para alocar o conteúdo do site e permitir que ele fique disponível para acesso. As informações de hospedagem estão disponíveis na ferramenta *whois.* Em algumas situações, o site pode estar registrado ou hospedado no mesmo prestador do serviço. Noutras, não. Caberá ao responsável pela investigação fazer a consulta, identificar o detentor e requisitar as informações necessárias à individualização da autoria. Essas devem ser confrontadas e complementadas com outros bancos de dados.

1.2 Cache do Site

O *cache* de um site permite a visualização da cópia de uma página. Essa funcionalidade é criada pelos buscadores para que os resultados de busca sejam exibidos de forma instantânea. Dessa maneira, pode-se utilizar esse recurso para verificar a última versão do site, mesmo que ele esteja *off-line*.

Uma das formas de visualizar no Google o *cache* de um site é utilizando o navegador *Chrome* e digitando na *URL* o termo "cache: página a pesquisar". Nesse caso, aparecerá a informação de que se trata de um *cache* do Google da página pesquisada, a data e hora em que foi gerada, bem como a advertência de que ela pode ter sido modificada nesse período. Este *cache* pode ser visto ainda clicando em uma seta logo após a *URL* do site fornecida pelo buscador, onde se permite ver o recurso ou páginas similares. Caso o buscador Google atualize esta página, o conteúdo não estará mais disponível.

Variadas ferramentas disponíveis em fontes abertas possibilitam a visualização de conteúdos armazenados nas páginas durante um longo período de tempo. Um dos principais meios utilizados para se fazer essa busca é o site Archive.org[iv] ou popularmente conhecido por *Wayback Machine*. A

ferramenta é bastante interativa, constando as datas especificas em que se tem a imagem da página disponível.

CONCLUSÃO

A preservação de um local de crime– quer seja físico ou virtual (virtualizado) – é de suma importância para a individualização da autoria delitiva. O investigador deve atuar de maneira célere e oportuna visando preservar e garantir a cadeia de custódia dos elementos informativos produzidos.

Muito embora deva haver essa celeridade, às vezes o conteúdo criminoso postado num site é excluído e não preservado pelo investigador por inúmeros fatores, dentre os quais se pode citar: falta de conhecimento na investigação de crimes cibernéticos e estrutura da polícia judiciária em desacordo com a Lei Azeredo[v].

Não obstante, a investigação do delito cibernético deve atuar para identificar outros dados que possam apontar o responsável pela postagem de um conteúdo criminoso num site. Para tanto, deverá utilizar ferramentas disponíveis em fontes abertas e identificar os dados de registro e de hospedagem de um determinado domínio.

De outra banda, a busca pelo *cache* do servidor revelará imagens de páginas na *Internet*, demonstrando como elas estavam dispostas em determinado momento, fornecendo dados úteis à investigação.

Frize-se que os caminhos acima apontados não exaurem em nenhum momento outras metodologias investigativas de crimes cometidos em *sites*, apenas direcionam o investigador na busca de elementos informativos.

REFERÊNCIAS

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

_____. WENDT, Emerson. CASELLI, Guilherme. Investigação Digital em Fontes Abertas. BRASPORT Editora. Rio de Janeiro. 2017.

_____. 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.

_____. Preservação da evidência eletrônica: desafio à Polícia Judiciária. **Direito e TI**, Porto Alegre, fev. 2016. Disponível em: <http://direitoeti.com.br/artigos/preservacao-da-evidencia-eletronica-desafio-a-policia-judiciaria/>. 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.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 25. fev. 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.

_____. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.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.

[i] Art.6º, inc.I do CPP.

[ii] Código de Processo Civil. Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.
Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.

[iii] Manual de Investigação Cibernética à Luz do Marco Civil da Internet. P. 29

[iv] Disponível em https://archive.org. Permite a busca do histórico de mais de duzentas e setenta e nove bilhões de páginas na Internet. O acervo conta ainda com a busca histórica de textos, vídeos, áudios, softwares e imagens.

[v] Lei 12.735, de 30 de novembro de 2012. Art. 4o 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.