ISSN 2447-1097

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

EXIF METADATA - A INVESTIGAÇÃO POLICIAL SUBSIDIADA POR SUA EXTRAÇÃO E ANÁLISE

Alesandro Gonçalves Barreto[1]

Guilherme Caselli[2]

RESUMO

O artigo analisa a utilização de metadados de arquivos como elemento para agregar informações úteis a investigações em andamento. O conteúdo postado na Internet traz consigo informações de extremo valor, incumbindo à polícia judiciária, todavia, a utilização de ferramentas e procedimentos na busca dessas evidências para a materialização dos delitos. Para tanto, procurou-se contextualizar a busca de *metadados*, não só em fotografias, mas em outros formatos de arquivos, visando a auxiliar a investigação criminal. Por fim, em estudo de caso, demonstrou-se a aplicabilidade desse procedimento numa investigação realizada com êxito.

Palavras-chave: Conteúdo; Eficiência; Internet; Investigação; Metadado.

INTRODUÇÃO

É fato que a Internet tem possibilitado uma grande exposição, principalmente em redes sociais, onde os indivíduos postam uma infinidade de informações sobre sua intimidade e suas relações sociais. Os criminosos, por vezes, trilham por caminho idêntico, colocando fotografias do produto do crime ou, em algumas situações, quando foragidos, imagens desdenhando da polícia e da sociedade.

A investigação policial não pode ser estanque. Distantes são os tempos em que estava adstrita apenas a declarações e exames periciais. A tecnologia tem agregado novas possibilidades ao investigador para individualizar a autoria e materialidade delitiva. Um desses caminhos a serem trilhados é a análise do *exif* das fotografias e arquivos postados na internet, os chamados *metadados*.

1 Delegado de Polícia Civil do Estado do Piauí e coautor do livro Inteligência Digital da Editora Brasport. delbarreto@gmail.com.

[2] Guilherme Caselli é Policial Civil do Estado do Rio de Janeiro – DRCI/RJ. caselli.guilherme@gmail.com

ISSN 2447-1097

Em nome da eficiência, a Polícia Judiciária deve utilizar os dados dispostos na internet para potencializar sua função precípua de investigar. Ao buscar os *metadados* o policial pode obter dados de localização de um foragido da justiça, informações sobre o tipo de equipamento utilizado para fazer a foto e ainda, em alguns casos, reconstituir cenários sobre as condições físicas nas quais aquela imagem ou o arquivo foi produzido.

1. *EXIF* METADATA: O QUE É?

O *exif* metadata é a informação adicional do arquivo da fotografia que pode ter dados sobre data e hora, tamanho, características da câmera ou do *smartphone*, dados de luminosidade e outras informações úteis. Em alguns casos, quando o GPS – *Global Positioning System* – do equipamento está ligado, é possível obter a real posição em que a fotografia foi tirada. Cada metadado traz consigo dados individualizadores da imagem produzida.

Os metadados inseridos nas fotografias podem ainda ser úteis na proteção dos direitos autorais: por exemplo, quando um fotógrafo posta uma imagem, ele pode incluir dados referentes ao nome do autor, direitos autorais, telefone e *e-mail* para contato.

Neste sentido, existe um forte movimento de manifesto exercido na internet contra a supressão dos metadados capitaneado pela IPTC – *International Press Telecommunications Council*[i]. Seu pleito baseia-se principalmente na preservação dos direitos autorais do autor da fotografia, bem como dos direitos associados à fotografia.

Os *metadados* não são exclusivamente de imagens e fotos, sendo possível verificá-los em arquivos de extensões variadas, como por exemplo editores de texto – .doc; .pdf –, sendo portanto, plenamente possível a inserção de elementos técnicos capazes de zelar pela preservação dos direitos autorais e intelectuais de seu autor.

Quando um arquivo é copiado, carregado ou baixado em qualquer lugar, os seus metadados o acompanham. A sua visualização não ocorre através da execução da imagem propriamente dita. Para visualizar esse conteúdo existem vários caminhos possíveis, que apresentarão diversos níveis de acesso a informações gravadas nos arquivos.

Assim, definido o que são os *metadados*, importante verificar como se dá a sua extração nas redes sociais e o que afeta na privacidade nesses ambientes.

ISSN 2447-1097

2. EXTRAÇÃO DO *EXIF VERSUS* PRIVACIDADE EM REDES SOCIAIS

Nos anos de 2013 e 2016 o *site* especializado em metadados[ii] – embeddedmetadata.org – realizou uma grande pesquisa de análise de matérias de imagens exibidos junto aos principais *sites* de mídias. Seu objetivo era verificar se, ao exibirem imagens postadas por seus usuários, preservavam os metadados originais da foto e, assim, garantiriam o direito autoral de seu titular.

Como resultado, verificou-se que diversas redes sociais, apesar de armazenarem os metadados dos arquivos dos usuários em seus servidores, não os disponibilizam. A lista completa do estudo pode ser acessada no sítio mencionado.

A fundamentação dos servidores das redes sociais para tanto são as mais variadas possíveis: necessidade de espaço nos servidores de armazenamento; preservação e proteção da privacidade do usuário; dinamização e otimização na execução dos arquivos, dentre outros.

Tais argumentos, no entanto, tecnicamente não convencem. O *exif* de fotografias restringe-se a pequenos elementos informativos que ocupam espaços mínimos de *bits*, sequer influenciando no armazenamento físico, comparando-se ao espaço demandado na guarda das fotografias e vídeos realizados pelos servidores.

O *Facebook*, por exemplo, retira as informações de metadados das fotos quando as mesmas são carregadas para a página do usuário. Nesse caso, resta infrutífera à investigação qualquer tentativa de leitura do conteúdo dessas imagens diretamente na página do usuário.

O *Twitter* segue o mesmo caminho, utilizando como padrão de georreferenciamento de uma postagem o disposto no GPS quando da marcação de um *tweet* e não os *geotags* da imagem. Também não disponibilizam para os demais usuários informações administrativas, como modelo do aparelho celular, data da realização da foto, dentre outros elementos[iii].

Populares mensageiros instantâneos, como *Whatsapp*[iv], *Viber*[v], *Telegram*[vi], dentre outros, também não disponibilizam para os usuários os metadados dos arquivos, impossibilitando o avanço de investigações na medida em que a materialidade delitiva se resume a um arquivo de imagem ou vídeo disseminado por algum destes aplicativos.

O *Whatsapp*[iv] anuncia em seu site, na parte de política de legalidade:

> Quando você usa o serviço WhatsApp, os nossos servidores registram certas informações em geral que o nosso aplicativo envia sempre que uma mensagem é enviada ou recebida, ou se você atualizar ou solicitar qualquer

> informação de estado, incluindo o tempo e carimbos de data e os números de telefone celular as mensagens foram enviadas a partir de e para."

O servidor do *Telegram*[vi] também informa preservar certos dados: "Storing data - Telegram apenas armazena os dados de que necessita para funcionar corretamente - por tanto tempo quanto você quer telegrama para funcionar.". Contudo não informa quais são estes dados necessários para o seu funcionamento.

De certo, apesar de os aplicativos afirmarem que armazenam estes dados, é fácil constatar que não os disponibilizam ao interlocutor das mensagens. Qualquer usuário pode baixar para o computador os arquivos de imagens e realizar os testes para visualização dos metadados que atestará a ausência de elementos técnicos.

Apesar de algumas redes sociais não disponibilizarem o acesso a esse tipo de informação, não implica que estes dados inexistem ou que estão inacessíveis. Cabe à autoridade policial, valendo-se do seu poder de requisição, demandá-las ao servidor, podendo ainda representar judicialmente pela sua obtenção. De bom alvitre lembrar que as aplicações de internet manterão esse conteúdo armazenado pelo prazo de 06 (seis) meses, nos precisos termos do art. 15 do Marco Civil da Internet.

Independente do caminho escolhido é recomendado que a autoridade policial, de pronto, expeça um ofício requerendo a preservação do conteúdo referente ao *exif* da imagem solicitada. A solicitação deverá conter, sob pena de não atendimento, identificação clara e precisa do conteúdo, possibilitando, assim, a localização inequívoca do conteúdo por parte da aplicação de internet, devendo também ser informada a *url – Uniform Resource Locator* – do arquivo respectivo.

3. DA BUSCA POLICIAL POR EVIDÊNCIAS EXISTENTES EM METADADOS

Como já discorrido, a análise dos metadados dos arquivos funciona como valioso recurso de coleta de dados, traduzindo-se como verdadeira impressão digital daquele arquivo, possibilitando individualizar sua criação, modificação, origem, geo marcação, dentre outros elementos.

Contudo, aqui cabe um alerta: deverá o agente analisar estes dados em conjunto como outros elementos da investigação, pois o *exif* dos arquivos pode ser deletado ou, até mesmo, editado através de *softwares* e plataformas *online*.

3.1. Furto ou roubo de máquina fotográfica

No caso de subtração de máquina fotográfica, existem aplicações de internet que possibilitam o rastreio desses equipamentos. É o caso dos sites *Camera Trace* e *Stolen Camera Finder*.[vii] A primeira ferramenta possui um banco de dados com mais de 11 milhões de máquinas cadastradas[viii], escaneando dados de fotografias expostas na internet. A aplicação possibilita o acesso a dados capazes de rastrear o equipamento fotográfico. Para tanto, deverá a autoridade policial encaminhar uma requisição via e-mail institucional, informando o número de série dos equipamentos a serem rastreados[ix].

Da mesma forma, a ferramenta *Stolen Camera Finder*[x] faz a busca de dados de fotografias carregadas na internet, fazendo sua relação com o número de série da máquina da qual foi tirada.

3.2. Utilização de sistemas operacionais, *softwares* e plataformas como leitores de metadados

Os sistemas operacionais, especificamente a versão Windows 7 e superiores, possibilitam a visualização de informações detalhadas sobre a origem da imagem, a data em que a fotografia foi tirada, o nome do programa, dimensão, fabricante e modelo da câmera, quando foi salva no computador, além de outros atributos. Sua visualização se dá clicado com o botão direito do *mouse* em cima do arquivo de imagem, acessando em seguida aba *detalhes*.

Softwares pagos, como *photoshop*, permitem visualizar estes elementos além de outros dados técnicos como: informações de IPTC, contato, descrição detalhada do arquivo e histórico.

Em opção *freeware*, há aplicações capazes de organizar, inserir ou editar metadados. Existem ainda outras opções de *softwares* gratuitos disponíveis no mercado com as mesmas funcionalidades[xi, xii]. Destacam-se, ainda, extensões para os navegadores *Google Chrome* e *Firefox*[xiii, xiv].

Em se tratando de plataformas *online*, existem diversos sites que permitem visualizar metadados de arquivos, sejam salvos nos computadores, sejam acessíveis em *sites* através de *links*[xv].

3.3. Análise de metadados em arquivos variados

Outro recurso a ser utilizado pelo investigador quando da coleta probatória é a verificação de metadados nos arquivos de editores de texto. Através deste procedimento é possível extrair valiosíssimas informações sobre o arquivo, tais como: autor do documento, origem, informações ocultas, data de criação, domínio, dentre outros.

A verificação em arquivos do tipo *Word*, a partir da versão 2007 pode ser feita da seguinte forma: após aberto o documento em questão, deve ser clicado no *botão Office*, que fica no canto superior esquerdo do menu principal, após deve ser acessada a opção *preparar* e, na aba que se abrir, escolher a opção *propriedade*.

Nas versões *Office 2010* e superiores, deve ser realizado o seguinte procedimento: após aberto o documento em questão, deve ser clicado na aba *arquivo*, que fica no canto superior esquerdo do menu principal. No canto direito da tela que abrir, serão exibidas informações sobre a origem do arquivo analisado, sobre seu autor e demais pessoas relacionadas. Nesta mesma tela, agora no canto inferior da direita, clicando na opção *mostrar todas as propriedades* serão apresentadas informações adicionais avançadas sobre o artigo analisado.

É possível editar ou eliminar estes metadados, devendo para tanto ser clicado na opção *arquivo* do *menu principal*, após, na opção *inspecionar elemento – inspecionar se há problemas* e, na tela que se abrir, *inspecionar documentos*. Através destes comandos, é possível verificar uma série de elementos incluídos no arquivo, havendo ainda a possibilidade de excluí-los.

No caso de arquivos do tipo *pdf*, a verificação dos metadados inseridos pode ser feita clicando na opção *file* (arquivo); após em *properties* (propriedades). Dependendo da versão do visualizador de PDF – *Portable Document Format* –, aparecerá uma tela com opções de *descrição, segurança, fonte, edição e avançados*, possibilitando assim, nesta última opção, verificar o título do arquivo, informações sobre o seu autor, data de criação, de modificação, domínio, aplicação que o gerou, dentre outros.

4. ESTUDO DE CASO

Na qualidade de policiais especializados em crimes de informática, utilizou-se a metodologia de busca via metadados em diversas investigações como meio para materialização

de fatos criminosos, bem como elemento individualizador de autoria. A investigação que será narrada ocorreu em junho de 2016, no Estado do Rio de Janeiro, pela Delegacia de Repressão a Crimes de Informática, e versou sobre violência sexual praticada contra menor de idade.

Em sede policial, uma menor de idade narrou, perante a autoridade policial, ter sido vítima de violência sexual. Relatou que não dispunha de elementos de convicção que apontassem o autor do fato, lembrado apenas que a relação sexual foi registrada através de um aparelho celular.

Após diligências, foram individualizados 02 (dois) possíveis suspeitos. A autoridade policial que presidiu as investigações representou judicialmente pela busca e apreensão a ser realizada nos endereços dos suspeitos. Durante a diligência, foram arrecadados celulares, computadores, *pen drives* e *hard disk*.

Em análise realizada nos periféricos apreendidos, foram encontradas imagens do ato sexual como narrado pela vítima. Verificou-se, então, os metadados destes arquivos de imagem, sendo possível colher informações como a data, hora e segundo em que os arquivos foram gerados; a geolocalização, apontando o local exato onde a atividade criminosa foi realizada; dados técnicos, como o fabricante da máquina de retrato, pertencente a um *smartphone*, modelo e seu *software*. Estas especificações técnicas eram as mesmas do celular apreendido de um dos suspeitos.

Assim, mediante a estas provas técnicas e as demais provas colhidas no bojo da investigação policial, conseguimos corroborar a materialidade e apontar a autoria delitiva.

CONCLUSÃO

A evolução tecnológica tem agregado valor à investigação policial. Não faz muito tempo, ao policial ensinava-se os procedimentos a serem tomados na busca de evidências para elucidar um delito. Todavia, os tempos são outros. Em vários delitos, o local de crime saiu do físico ao virtual e essa nova realidade permite ao policial inovar e buscar outros elementos na individualização da autoria e materialidade delitiva.

O policial não deve, portanto, abdicar da busca de “impressões digitais” de arquivos postados na internet, principalmente em redes sociais ou de conteúdo encontrado em poder do investigado. A utilização das informações extraídas de *metadados* já se mostrou útil em procedimentos investigativos para materialização de eventos criminosos.

A digitalização das relações sociais possibilita ao investigador novos horizontes na arte de investigar delitos. Cabe ao policial adequar-se às novas tecnologias para trazer resultados mais eficazes no cumprimento do seu dever.

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 10. jul. 2016.

EMBEDDED METADADA MANIFESTO. **Social Media Photo Metadata Test Results**. Disponível em: <http://www.embeddedmetadata.org/social-media-test-results.php>. Acesso em: 10. jul. 2016.

TWITTER. O que acontece com os dados do exif na minha foto. **Support**. Central de Ajuda. Disponível em: <https://support.twitter.com/articles/20169216>. Acesso em: 10 jul. 2016.

TELEGRAM. **Privacy Policy**. Disponível em: <https://telegram.org/privacy>. Acesso em: 10 jul. 2016.

VIBER. **Política de Privacidade**. Última atualização em: 28 abr.2014. Disponível em: <https://www.viber.com/pt/privacypolicy.html>. Acesso em 10 jul.2016.

WENDT, Emerson; BARRETO, Alesandro Gonçalves. **Inteligência Digital**. Brasport, 2013.

WHATSAPP. Informação Legal do WhatsApp. **Terms of Service**. Última Modificação em 07.jul.2012. Disponível em: <https://www.whatsapp.com/legal/>. Acesso em 10 jul.2016.

[i] International Press Telecommunications Council. Embedded metadata manifesto: this is where you find information about embedding metadata into digital media files. 2016. Disponível em: <http://www.embeddedmetadata.org/>. Acesso em: 10 jul. 2016.
[ii] Embedded Metadada Manifesto.
[iii] Twitter. Support. Central de Ajuda. O que acontece com os dados do exif na minha foto.
[iv] Informação Legal do WhatsApp
[v] Política de Privacidade do Viber.
[vi] Telegram. Privacy Policy.
[vii] Vide WENDT, Emerson; BARRETO, Alesandro Gonçalves. **Inteligência Digital**. Brasport, 2013.
[viii] Camera Trace Featured Details. Disponível em http://www.cameratrace.com/learn-more.
[ix] As solicitações devem ser enviadas diretamente para o email support@gadgettrak.com.
[x] Stolen Camera Finder. Disponível em: http://www.stolencamerafinder.com/.
[xi] Phil Harvey. ExifTool. 2016. Disponível em: <http://www.sno.phy.queensu.ca/~phil/exiftool>. Acesso em: 10 jul. 2016.
[xii] Two Pilots™. Editing, Creating, and Viewing EXIF, IPTC, and XMP Data with Free Exif Pilot Editor. 2016. Disponível em: <http://www.colorpilot.com/exif.html>. Acesso em: 10 jul. 2016.
[xiii] EXIF Viewer. 2015. Disponível em: <https://chrome.google.com/webstore/detail/exif-viewer/nafpfdcmppffipmhcpkbplhkoiekndck>. Acesso em: 10 jul. 2016.
[xiv] Eyrich, Christian; Mielczarek, Ted. FxIF. 2015. Disponível em: <https://addons.mozilla.org/pt-BR/firefox/addon/fxif/>. Acesso em: 10 jul. 2016.
[xv] Jeffrey Friedl's. Image Metadata Viewer. 2016. Disponível em: <http://regex.info/exif.cgi>. Acesso em: 10 jul. 2016.