Metadados em WhatsApp: Uma nova perspectiva de coleta de evidências

Por **Juristas** - 27/03/2019

-
-
-
-
-

Avalie (23 Votos)

*Por Guilherme Caselli**

RESUMO

Créditos: Wachiwit | iStock

Pretendemos através do presente artigo realizar um enfrentamento técnico comprobatório de que o aplicativo *WhatsApp* colhe, armazena e compartilha elementos sobre os usuários e mídias que transitam por seus servidores. Estes dados, caso fossem encaminhados para as Autoridades Públicas, obedecida a legislação pátria, individualizariam criminosos e evitariam a propagação de crimes em massa virtual como *Fake News*.

PALAVRAS-CHAVE: *WhatsApp* – Crimes Cibernéticos – "metadados" – Polícia Judiciária – Investigação Digital.

SUMÁRIO: INTRODUÇÃO. 1 DA UTILIZAÇÃO EM MASSA DO APLICATIVO WHATSAPP; 2. ESTUDO DE CASOS – MEIO CIENTÍFICO DA PESQUISA APLICADA: OBJETIVO, METODOLOGIA E FERRAMENTAS DE ANÁLISE; 2.1 FERRAMENTAS DE ANÁLISE; 2.2. ESTUDO DE CASO 01; 2.3. ESTUDO DE CASO 02; 2.4. ESTUDO DE CASO 3. CONCLUSÃO.

INTRODUÇÃO:

É fato notório que o programa de mensageria instantânea *WhatsApp* é um dos principais meios de comunicação, já tendo sido determinado em julgados que a manutenção dos seus serviços teria como base legal o inafastável e sagrado direito à informação sobrepondo inclusive, em uma balança de ponderação ao dever de empresa particular, o cumprimento de ordem judicial (1)

"Ora, a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa. (…)""

Contudo, a má utilização deste aplicativo pode vir a acarretar resultados em diversos ramos do direito como o penal, tendo crimes sido executados através de seus serviços, trabalhista advindo justa causa e consequentemente a recisão do contrato de trabalho; família, ocasionando separações; cível derivando em danos morais a serem indenizados; FakeNews que resultam em instabilidade social etc.

No ano de 2017 foi realizada audiência pública (2) no STF para discutir o bloqueio judicial do *WhatsApp* e Marco Civil da Internet com fundamento na Ação Direta de Inconstitucionalidade 5.527 e Arguição de Descumprimento de Preceito Fundamental 403

Na oportunidade, Brian Acton, um dos fundadores do aplicativo *WhatsApp* foi arguido por diversos estudiosos sobre a possibilidade de efetivação de técnica de cooperação do aplicativo com os Órgãos Públicos. Também foi instado, por diversas vezes, a se manifestar especificamente sobre a coleta e disponibilização de "metadados" nos arquivos transitados em seus servidores, contudo, Brian não enfrentou diretamente a *questão.

O único documento oficial produzido pela empresa *WhatsApp* sobre a coleta de dados de mídia e de usuários que utilizam seus serviços e passível de ser fornecido às Autoridades Públicas é o intitulado "Informações para as autoridades policiais", em: *Frequently Asked Questions* [3].

Na conformidade do documento indicado, é possível a divulgação dos seguintes dados mediante autorização judicial: registro de contas; o que pode incluir nome, data de início do serviço, data da última visualização, endereço IP e endereço de email; informações sobre "recados", fotos de perfil, informações de grupo e lista de contatos, caso disponíveis.

O mesmo documento, na sessão: Estados Unidos – Requisitos legais de processos, também informa não ser possível ter acesso ao conteúdo de comunicações, como números que o usuário bloqueou ou números que bloquearam o usuário, além dos registros básicos dos assinantes descritos acima. Desta forma, caso alguém receba um arquivo de mídia (áudio, foto e vídeo) via *WhatsApp* e tente buscar por seus "metadados", verificará que o *WhatsApp* não disponibiliza as informações de "metadados" ([4].

Ocorre que, nas informações legais[5], o *WhatsApp* declara de forma objetiva que pode coletar, usar, reter e compartilhar dados, não especificando claramente quais:

"Proteção jurídica

Podemos coletar, usar, reter e compartilhar dados quando acreditarmos em boa fé que isso se faz necessário para: (a) atuar conforme exigido pela legislação aplicável ou em processos judiciais ou administrativos; (b) impor nossos Termos e outros termos e políticas aplicáveis, inclusive investigações sobre possíveis violações; (c) detectar, investigar, prevenir e resolver atividades fraudulentas e ilícitas ou questões de segurança ou técnicas; ou (d) proteger os direitos, a propriedade e a segurança de nossos usuários, do *WhatsApp*, da família de empresas do Facebook ou de terceiros."

De forma prática, hoje já é possível requerer judicialmente que a empresa forneça: I) dados cadastrais atribuídos ao perfil, com o número telefônico, modelo do aparelho e ip de criação da conta; II) histórico de ip's utiliados; agenda de contatos e ainda, informações dos grupos que o requerido faz parte; o avatar (imagem) de cada um dos grupos, informações de quem criou o grupo, data e quantos membros fazem parte dele. É possível também cumular o pedido para que o *WhatsApp* forneça todas essas informações dos membros de cada um dos grupos.

Também já é possível determinar, via ordem judicial, que o *WhatsApp* proceda à exclusão de mídias com conteúdo ilícito de seus servidores. Explicando de forma técnica, a empresa tendo por base o código *hash* (um expediente técnico capaz de individualizar um arquivo; uma espécie de DNA, porém de muito mais precisão) da criptografia atribuída ao elemento questionado, coloca aquela assinatura digital (código *hash*) em uma *blacklist*, impossibilitando compartilhamentos.

Evidentemente, em se tratando de mídias contendo cenas de sexo envolvendo crianças e adolescentes, a colocação do respectivo código do *hash* em *blacklist* independe de ordem judicial, podendo os responsáveis pela recusa responder pelo tipo previsto no §2º do art. 241-A da lei 8.069/90.

Tecnicamente os dados fornecidos para as Autoridades Públicas podem ser categorizados como elementos formais por não guardar dados de conteúdo das comunicações em si. Ainda, de not que estes recursos disponíveis pelo provedor de aplicação *WhatsApp* para as Autoridades Públ se referem sempre ao usuário do aplicativo, não havendo, de forma objetiva, nenhum mecanismo

técnico de fornecimento de informações para os Entes Estatais relacionadas à conteudo, incluindo textos ou arquivos de mídia.

Esse meio de coleta probatória disponível pode ser eficaz quando o modelo de apuração foca o investigado como meio para se chegar a elementos relacionados ao crime. Contudo, tendo como norte apuratório somente um arquivo de mídia com conteúdo ilícito trafegado pelos servidores do *WhatsApp*, os possíveis meios de coleta de dados, até então dispostos pela empresa se tornam irrelevantes. Assim, para o êxito neste modelo de investigação que foca a mídia – categorizados como elementos materiais, é imprescindível ter acesso aos "metadados" do tipo administrativos e descritivos.

Para ilustrar, imaginem o seguinte exemplo: um arquivo de mídia (foto, vídeo ou áudio) com uma cena de um crime passa a ser divulgado em massa pelos usuários do *WhatsApp*. Os meios de coletas de informação disponíveis pelo *WhatsApp* em nada adiantarão para elucidação dos fatos, ou seja, não são aptos a apontar a origem daquele material de mídia ou, ainda, o primeiro usuário que encaminhou tal arquivo, elementos imprescindíveis para atribuir a autoria do fato criminoso registrado naquele arquivo de mídia.

Não pretendemos, no presente artigo, ingressar na seara da possibilidade de fornecimento de conteúdo das mesagens trocadas via texto, assunto indicutivelmente polêmico. Queremos através destas linhas asseeverar que é possível sim o *WhatsApp* fornecer "metadados" dos arquivos de mídias que transitam em seus servidores.

Antes de aprofundarmos no assunto, mister se faz esclarecer o que se entende por "metadados": em uma linguagem objetiva, metados são definidos como dados sobre dados, ou seja, informações que são adicionadas sobre aquele arquivo e que exercem a função descritiva, informativa sobre aquele arquivo em questão. Estruturalmente, podemos organizar[(6)] os "metadados" em ao menos três tipos:

"METADADOS" DESCRITIVOS incluem informações como pontos de contato, título ou autor de uma publicação, um resumo de uma obra, palavras-chave usadas em uma obra, uma localização geográfica ou até mesmo uma explicação da metodologia. Esses dados são úteis para descobrir, coletar ou agrupar recursos de acordo com as características compartilhadas pelos recursos.

"METADADOS" ESTRUTURAIS explicam como um recurso é composto ou organizado. Um livro digitalizado, por exemplo, pode ser publicado como imagens de páginas individuais, arquivos PDF ou HTML. Essas páginas ou componentes podem ser agrupados em capítulos. Os dados do capítulo, tabela de conteúdo ou detalhes do layout da página são considerados "metadados" estruturais. Um mapa estrutural das páginas ou outros recursos de um site, tipos de registro de evento de intrusão de segurança ou registros de detalhes de chamadas de voz também são tipos de "metadados" estruturais.

"METADADOS" ADMINISTRATIVOS são usados para gerenciar um recurso. Datas de criação ou aquisição, permissões de acesso, direitos ou proveniência, ou diretrizes para disposição, como retenção ou remoção, são exemplos de direitos que um arquivista digital, curador, pode empregar. "metadados" semelhantes seriam relevantes para um administrador de banco de dados ou para administradores responsáveis por capturar fluxos de tráfego de telecomunicações ou de rede de dados ou log de segurança e dados de eventos.

A rigor, durante as investigações policiais realizadas sobre crimes ocorridos no cenário virtual, os modelos descritivos e administrativos são os mais utilizados.

A utilidade prática deste recurso como meio de coleta de probatória, objetiva a busca por evidências e elementos ensejadores da autoria. Por ser tratar de meio de coleta probatória, este recurso não se atém somente à seara Penal, podendo ser utilizado em qualquer ramo do direit

1. DA UTILIZAÇÃO EM MASSA DO APLICATIVO *WHATSAPP*:

Com a facilitação e democratização do acesso à internet a massa da população mundial passou a aceder ao posto de usuários de redes sociais como Instagram e Facebook, além do aplicativo de serviço de mensageria *WhatsApp*, poderosa ferramenta de difusão de informações.

Contudo, a benesse desta ferramenta que concede acesso à informação trouxe a reboque usuários mal-intencionados que utilizam estes serviços de forma deturpada para a execução de atividades ilícitas ou irregulares como a difusão de *Fake News*.

Estudos apontam que a difusão de informações inverídicas, conhecidas como *Fake News*, impactou cerca de 8,8 milhões de brasileiros no primeiro trimestre de 2018. Segundo o laboratório da PSafe[(7)] especializado em crimes cibernéticos, mais de 95% das *Fake News* foram enviadas via *WhatsApp*.

O fenômeno das *Fake News* e o seu impacto no pleito eleitoral também foi objeto de estudo publicado em 2018 pela faculdade Dartmouth[(8)] sobre as eleições presidenciais ocorridas nos Estado Unidos em 2016. Os pesquisadores apuraram que 65% das visitas a sites de notícias falsas vinha de um mesmo grupo, composto por 10% dos eleitores identificados como mais conservadores. Ainda, 27% dos eleitores leram pelo menos uma notícia falsa no período analisado e que estas representaram 2,6% de todos os textos lidos em sites noticiosos (incluindo os veículos tradicionais), sendo a maioria dos textos falsos "esmagadoramente pró-Trump". Das 5,45 notícias falsas lidas, em média, por leitores de *Fake News* durante o período, 5 eram identificadas como favoráveis ao republicano.

Esses espantosos números aliados à divulgação em massa através de redes sociais e serviços de mensagem instantânea certamente são hábeis a causar um resultado nefasto no cenário político assim como causar grave instabilidade social.

Sob a ótica da polícia investigativa – Civil ou Federal, uma investigação tendo por elemento tão somente um arquivo de mídia encaminhado via *WhatsApp* se torna muitas das vezes verdadeira quimera. Um dos poucos recursos possíveis cinge-se a simples análise reversa das imagens em serviços de buscadores da web resultando, em grande parte, como infrutífera, haja vista o arquivo de mídia analisado não estar presente em nenhuma base de dados indexável – como um servidor de site, por exemplo.

Veículos de mídias especializados em tecnologia[(9)] recentemente noticiaram um recurso que em breve estará disponível no aplicativo *WhatsApp* na versão 2.19.73 do *WhatsApp* Beta. Trata-se de uma opção de busca reversa de imagem no Google. O prexto deste serviço seria o combate às *Fake News*, ou seja, ao receber uma imagem no *WhatsApp*, o usuário poderia diretamente pelo aplicativo realizar buscas de imagens semalhantes

Contudo, a análise reversa de imagem é apenas um dos possíveis recursos que devem ser lançados pelos investigadores. Entedemos que muito mais eficaz na apuração de atividades relacionadas ao envio de mídias seria análise de "metadados".

Imaginemos o seguinte exemplo: é noticiado para a Autoridade Policial competente que um arquivo de mídia do tipo áudio com um conteúdo ilícito estaria circulando entre os usuários do aplicativo. Com base nos termos de serviço da empresa, nenhum dos elementos disponíveis às Autoridades Públicas serviriam para indicar a autoria do áudio. Como já dito, os dados passíveis de serem fornecidos se referem exclusivamente ao usuário e não aos textos ou mídias.

Com base nestes elementos apontados, a investigação conduzida pelo Delegado de Polícia estaria fadada ao insucesso. A grande indagação que deve ser feita é: será que realmente o *WhatsApp* não dispõe de meios técnicos aptos a apontar os "metadados" descritivos e estruturais deste arquivo?

2. ESTUDO DE CASOS – MEIO CIENTÍFICO DA PESQUISA APLICADA: OBJETIVO, METODOLOGIA E FERRAMENTAS DE ANÁLISE.

Nos estudos de casos que iremos tratar, tivemos como objetivo verificar a possível existência de "metadados" em arquivos de mídia que transitaram pelo servidor do *WhatsApp*. Como registro de mídia questionado, utilizamos arquivos de mídia do tipo áudio no formato "mp3" arrecadado através de serviço de *backup* realizado no "cloud" do Google Drive; arquivos de texto no formato *Portable Document Format* "PDF" e arquivos de imagem de extensão "WebP". Esses dois últimos foram arrecadados diretamente do aplicativo *WhatsApp*.

A metodologia aplicada foi a utilização de recursos computacionais adequados para o processamento e reprodução dos arquivados e encaminhados, programas de visualização de mídias com seus respectivos atributos e "metadados", de análise de binários e edição de "metadados" exif, possibilitando uma análise perceptual e técnica dos seus elementos.

2.1 FERRAMENTAS DE ANÁLISE:

Na análise dos arquivos ora questionados utilizamos as seguintes ferramentas:

I) HEX EDITOR NEO VERSION 6.24.00.5920; II) VLC media player Version 3.0.6 • Windows 64bit; III) Portable Document Format – PDF; IV) Criar figurinhas para *WhatsApp* – WAStickerApps e V) Sistema operacional Windows 10, versão 1809, 64 bits

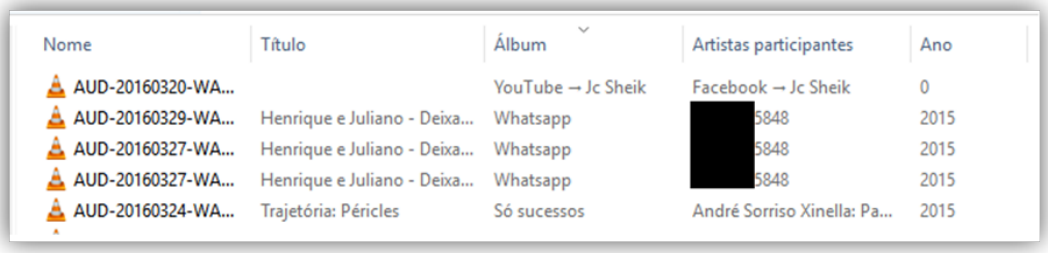
2.2. ESTUDO DE CASO 01

Enquanto policial especializado em crimes cibernéticos, no ano de 2016, no Estado do Rio de Janeiro, participamos de uma investigação em que um dos meios de coleta probatória foi o aplicativo *WhatsApp*. Nesta oportunidade, procedemos a coleta dos aspectos formais – dados cadastrais e históricos de acesso (ip's) e ainda dos aspectos materiais – conteúdo das mídias de imagens e de áudio. Estes arquivos foram colhidos remotamente, por meio de ordem judicial, através dos serviços de *backup* realizados em *clouds*.

Interessante notar que, os arquivos de mídia analisados, advindos desta quebra de sigilo judicial, apesar de terem transitado pelos servidores do *WhatsApp* não estavam criptografados além de terem mantido a integralidade dos "metadados".

Na figura abaixo é possivel ver através do visualisador de arquivos do sistema operacional windows a descrição dos arquivos de áudio que estavam alocados no *backup* do investigado. O segundo (AUD-20160329-WA…), terceiro (AUD-20160327-WA…) e quarto arquivo (AUD-20160327-WA…) da lista apresentam como "metadados" administrativos sua data de criação: 2015.

Apresentam também como "metadados" descritivos as seguintes informações: "Título" – Henrique e Juliano – Deixa; "Álbum" – *WhatsApp*; "Artistas participantes" XXXXXXX-5848



Nome	Título	Álbum	Artistas participantes	Ano
AUD-20160320-WA...		YouTube → Jc Sheik	Facebook → Jc Sheik	0
AUD-20160329-WA...	Henrique e Juliano - Deixa...	Whatsapp	[redacted]5848	2015
AUD-20160327-WA...	Henrique e Juliano - Deixa...	Whatsapp	[redacted]5848	2015
AUD-20160327-WA...	Henrique e Juliano - Deixa...	Whatsapp	[redacted]5848	2015
AUD-20160324-WA...	Trajetória: Péricles	Só sucessos	André Sorriso Xinella: Pa...	2015

Figura 01. Arquivos de áudio armazenados no cloud

Outra informação valiosa: Nos três arquivos analisados também foi preservada a imagem do álbum que é uma imagem atribuída quando da criação do arquivo.

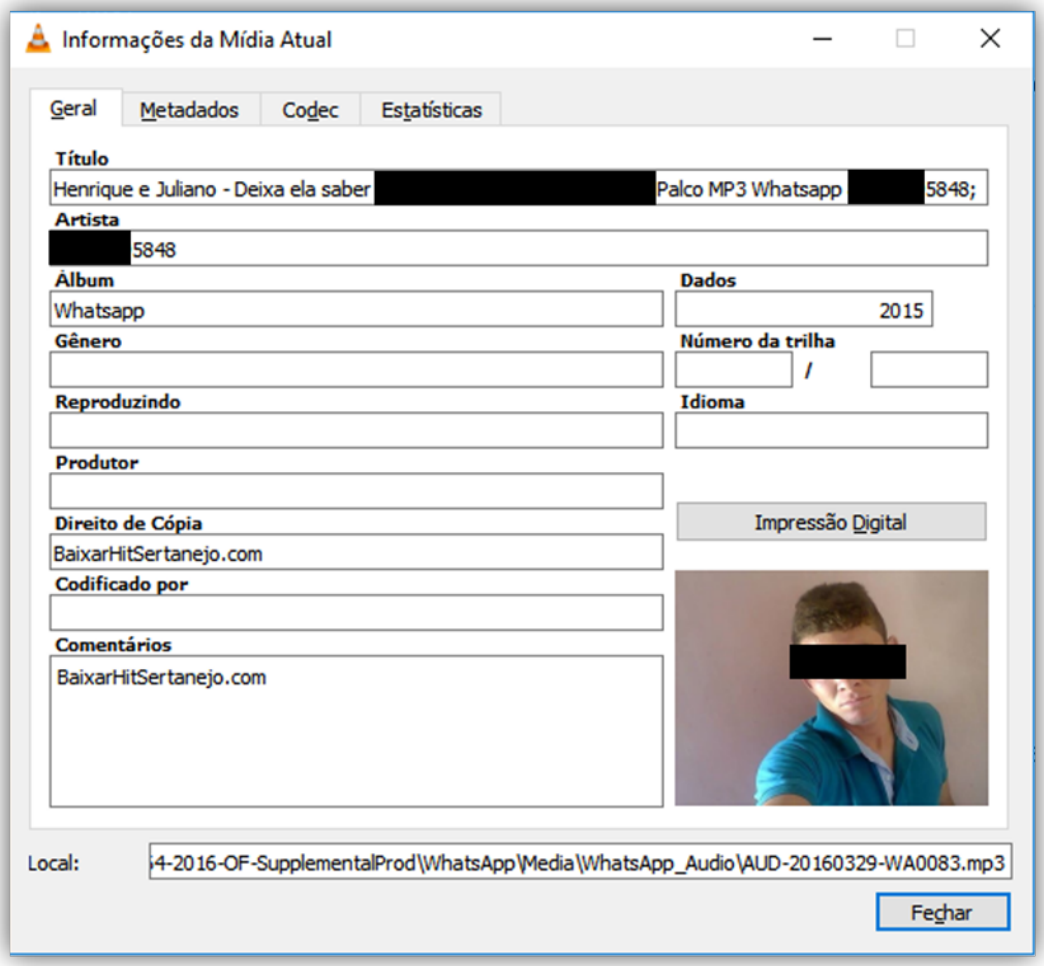


Figura 02. Analise dos "metadados" administrativos e descritivos, incluindo foto de capa. Visualização feita através do programa VLC

Realizamos buscas complementares em fonte aberta para, com base no número *WhatsApp*, localizar possíveis perfis nas redes sociais. Desta forma, localizamos o perfil do autor do arquivo de áudio. Interessante notar que detectamos a mesma foto usada como capa exposta no álbum público do indigitado:

Figura 03. Imagem no perfil do detentor da conta WhatsApp que gerou o arquivo de áudio

Também utilizamos técnicas de coleta em fonte aberta para comprovar que o perfil apontado é titular da conta *WhatsApp* indicada. A comprovação veio através de uma postagem realizada no dia 13 de dezembro de 2017 em que o localizado divulga sua conta WhatApp como se vê:

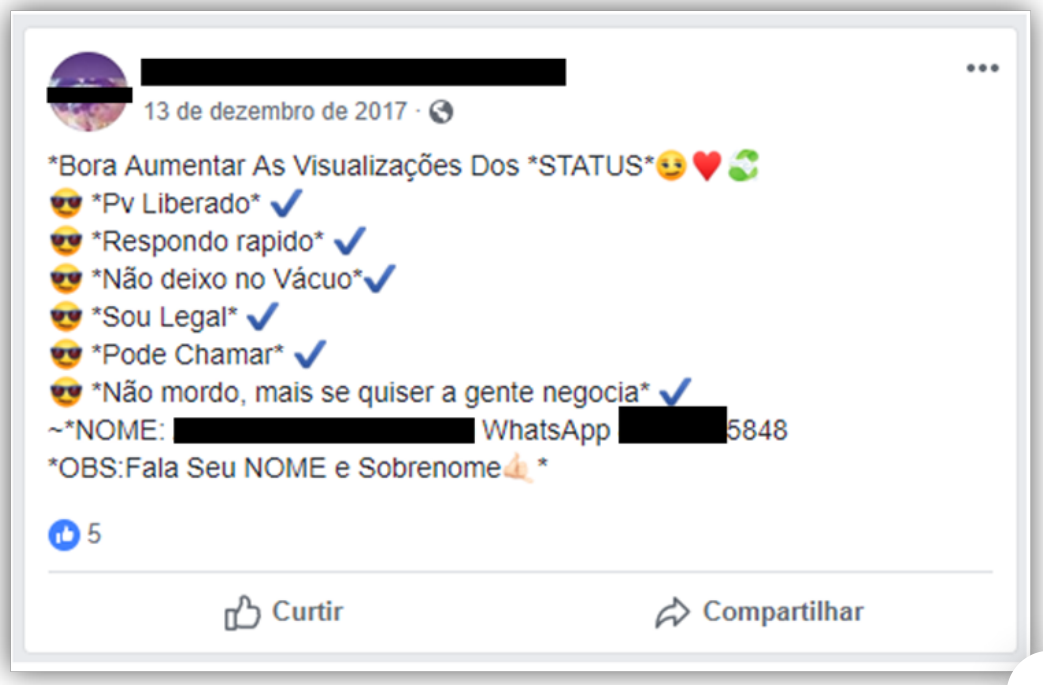


Figura 04. Imagem da postagem com a divulgação de sua conta WhatsApp

Ou seja, o *WhatsApp* colhe e preserva informações extremamente sensíveis de "metadados" dos arquivos de mídias dos usuários de seus serviços. Estas informações poderiam sim ser fornecidas para as Autoridades Públicas em casos graves envolvendo ilícito como por exemplo: ataques terroristas; difusão de mídias com conteúdo de abuso sexual de crianças ou contendo cenas de execução de seres humanos; disseminação de *Fake News*, dentre outros. Estes dados possibilitariam a individualização dos criminosos registrados nas mídias.

2.2. ESTUDO DE CASO 02

Outro caso prático que avançamos com a utlização de análise de "metadados" descritivos se deu em meados de agosto/novembro do ano de 2018 no Estado de São Paulo, na decretação do fim da greve dos caminhoneiros. Pouco tempo após a desmobilização da categoria, passou a circular no *WhatsApp* um arquivo em formado PDF com o seguinte título: Comunicado UDC Brasil 31082018.

O documento noticiava nova mobilização nacional paralisando por tempo indeterminado todo transporte rodoviário de carga com o único objetivo de chamar a atenção do Governo Federal.

Analisando os "metadados" presentes no arquivo através do programa *Adobe Acrobat Reader*, conseguimos verificar como "metadados" administrativos a data de criação: 31/08/2018, às 17:13:20. Já como "metadados" descritivos, uma informação nos chamou a atenção: o autor do arquivo analisado era uma grande empresa de logística que, por óbvio, possuía interesse contrário a qualquer tipo de suspensão do serviço de transporte por parte dos caminhoneiros, razão pela qual conseguimos classificar a convocação como *Fake News*.

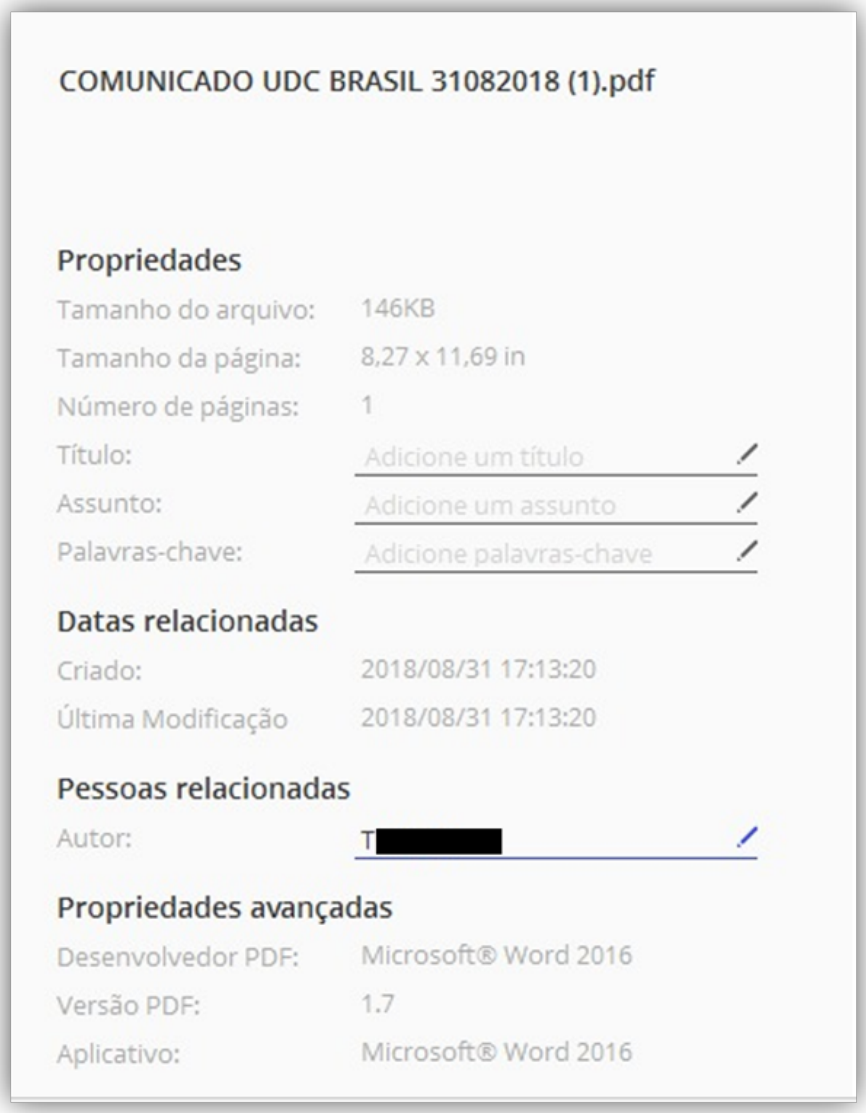


Figura nº 05. Arquivo tipo PDF analisado com a preservação do metadado descritivo do autor do documento

2.3. ESTUDO DE CASO 3.

Em meados de outubro de 2018 o *WhatsApp* habilitou a função envio de stikers (figurinhas). Trata-se da possibilidade de envio de arquivos de mídia do tipo WebP[10] com recurso que possibilita ao usuário do aplicaitivo a visualização da mídia independe do usuário salvar em seu dispositivo.

Este tipo de mídia foi criado recentemente pelo Google e busca oferecer tamanhos de arquivo menores para compressão com e sem perda a uma qualidade visual aceitável. O Google também usa em sites de produção, como o Google Play e o YouTube. Outras plataformas também já utilizam este formato de compressão destacando-se o Netflix, Amazon, Quora, Yahoo, Walmart, Ebay, The Guardian, Fortune e USA Today com WebP para navegadores compatíveis.

Importante destacar que este formato do arquivo WebP é compatível com a preservação dos "metadados" de foto EXIF e "metadados" do documento de XMP digital. Ou seja, em que pese haver maior compressão dos arquivos, ainda assim é capaz de preservar e trafegar os "metadados".

Com base nessas constatações, passamos a verificar a possibilidade deste tipo de mída, ainda que enviada via aplicativo *WhatsApp*, preservar seus "metadados". Para tanto, utilizamos o aplicativo *WhatsApp* para análise dos "metadados" dos stikers. Também utilizamos o aplicativo "Criar figurinhas para *WhatsApp* – WAStickerApps" para gerar os stikers. Importante recordar que estes arquivos são do tipo mídia, cuja extensão é a WebP.

Assim, através de um dispositivo com sistema operacional Android criamos um stiker de uma foto do Professor Dr. Walter Aranha Capanema e o salvamos no álbum cujo atributo descritivo criador foi denominado de "Guilherme Caselli". Após, integramos o stiker ao aplicativo *WhatsApp*, conforme imagem que segue. Interessante observar que, na imagem ficou gravado o metadado administrativo de nome "Guilherme Caselli".

Notamos também que, por mais que os usuários salvem a imagem recbida como favoritos em seus dispostivos, replicando-a em outro momento, ainda assim, ao clicar em cima do stiker aparecerá o nome de criador do arquivo. No nosso exemplo: "Guilherme Caselli".

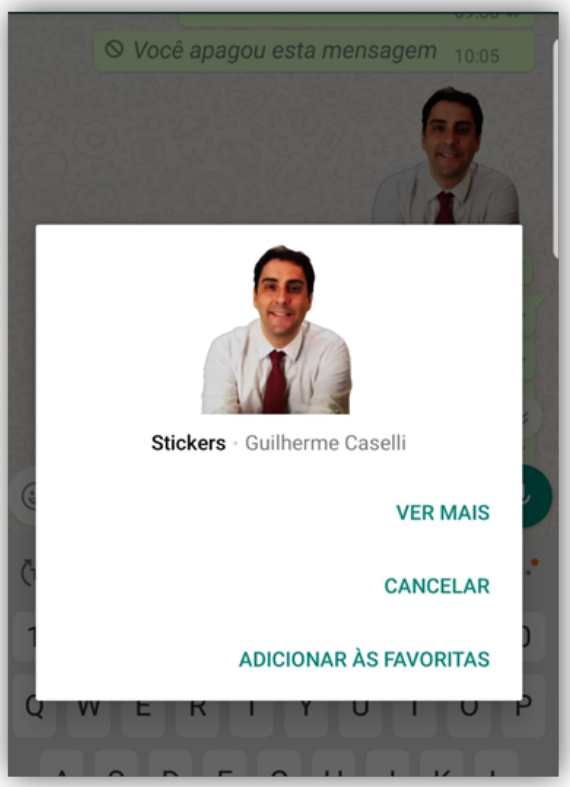


Figura 06. Visualização do metadado descritivo do autor da criação – Guilherme Caselli

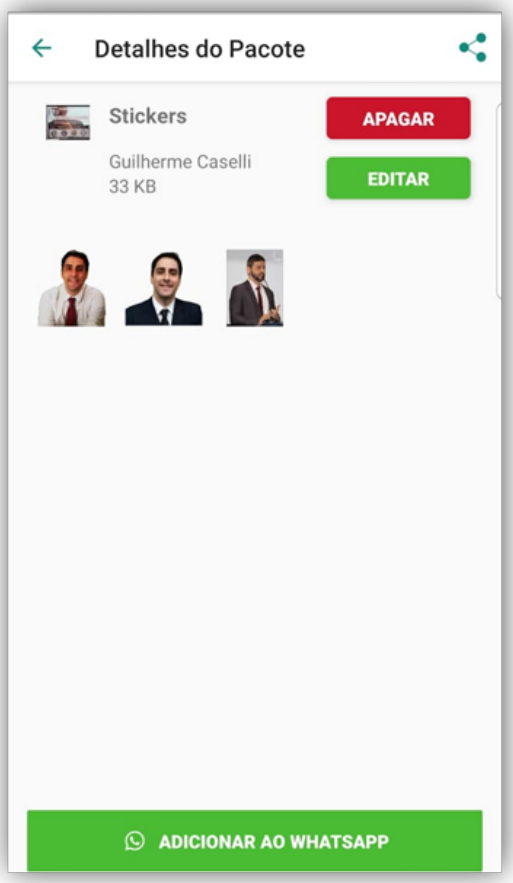


Figura 07. integração do stikers criado ao whstapp.

Em colaboração com o presente artigo, o Professor Dr. Walter Capanema criou um stikers com a imagem do Professor Dr. Fabrício Rabelo Patury. Notem que o Dr. Capanema atribuiu como nome do "álbum" a palavra "professores". Como atribuito "criador" o metadado descritivo "Walter Capanema".

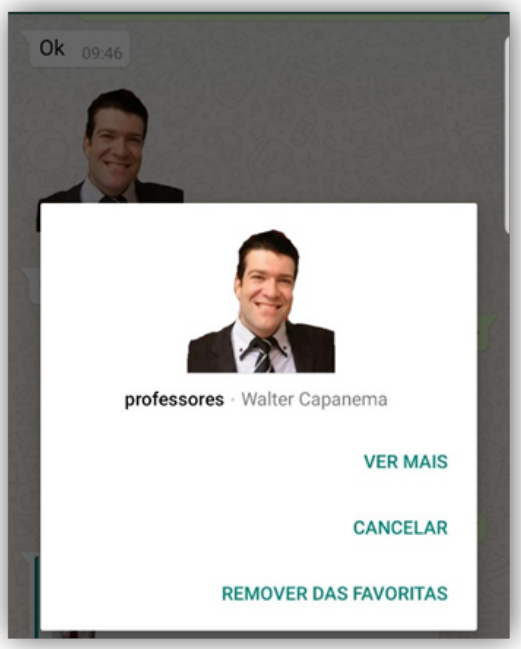


Figura 07. Visualização do metadado descritivo do álbum: "professores" e do autor da criação – Walter Capanema.

Também realizamos a análise dos arquivos com o programa HEX EDITOR NEO. As pesquisas comprovam que os arquivos de mídia WebP, em formato stikers ou figurinhas transitados pelo *WhatsApp* preservam os "metadados" de criação. Reparem na imagem abaixo destacada a individualização do nome atribuído como autor (grifamos) da mídia: "Guilherme Caselli"

Ainda, através desta metodologia de análise foi possível verificar, inclusive, a preservação da indicação do tipo do aplicativo utilizado, inclusive com o endereço eletrônico da loja de aplicativos da Google de onde este utilitário foi adquirido.

```
000036d0  52 a2 cf 81  91 e8 00 00   45 58 49 46  30 01 00 00   R¢Ï ‘è..EXIF0...
000036e0  49 49 2a 00  08 00 00 00   01 00 41 57  07 00 1a 01   II*.......AW....
000036f0  00 00 16 00  00 00 7b 22   73 74 69 63  6b 65 72 2d   ......{"sticker-
00003700  70 61 63 6b  2d 69 64 22   3a 22 63 6f  6d 2e 65 61   pack-id":"com.ea
00003710  73 79 63 6f  64 65 73 2e   73 74 69 63  6b 65 72 63   sycodes.stickerc
00003720  72 65 61 74  6f 72 2e 73   74 69 63 6b  65 72 63 6f   reator.stickerco
00003730  6e 74 65 6e  74 70 72 6f   76 69 64 65  72 20 33 22   ntentprovider 3"
00003740  2c 22 73 74  69 63 6b 65   72 2d 70 61  63 6b 2d 6e   ,"sticker-pack-n
00003750  61 6d 65 22  3a 22 53 74   69 63 6b 65  72 73 22 2c   ame":"Stickers",
00003760  22 73 74 69  63 6b 65 72   2d 70 61 63  6b 2d 70 75   "sticker-pack-pu
00003770  62 6c 69 73  68 65 72 22   3a 22 47 75  69 6c 68 65   blisher":"Guilhe
00003780  72 6d 65 20  43 61 73 65   6c 6c 69 22  2c 22 61 6e   rme Caselli","an
00003790  64 72 6f 69  64 2d 61 70   70 2d 73 74  6f 72 65 2d   droid-app-store-
000037a0  6c 69 6e 6b  22 3a 22 68   74 74 70 73  3a 5c 2f 5c   link":"https:\/\
000037b0  2f 70 6c 61  79 2e 67 6f   6f 67 6c 65  2e 63 6f 6d   /play.google.com
000037c0  5c 2f 73 74  6f 72 65 5c   2f 61 70 70  73 5c 2f 64   \/store\/apps\/d
000037d0  65 74 61 69  6c 73 3f 69   64 3d 63 6f  6d 2e 65 61   etails?id=com.ea
000037e0  73 79 63 6f  64 65 73 2e   73 74 69 63  6b 65 72 63   sycodes.stickerc
000037f0  72 65 61 74  6f 72 22 2c   22 69 6f 73  2d 61 70 70   reator","ios-app
00003800  2d 73 74 6f  72 65 2d 6c   69 6e 6b 22  3a 22 22 7d   -store-link":""}
```

Figura 08. Visualização via hexadecimal dos "metadados" descritivo do autor: "Guilherme Caselli" e a indicação do aplicativo acompanhado da *url* da loja da Googleplay.

Realizamos os mesmos testes nos arquivos de mídia do tipo WebP criados pelo Professor Dr. Walter Capanema. O resultado foi o seguinte: preservação dos "metadados" descritivos atribuídos ao album onde as imagens foram adicionadas *(sticker-pack-name)* "professores". Também foram preservados dos "metadados" descritivos indicativos do autor "Walter Capanema", assim como a indicação do aplicativo e o endereço da loja da Google onde o utilitário foi adquirido, conforme presente na figura abaixo destacada:

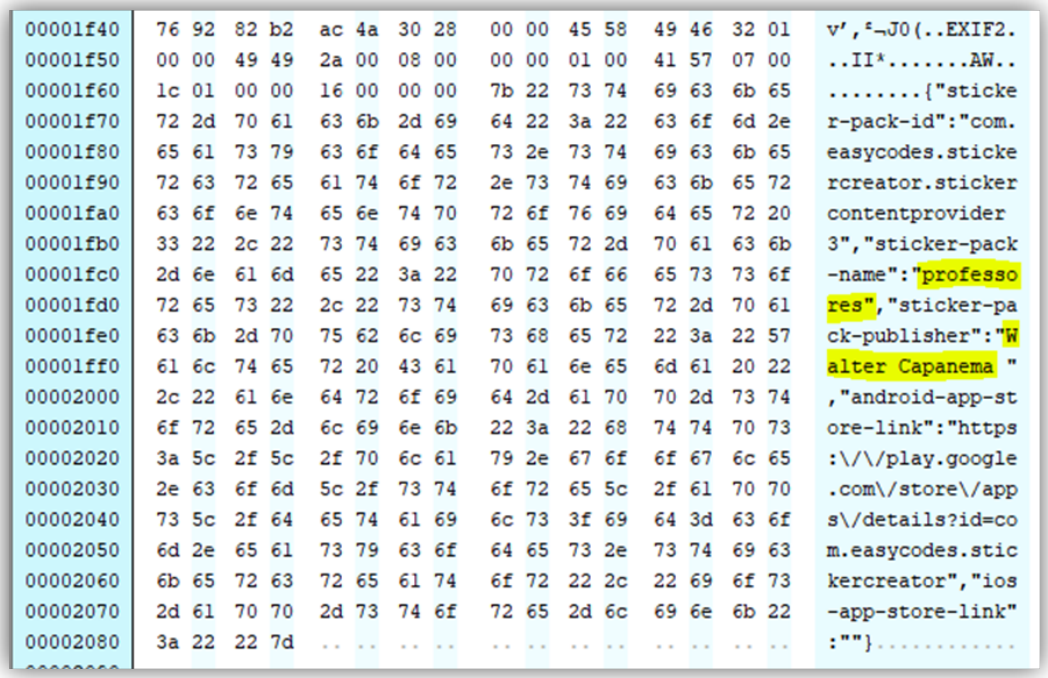


Figura 09. Visualização via hexadecimal dos "metadados" descritivo do álbum: "professores"; autor: "Walter Capanema" e a indicação do aplicativo acompanhado da *url* da loja da Googleplay.

Por fim, realizamos o mesmo teste com um stiker que criamos na data de 09 de dezembro de 2019 com a imagem do Delegado de Polícia Dr. Alexandre Bolonha. Atribuímos ao álbum o nome "eu" e para o criador, o mesmo nome: "eu".

Interessante notar que, após a criação e envio da imagem, excluímos a mídia do nosso dispositivo. Contudo, mesmo após 105 dias, a imagem permace acessível e visível no aplicativo *WhatsApp* com os atributos preservados (grifamos a imagem):

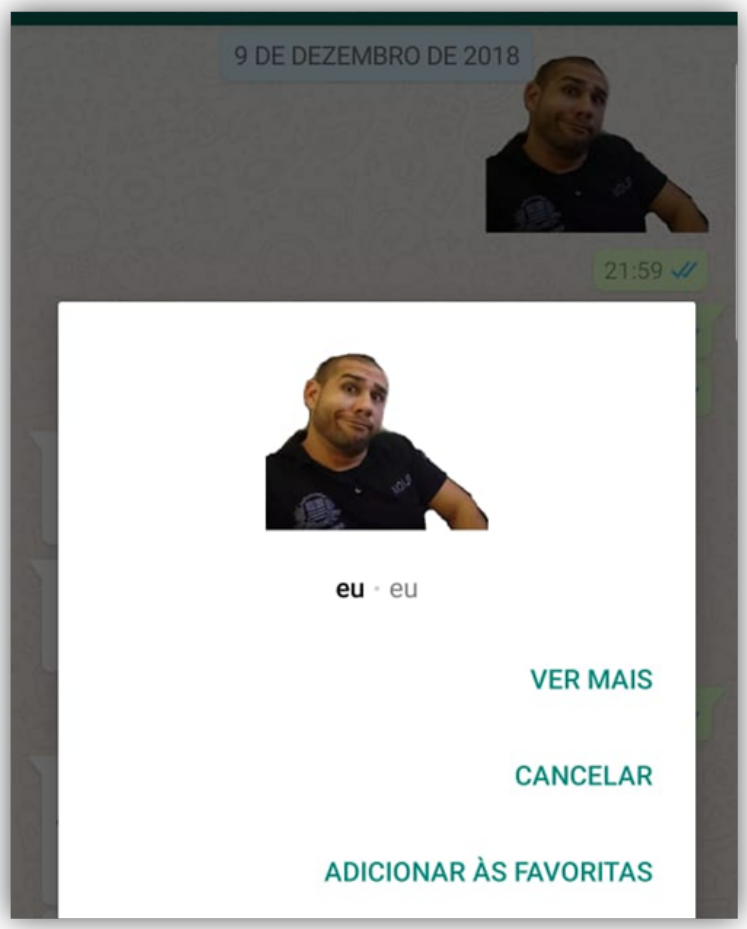


Figura 10. Visualização via hexadecimal dos "metadados" descritivo do álbum: "eu"; autor: "eu" e a indicação do aplicativo acompanhado da url da loja da Googleplay.

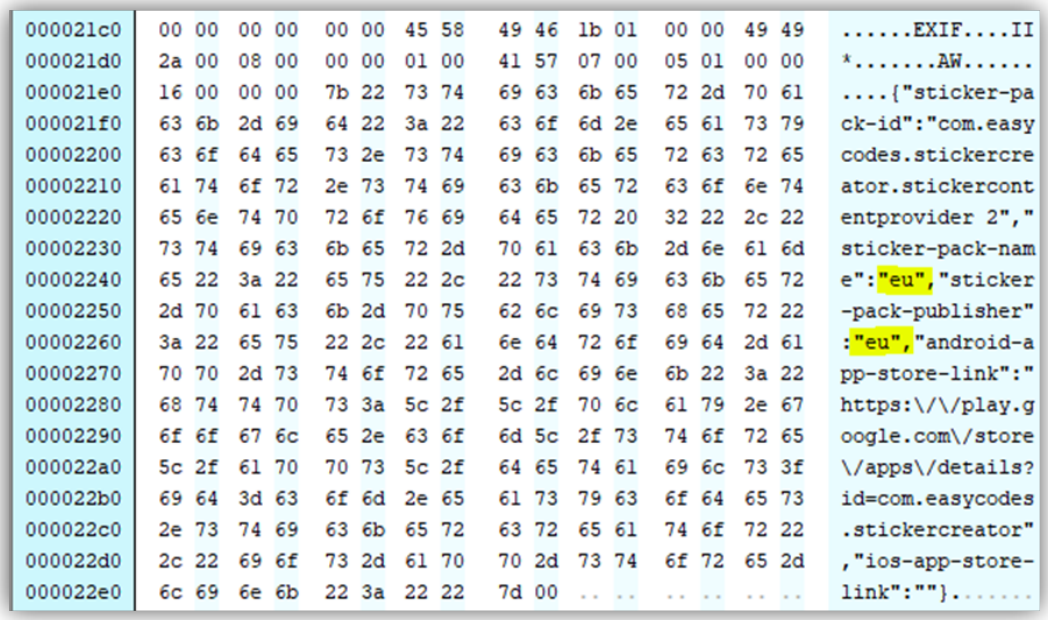


Figura 11. Visualização via hexadecimal dos "metadados" descritivo do álbum: "eu"; autor: "eu" e a indicação do aplicativo acompanhado da url da loja da Googleplay.

Ou seja, preservação dos "metadados" descritivos atribuídos ao album onde as imagens foram adicionadas *(sticker-pack-name)* "eu" e indicativos do autor: "eu". Ainda, o endereço da loja d Google onde o aplicativo foi adquirido.

CONCLUSÃO:

Através das pesquisas realizadas com documentos e arquivos de mídias transitados pelo servidor do *WhatsApp* e arrecadados diretamente no aplicativo ou através do serviço de cloud, independente da fatia amostral utilizada, conseguimos positivar a existência de atributos de "metadados" capazes de apontar, ainda que de forma rasa, o autor do arquivo.

É cediço que a empresa *WhatsApp* após muitos embates jurídicos passou a fornecer dados formais relacionados aos usuários de seus serviços, bem como procedeu a colocação em *blacklist* do *hash* da criptografia de arquivos apontados pelas Autoridade Públicas como de conteúdo ilícito. Porém somente estas informações não são suficientes quando a ótica investigatória recai sobre documentos e arquivos de mídias transitados em seus serviços.

Desta forma, em consonância aos termos e serviços em que declaram diretamente coletar, usar, reter e compartilhar dados as indagações ainda sem resposta são: Por que o *WhatsApp* não esclarece quais são os dados dos usuários coletados, utilizados, retidos e compartilhados de seus usuários? Por que a empresa não fornece para as Autoridades Públicas informações sobre os usuários de seu sistema que primeiro encaminhou os documentos ou arquivos de mídia com conteúdo ilícito.

Por fim, ainda que a empresa *WhatsApp*, por mera suposição acadêmica, ainda não preserve os dados do usuário que primeiro compartilhou um arquivo, por quê, ciente da existência da execução de diversos crimes realizados através dos seus serviços, não altera a configuração de seus servidores para preservá-los e assim poder contribuir com as Autoridades Públicas no combate à criminalidade. Com a plavra a corporação detentora das respostas.

Bibliografia

Supremo Tribunal Federal STF. ARGÜIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL – ADPF 4000331-63.2016.1.00.0000 DF – DISTRITO FEDERAL 4000331-63.2016.1.00.0000. Rel. Min. Edson Fachin. Em de outubro de 2016. Disponível em <https://stf.jusbrasil.com.br/jurisprudencia/392886255/arguicao-de-descumprimento-de-preceito-fundamental-adpf-403-df-distrito-federal-4000331-6320161000000>. Acesso: 20 mar. 2019.

2. Supremo Tribunal Federal STF. ATA DA AUDIÊNCIA PÚBLICA – MARCO CIVIL DA INTERNET AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5.527. Rel. Min. Rosa Weber e BLOQUEIO JUDICIAL DO *WHATSAPP*. ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403. Rel. Min. Edson Fachin. 05 de junho de 2017. Disponível em:< http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdo*WhatsApp*.pdf>. Acesso 22 mar. 2019.

3. *WHATSAPP*. Informações para as autoridades policiais. Disponível em: <https://faq.*WhatsApp*.com/26000050>. Acesso: 23 mar. 2019.

4. CASELLI, G. ; BARRETO, A. G. ; Emerson Wendt . Investigação Digital em Fontes Abertas. 1. ed. Rio de Janeiro: brasport, 2017. v. 1. 280p .

5. *WHATSAPP*. Informação Legal. Terms of Service. Disponível em: <https://www.*WhatsApp*.com/legal/#Privacy>. Acesso: 23 mar. 2019.

6. RILEY, Jenn. UNDERSTANDING METADATA WHAT IS METADATA, AND WHAT IS IT FOR? Disponível em: <https://groups.niso.org/apps/group_public/download.php/17446/Understanding%20Metadata.pdf>. Acesso em: 23 mar. 2019.

7. PSAFE. 8,8 milhões de brasileiros foram impactados por notícias falsas no primeiro trimestre de 2018, estima dfndr lab. Disponível em: <https://www.psafe.com/dfndr-lab/pt-br/brasileiros-noticias-falsas-2018/>. Acesso: 23 mar. 2019.

8. GUESS, Andrew; REIFLER, Jason; NYHAN, Brendan. Selective Exposure to Misinformation:Evidence from the consumption of *Fake News* during the 2016 U.S. presidential campaign. Disponível em:<https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf>. Acesso: 23 mar. 2019.

9. Wabetainfo. *WhatsApp* beta for Android 2.19.73: what's new?. 13 de Março de 2019. Disponível em: <https://wabetainfo.com/*WhatsApp*-beta-for-android-2-19-73-whats-new/>. Acesso: 23 mar. 2019.

10. OSMANI, Addy. Automatizar a otimização da imagem. Disponível em: <https://wabetainfo.com/*WhatsApp*-beta-for-android-2-19-73-whats-new/>. Acesso: 22 mar. 2019.

**Guilherme Caselli é delegado da Polícia Civil de São Paulo.*

Juristas


MANDATO PARA MINISTRO DO STF
OS MINISTROS DO SUPREMO DEVERIAM TER MANDATO?
SE SIM, CURTA O POST.
SE NÃO, COMENTE COM O MOTIVO.
JURISTAS


QUESTÕES EM CONCURSO PÚBLICO SÓ SÃO ANULADAS CASO HAJA DIVERGÊNCIA COM EDITAL
JURISTAS


USAR FOTOS SEM CRÉDITO PARA FINS LUCRATIVOS CARACTERIZA DANO MORAL
JURISTAS


REGISTRO EM BLOCKCHAIN É PROVA VÁLIDA
BlockChain
JURISTAS


SUBESTAÇÕES DE TREM SÃO LOCAIS DE TRABALHO DE RISCO, DECIDE TST
JURISTAS


SENTENÇA DE IMPRONÚNCIA NÃO PODE SER REFORMADA COM IN DUBIO PRO SOCIETATE
JURISTAS