**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**

**REVISTA SOCIEDADE CIENTÍFICA, VOLUME 7, NÚMERO 1, ANO 2024**

*ARTIGO ORIGINAL*

# Mídia ilícita no WhatsApp: uma análise do julgamento da representação eleitoral nº 601686-42.2018 à luz do Marco Civil da internet

*Jorge Messias de Brito*[1]

**Como Citar:**
*DE BRITO, Jorge Messias*. Mídia ilícita no WhatsApp: uma análise da Representação Eleitoral nº 601686-42.2018 à luz do Marco Civil da Internet. Revista Sociedade Científica, vol.7, n.1, p.1920-1942, 2024. https://doi.org/10.61411/rsc202441917

**DOI:** 10.61411/rsc202441917

**Área do conhecimento:** Direito.

**Sub-área:** Direito digital.

**Palavras-chaves**: WhatsApp; Fake news; Crime cibernético; Marco Civil da Internet; Representação Eleitoral nº 601686-42.2018.

**Publicado**: 15 de abril de 2024.

## Resumo

Trata-se de artigo científico pautado em pesquisa documental descritiva, com análise de decisão judicial, sob o título: "Mídia ilícita do WhastsApp: uma análise do julgamento da Representação Eleitoral nº 601686-42.2018 à luz do Marco Civil da Internet". O mensageiro instantâneo WhatsApp tem negado prestar informações às autoridades judiciárias do país, com a justificativa de que, por utilizar criptografia de ponta-a-ponta não consegue ter acesso às informações trocadas entre seus usuários. Ocorre que a Lei 12.965/2014 (Marco Civil da Internet - MCI) é clara quanto à obrigatoriedade da guarda dos registros de acesso a aplicação de internet. Este artigo faz uma breve análise do julgamento da Representação Eleitoral nº 601686-42.2018 à luz do Marco Civil da Internet, explicitando alguns caminhos alternativos para se chegar à autoria de um conteúdo ilícito compartilhado no aplicativo WhatsApp.

## 1. Introdução

As tecnologias da informação e comunicação têm, cada vez mais, adentrado nos lares brasileiros. Apesar das diversas tecnologias disponíveis, uma delas tem contribuído consideravelmente para a inclusão digital no Brasil: o WhatsApp.

O WhatsApp é o mensageiro instantâneo mais utilizado no Brasil. Conforme dados do *Statista*[2] (janeiro/2024), o aplicativo possuía no país o maior mercado fora da Ásia, o terceiro maior do mundo, com mais de 96% da sua população sendo usuária ativa do mensageiro. É, de longe, a plataforma social mais usada no Brasil.

Além de mensagens de texto, o WhatsApp permite o envio de imagens, áudios,

[1]Bacharel em Direito - Centro Universitário FG (UNIFG/BA). Tecnólogo em Informática – Faculdade Prudente de Moraes (FPM/SP). ✉

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



vídeos e documentos entre seus usuários, bem como, a realização de ligações gratuitas e pagamento/transferência de valores.

Em junho de 2020 a empresa disponibilizou no Brasil, de forma integrada ao mensageiro, recurso para envio/transferência de dinheiro entre seus usuários, no entanto a ideia não foi bem vista pelo Banco Central do Brasil, que temia pela fragmentação do mercado de pagamentos e concentração em agente específico[3]. Em novembro de 2020, o Banco Central lançou, oficialmente, o PIX - recurso de pagamento/transferência instantânea de valores[4].

## 1.1 Suspensões do WhatsApp no Brasil

Em fevereiro de 2015 o WhatsApp foi suspenso no território brasileiro por se negar a fornecer informações à Justiça do Piauí para apuração de um crime de pedofilia na capital Teresina[5]. No entanto, a decisão monocrática logo foi derrubada pelo Tribunal de Justiça do Estado[6].

No ano de 2016, o aplicativo teve seu funcionamento novamente suspenso pela Justiça de Sergipe[7]. A decisão foi fruto de um pedido de medida cautelar da Polícia Federal, em razão do Facebook, proprietário do WhatsApp, não cumprir decisão judicial de compartilhar informações que subsidiariam uma investigação criminal. A decisão não vingou por muito tempo.

Em julho de 2016, o WhatsApp voltou a ser suspenso por decisão da Justiça do Rio de Janeiro[8]. Contudo, no mesmo o dia, o Supremo Tribunal Federal suspendeu a decisão, liberando o uso do aplicativo no país[9].

Ao que se percebe, o WhatsApp deixou de ser um mero aplicativo privado, transformando-se num serviço de relevante interesse público. Vale mencionar que até mesmo o Judiciário brasileiro se utiliza dos seus serviços. Um exemplo disso é o "Juízo 100% Digital", regulamentado pelo TJBA[10] a partir da Resolução CNJ nº 345/2020[11].

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



## 2. Julgamento da Representação Eleitoral nº 0601686-42.2018.6.00.0000 (TSE)

Um exemplo prático do comportamento dos provedores de aplicação quanto ao fornecimento de dados de seus usuários pode ser observado no julgamento da Representação Eleitoral nº 0601686-42.2018.6.00.0000 (TSE).

A ação foi proposta contra a Google Brasil Internet Ltda., para remoção de conteúdo irregular na internet (vídeo publicado no Youtube), nos termos do art. 33, § 5º, da Res.-TSE nº 23.551/2017.

O Ministério Público Eleitoral ingressou no feito pleiteando, também, a inclusão da empresa Whatsapp Inc. no polo passivo da demanda, tendo em vista que o vídeo teria sido largamente difundido no aplicativo de mensagem instantânea, pugnando, ainda, pela identificação dos responsáveis pela infração às normas eleitorais e, em segundo momento, responsabilizá-los pela inobservância do ordenamento jurídico, na forma do art. 57-H, da Lei nº 9.504/97.

### 2.1 Cumprimento da determinação judicial pelo Youtube

Foi deferido pedido liminar para remoção dos vídeos da plataforma do Youtube, no prazo de 24h, referentes às URLs abaixo, na forma da Res.-TSE nº 23.551/2017:

**Imagem 01: Parte da decisão liminar deferindo pedido de remoção dos vídeos**

Ante o exposto, **defiro a liminar pleiteada**, para determinar a Google Brasil Internet Ltda. que, no prazo de 24h, proceda à remoção dos conteúdos vinculados às seguintes URLs:

https://www.youtube.com/watch?v=5VrKQWNC0r4

https://m.youtube.com/watch?v=FD6oM68KeKY

https://m.youtube.com/watch?v=jWNcg3WIl1Y

https://m.youtube.com/watch?v=w63KvX0sie4

https://m.youtube.com/watch?v=z5EkUtoAapg

https://m.youtube.com/watch?v=9hOedFUkb1w

https://m.youtube.com/watch?v=3kP-_8AUXqc

https://m.youtube.com/watch?v=miLgDpWM7dQ

**Fonte: (Processo nº 0601686-42.2018.6.00.0000)**

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



O Ministério Público Eleitoral pleiteou, ainda, a identificação dos IPs que criaram os perfis responsáveis pelas postagens dos vídeos na plataforma Youtube, com base nas respectivas URLs informadas (Imagem 01), bem como, a identificação do usuário responsável pelo mais remoto *upload* do vídeo no aplicativo WhatsApp e o bloqueio do encaminhamento sucessivo do vídeo, entre outros.

**Imagem 02: Pedidos do MP**

(a) intimação da Google Brasil Internet Ltda. para apresentação de defesa e encaminhamento das seguintes informações: (a.1) identificação do número de IP da conexão utilizada no cadastro inicial dos perfis responsáveis pelas contas representadas; (a.2) dados cadastrais dos responsáveis, nos termos do art. 10, § 1º, da Lei nº 12.965/14; (a.3) registros de acesso à aplicação de internet eventualmente disponíveis (art. 34 da Resolução TSE nº 23.551/2017);

(b) intimação do WhatsApp Inc./Law Enforcement & Safety Manager, por meio do canal de comunicação previsto no art. 9º da Resolução TSE nº 23.551/2017, determinando-se: (b.1) bloqueio do encaminhamento sucessivo da URL https://mmg-fna.whatsapp.net/d/f/AkhlLOVq9DnbxiZhu3Ieu2tS9NTg-My7hw4SZQn4qAPW.enc no aplicativo *WhatsApp*; (b.2) identificação do algoritmo de Hash do referido arquivo; (b.3) rastreamento do mais remoto *upload* do arquivo e identificação do usuário responsável;

(c) citação do responsável ou dos responsáveis pela divulgação inicial do vídeo para apresentação de defesa (art. 8º da Resolução TSE nº 23.547/2017);

(d) aplicação de multa aos responsáveis pelas publicações, tanto no *YouTube* quanto no *WhatsApp* (art. 30 da Resolução TSE nº 23.551/2017), caso configurem, ao final do processo, propaganda eleitoral ilícita ou, ainda, manifestação político-eleitoral não autorizada.

**Fonte: (Processo 0601686-42.2018.6.00.0000, Id. 532131)**

A representada Google atendeu às requisições do Poder Judiciário, removendo os conteúdos vinculados às URLs informadas e fornecendo as informações requeridas, cuja resposta seguiu o padrão abaixo:

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



**Imagem 03: Dados de um dos usuários responsáveis pela postagem do vídeo.**

```
User name:Bolsomito Tv
External Id:E9vVa_LtWmINdbgBn4-L-g
URL:http://www.youtube.com/channel/UCE9vVa_LtWmINdbgBn4-L-g
E-mail:lucashcm_6@hotmail.com (confirmed)
User Status:USER_ACTIVE
Creation Date:November 30, 2015 at 2:50 AM UTC
Creation IP:234.224.0.100
First Name:Bolsomito
Last Name:Tv
User Provided Country:Brazil
Date of Birth:UNAVAILABLE


############## IP LOGS ###############

+-------------+----------------------------------+----------------------
------------------+
| Action Type | Date                             | IP address
|
+-------------+----------------------------------+----------------------
------------------+
| Login       | October 12, 2018 at 1:25 AM UTC | 177.157.149.237
|
| Login       | October 12, 2018 at 1:54 AM UTC |
2804:7f1:4480:9586:f1ac:294a:7e8:d768 |
+-------------+----------------------------------+----------------------
------------------+


Google Confidential & Proprietary

Video Data

        Time Created          Encrypted ID     Upload IP     Uploader External User ID
October 12, 2018 at 1:34 AM UTC miLgDpWM7dQ 177.157.149.237 E9vVa_LtWmINdbgBn4-L-g
Google Confidential & Proprietary
```

**Fonte: (Processo 0601686-42.2018.6.00.0000)**

Alguns dados constantes do cadastro do usuário junto à plataforma Youtube são pouco relevantes para a identificação real do utilizador do serviço, a exemplo do *User name* (nome do usuário). No entanto, há dados bastante relevantes, como o endereço IP que criou a conta no Youtube e o endereço de e-mail utilizado para validação da conta. O histórico de login do usuário (IP Logs) também pode ajudar na identificação.

Como o Youtube e o WhatsApp se inserem na categoria de provedores de aplicação, estes não têm acesso à identidade civil do usuário por detrás dos endereços IPs utilizados para a postagem dos vídeos, nos termos do MCI. Tal identificação cabe aos provedores de acesso.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



Com os dados dos IPs que criaram as contas/perfis no Youtube, o MP requereu a identificação das pessoas por detrás de cada IP, junto aos provedores de acesso Tim Celular, Telefônica, Telemar, Viveiros e Araújo Prov. de Internet, Atento Telecom, Claro, Level3 Comunicações e Way.com Provedor.

Após as respostas das empresas de telefonia e demais provedores de internet, oito pessoas foram identificadas e citadas para integrarem o polo passivo da ação.

## 2.2 Cumprimento da determinação judicial pelo WhatsApp

Em relação ao WhatsApp, o Min. Relator proferiu a seguinte decisão:

**Imagem 04: Decisão em face do WhatsApp**

Determino, também, a WhatsApp Inc. – Law Enforcement & Safety Manager que ***(a)*** efetue, no prazo de 24h, o bloqueio do encaminhamento sucessivo da URL https://mmgfna.whatsapp.net/d/f/AkhlLOVq9DnbxiZhu3Ieu2tS9NTg-My7hw4SZQn4qAPW.enc no aplicativo WhatsApp; ***(b)*** proceda, no prazo de 48h, à identificação do algoritmo de Hash do referido arquivo; e ***(c)*** realize, igualmente no prazo de 48h, o rastreamento do mais remoto *upload* do arquivo e identificação do usuário responsável.

Por fim, determino a citação de WhatsApp Inc. – Law Enforcement & Safety Manager para que apresente defesa.

**Fonte: (0601686-42.2018.6.00.0000)**

O Ministério Público Eleitoral informou que:

> Após ser intimado do teor da decisão, o advogado da representada WhatsApp Inc. - Law Enforcement & Safety Manager, entrou em contato com a Procuradoria-Geral Eleitoral para explicar que **o efetivo cumprimento da ordem judicial pressupõe o recebimento do vídeo impugnado, pelo próprio aplicativo Whatsapp**, em uma conta específica criada para empresa para tanto, a fim de que se confirme o teor do vídeo a ser bloqueado.
>
> Objetivando propiciar o cumprimento da decisão, e considerando as questões técnicas sustentadas pelo causídico, o signatário remeteu o arquivo de mídia impugnado, via aplicativo, para o número indicado.

Em relação ao cumprimento da decisão liminar, o WhatsApp informou que:

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



> recebeu o arquivo de mídia em discussão via aplicativo WhatsApp, bem como a sua devida identificação, e **cumpriu a determinação judicial na medida em que é tecnologicamente viável, dento do prazo que lhe foi concedido de 24 horas**.
>
> Adotadas as providências para a cessação da divulgação da propaganda entendida como irregular, não há de se falar em responsabilização do WhatsApp, nos termos do artigo 57-F da Lei 9.504/19971.

O WhatsApp reiterou, ainda, em sua defesa, que:

> cumpriu tempestivamente a determinação judicial (liminar) na medida em que é tecnologicamente viável.
>
> O WhatsApp somente consegue identificar um conteúdo circulado em sua plataforma através do **código identificador** a ser fornecido pelo Representante - **usuário que tem acesso ao conteúdo das mensagens**.
>
> No caso dos autos, como esclarecido na petição ID n° 533606, o WhatsApp recebeu o arquivo de mídia em discussão via aplicativo WhatsApp, **bem como a identificação já fornecida pelo Representante**, e cumpriu a determinação judicial na medida em que é tecnologicamente viável, restando prejudicada a requisição ministerial.
>
> Quanto aos demais dados requisitados, o WhatsApp esclarece que é essencial a indicação precisa de qual é o **número da conta WhatsApp vinculada** aos dados que se pretende sejam fornecidos.
>
> Nos termos do artigo 320 do CPC/2015 e do artigo 19, parágrafo 1°, do Marco Civil da Internet, é essencial a identificação clara e específica do conteúdo apontado como infringente na internet. Diferentemente de conteúdos publicados na Web - cujo conteúdo é acessível e está disponível através de uma URL -, **a indicação precisa e clara para fornecimento de dados e registros eletrônicos no WhatsApp se dá através do número de telefone utilizado para o registro.**
>
> Não há, contudo, viabilidade técnica de fornecer tais informações sem a **precisa identificação do número completo** do telefone celular registrado no Brasil: +55 (DDD) NÚMERO DE TELEFONE CELULAR.

Por se tratar de plataforma de troca de mensagens com criptografia de ponta-a-ponta, o WhatsApp afirma possuir técnica de registro de dados diferente da maioria dos

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



provedores de aplicação, como o Youtube e o Facebook. Nestes últimos, a publicação de uma mídia gera uma URL, **que é registrada em conjunto com o IP** do usuário responsável pelo envio, em obediência ao art. 15 do MCI.

Quando um usuário posta uma mídia no WhatsApp, o aplicativo faz o *upload* dessa mídia em seu servidor e gera um link (URL) correspondente. Quando essa mídia é repassada (compartilhada) a outros destinatários, estes apenas a carregam a partir do link originário. Esse link (e provavelmente o IP do usuário que o criou) fica armazenado nos servidores do WhatsApp.

Freitas (2019)[12], questiona "se o WhatsApp realmente não teria capacidade técnica de fornecer o endereço IP do usuário que fez o primeiro *upload* na plataforma", fazendo um comparativo com outros provedores de aplicação como o Google e Facebook:

**Imagem 05: Comparativo de registro de dados – whatsapp x outros provedores**

**Provedores de aplicações de Internet**

| Aplicação | Hospedagem de sites Google, Facebook etc | WhatsApp |
|---|---|---|
| **Autenticação** | Exige autenticação do usuário para upload de arquivos | Exige autenticação do usuário para upload de arquivos |
| **Endereço IP** | Conhece o endereço IP do terminal que está fazendo upload | Conhece o endereço IP do terminal que está fazendo upload |
| **URL** | Gera URL que pode ser usado como identificador inequívoco nos termos da Lei 12.965/14 Art. 19 Par. 10 | Gera URL que pode ser usado como identificador inequívoco nos termos da Lei 12.965/14 Art. 19 Par. 10 |
| **Guarda de registros de acesso** | **É obrigado a manter os registros de acesso por 6 meses nos termos da Lei 12.965/14 Art. 15** | **?** |

**Fonte: https://legis.senado.leg.br/sdleg-getter/documento/download/655c4226-698e-47fe-9deb-71e178bef7a5. Acesso em: 07/03/2024.**

O Direito Comparado poderá auxiliar na obtenção de entendimentos jurídicos já firmados em outros países quanto ao fornecimento de dados pelo aplicativo WhatsApp.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



O artigo 15 do MCI é claro ao estabelecer que tais provedores devem "manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento".

A *mens legis* do referido dispositivo é no sentido de que a guarda do registro de acesso a aplicação, serviço ou recurso da internet é obrigatória. Quando um usuário faz o *upload* de um arquivo para os servidores de hospedagem do WhatsApp, ele está usando um serviço/recurso da internet, e, portanto, o provedor tem a obrigação de registrar tal atividade, nos termos do inciso VIII, artigo 5º, do MCI (data e hora de uso da aplicação/recurso e o IP utilizado para tal).

Vale consignar que registrar a data e o tempo de uso de uma determinada aplicação com o correspondente endereço IP de quem a acessou não viola o sigilo das comunicações, visto que este ato não se traduz em conhecer o conteúdo acessado e o nome da pessoa por detrás do IP utilizado.

Ocorre que, quando o assunto é fornecer dados dos seus usuários, o WhatsApp tem dito que:

> As mensagens trocadas entre usuários do WhatsApp, incluindo conversas em grupo são protegidas por criptografia de ponta-a-ponta. A criptografia ponta-a-ponta significa que o processo de encriptação e de decriptação de todas as mensagens ocorre apenas no aparelho celular dos usuários.
>
> Em razão do atual sistema de criptografia do WhatsApp, as mensagens são criptografadas antes de passarem pelos servidores da empresa e, portanto, nem o WhatsApp, nem terceiros, conseguem ler ou ouvir as mensagens.
>
> Ademais, como não possui acesso ao aparelho celular de seus usuários, o WhatsApp não consegue remover arquivos de mídia já recebido por usuários.

No que se refere ao pedido de rastreamento do mais remoto *upload* de um arquivo e a identificação do usuário responsável ou de quem o tenha propagado, o WhatsApp argumenta que:

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



> em razão da criptografia ponta a ponta, o WhatsApp não consegue ler ou rastrear as mensagens transmitidas por seu aplicativo, impossibilitando a identificação do histórico de transmissão de uma mensagem. O WhatsApp, igualmente, não armazena informação sobre quem foi seu remetente originário. Trata-se, portanto, de obrigação impossível de ser adimplida.

A empresa defende que, nos termos do artigo 19 do MCI, não é responsável pela divulgação de conteúdo na plataforma e tampouco possui obrigação legal de monitoramento sobre as mensagens trocadas por terceiros. Faz menção ao seguinte precedente:

> Pretender que os provedores de aplicações de Internet tenham o dever de monitorar conteúdo elaborado pelos seus usuários, sob o pretexto de prevenir a divulgação de material eventualmente contrário à lei corresponderia a impedir a livre manifestação do pensamento e permitir a censura, em violação ao artigo 220 da Constituição Federal. (TRE/RR, Representação Eleitoral n° 0600885-87.2018.6.23.0000, Juíza Maria Aparecida Cury, j. 10.09.2018)

Nesse ponto, a plataforma Youtube tem tido mais cautela com o material que é veiculado em sua rede. O Youtube utiliza filtros (algoritmos e inteligência artificial) para análise de conteúdo impróprio (como incitação ao suicídio, à automutilação, nudez, conteúdo sexual, perigoso ou nocivo, entre outros)[13]. No que se refere a violações de direitos autorais, a plataforma tem utilizado as ferramentas *Content ID*[14] e *Copyright Match Tool*[15]

Poderia o WhatsApp se furtar a registrar/armazenar as informações referentes à "data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP"? Certamente que não. A criptografia de ponta-a-ponta não pode ser utilizada como desculpa para o descumprimento do art. 5º, VIII e art. 15, ambos do MCI.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



A principal lei que rege o ambiente virtual no país, Lei Federal 12.965/14[16], conhecida como Marco Civil da Internet - MCI "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil".

Com a finalidade de "formar conjunto probatório em processo judicial cível ou penal" a mencionada lei garante acesso a determinadas informações dos usuários de internet:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de **registros de conexão ou de registros de acesso a aplicações de internet**.

O MCI estabeleceu quais informações e por quanto tempo os provedores de internet deveriam guardar dos seus usuários. Os provedores de acesso/conexão estão obrigados à guarda dos registros de conexão pelo prazo de 1 (um) ano.

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Já os provedores de aplicação/conteúdo estão obrigados a manter os registros de acesso a aplicações pelo prazo de 6 (seis) meses.

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

O diploma legal definiu ainda o que se entende por registro de conexão e registro de acesso a aplicações de internet:

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



> **Art. 5º,**
>
> (...)
>
> **VI - registro de conexão**: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> (...)
>
> **VIII - registros de acesso a aplicações de internet**: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Certamente, o legislador poderia ter melhorado a redação dos incisos VI e VIII, acrescentando as informações de "porta lógica" quando o IP for nateado (compartilhado), bem como, poderia ter substituído a expressão "uma determinada aplicação de internet" por "um determinado recurso de internet".

Apesar das imprecisões, o MCI tem subsidiado a instrução probatória em várias ações judiciais, tendo como ponto de partida o seu artigo 22.

Como o WhatsApp não possui acesso ao conteúdo das mensagens trocadas entre seus usuários, cabe a quaisquer dos usuários participantes do diálogo realizarem o levantamento dos *metadados* correspondentes à mídia impugnada, através dos quais instruirão seus pedidos junto ao Poder Judiciário.

## 3. Buscando o autor de uma mídia ilícita do WhatsApp

Barreto (2020)[17], utilizando-se de metodologia apresentada pela Secretaria Nacional de Segurança Pública[18], explica como identificar a URL de encaminhamento de uma mídia publicada no WhatsApp. Para tal, faz uso do navegador Chrome e do Web WhatsApp (figuras 1 a 5):

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**




**Figura 1**

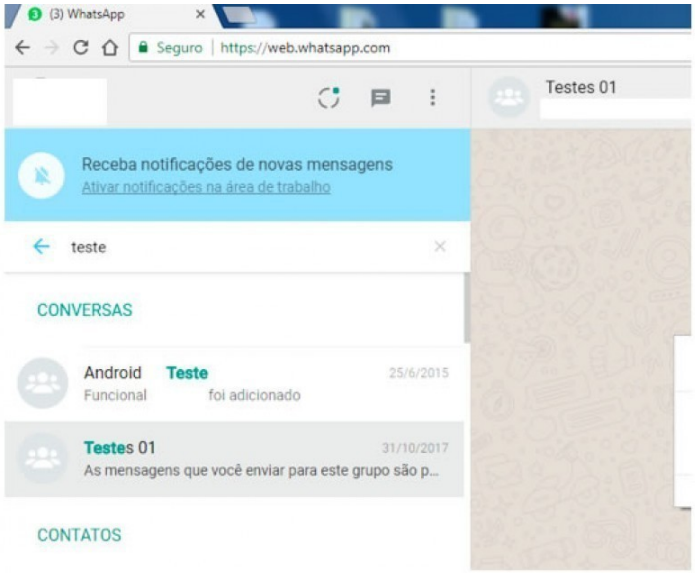



**Figura 2**

**Figuras 1 e 2. Abra o aplicativo WhtatsApp Web pelo navegador Google Chrome. Cria-se um novo grupo de usuários ("Testes 01") para fazer o encaminhamento da mídia ilícita. Essa ação é importante para possibilitar a rápida e segura identificação da URL do arquivo, uma vez que se o procedimento for feito em uma janela de diálogo já existente pode-se incorrer em erro, extraindo informações de arquivo diverso do pretendido.**

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



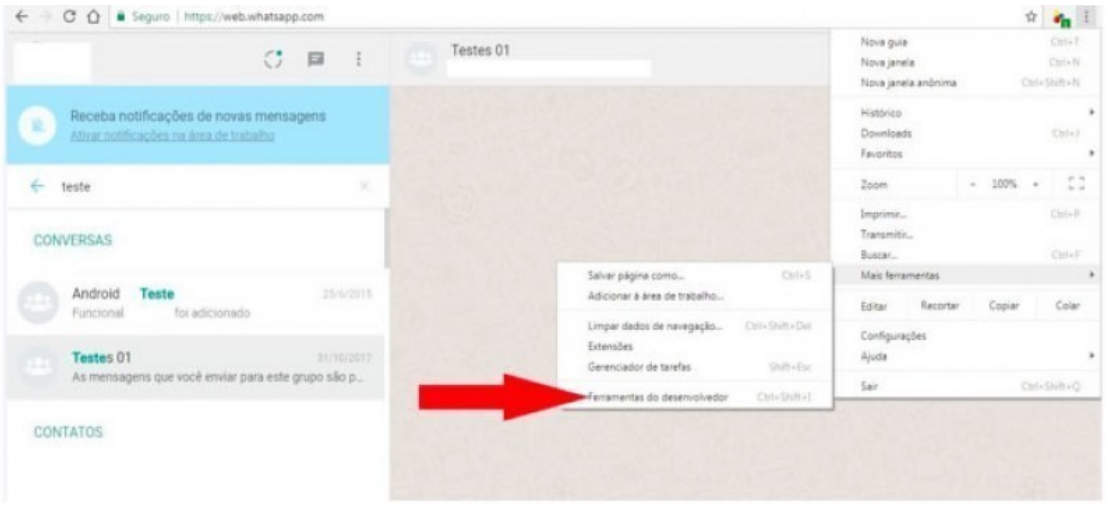



**Figura 3. Clique no ícone "Menu"( ) da barra de ferramentas do browser e em seguida acesse a guia "Mais ferramentas", após isto selecione "Ferramentas do desenvolvedor".**

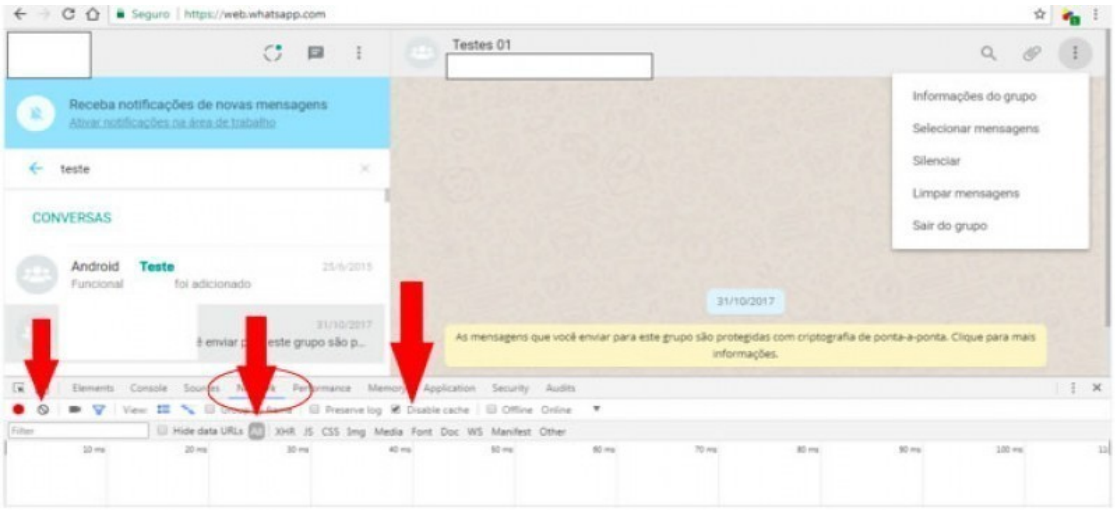



**Figura 4. Com a nova janela aberta na parte inferior da tela selecione o menu "Network" (círculo vermelho). Selecionado o menu "Network", marque a opção "disable cache", após isto selecione todos os arquivos clicando no botão "All" e promova a limpeza da guia clicando no ícone de "clear" ( ). Pronto, agora a mídia ilícita já pode ser enviada para o grupo de teste.**

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



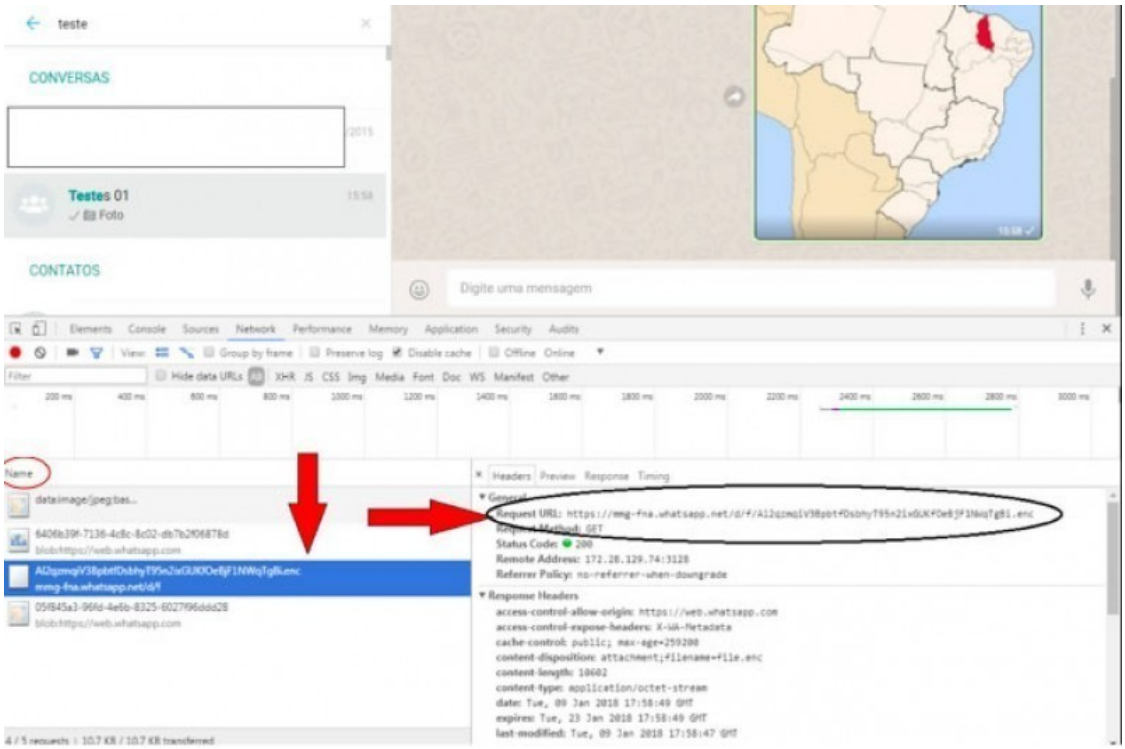



**Figura 5. Assim que o arquivo é carregado irão aparecer algumas URLs na aba "Name". A URL do arquivo encriptado será aquela com a transcrição <https://mmg-fna.whatsapp.net/d/f/**********.enc>. Ao selecionar o arquivo é possível copiar a URL na janela que se abrirá no lado direito da tela.**

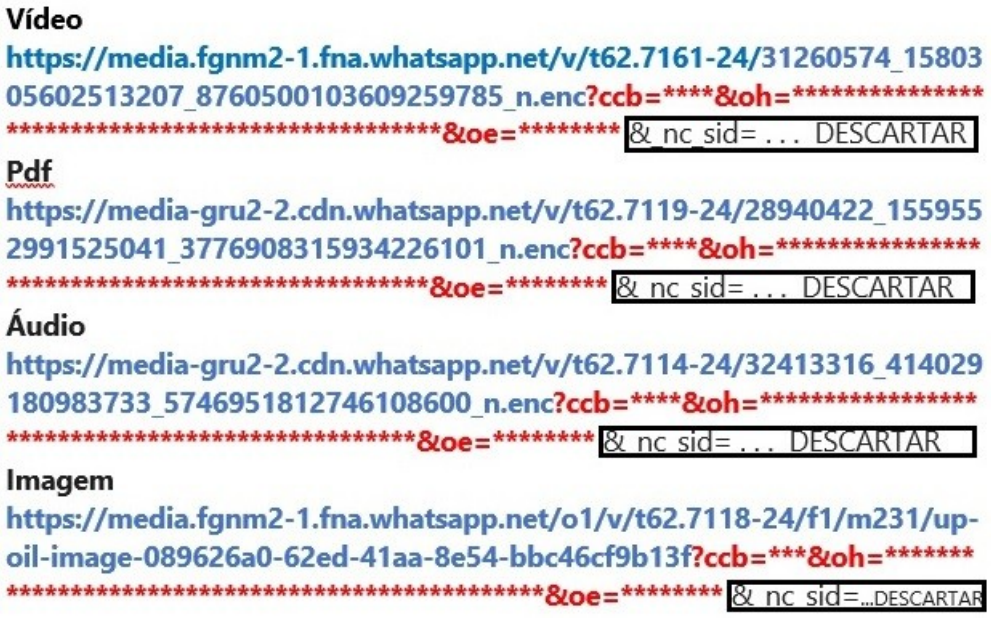
Uma vez obtida a URL de encaminhamento sucessivo da mídia impugnada, bastará representar à autoridade policial ou judiciária para que proceda ao seu bloqueio/suspensão junto à empresa detentora do aplicativo WhatsApp.

Testamos o procedimento acima e também conseguimos obter a URL de encaminhamento de uma mídia do WhatsApp. As URLs das mídias (criptografadas) tinham o seguinte padrão:

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



**Imagem 06: Padrão de URL de encaminhamento sucessivo do WhatsApp**




**Fonte: Elaborado pelo Autor**

A URL de encaminhamento sucessivo corresponde à parte destacada em azul (Imagem 06). Ao incluirmos os parâmetros “ccb”, “oh” e “oe” (parte vermelha), a referida mídia (criptografada) é baixada através do navegador.

Conforme já mencionado, é importante que se crie um grupo específico para receber as mídias a serem analisadas no Web WhatsApp. O arquivo a ser escolhido na aba “Name” do navegador Chrome é aquele representado por um ícone totalmente branco (vide figura 5). Para limpar a referida aba, utilize o botão “clear” (vide figura 4). Sendo o caso, exclua a mídia do grupo e envie o arquivo novamente. Caso o arquivo representado pelo ícone branco não apareça na aba “Name”, limpe o histórico do navegador e reinicie o processo.

Uma vez obtida a URL (identificador inequívoco de conteúdo - art. 19, §1º, MCI) correspondente à mídia impugnada, bastará acionar o Judiciário para que o WhatsApp bloqueie o encaminhamento sucessivo da referida mídia, bem como, forneça os registros de acesso do usuário responsável pelo *upload* do arquivo.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



Vale mencionar que nem sempre é necessário autorização judicial para retirada de conteúdo irregular da internet, bastando apenas a notificação do provedor de aplicação, consoante disposto no art. 21 do MCI, *in verbis*:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da **divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado** quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Em sua FAQ (página de perguntas frequentes)[19], o WhatsApp informa quais dados dos seus usuários podem ser compartilhadas com autoridades governamentais:

> (...)Dependendo da solicitação, a resposta do WhatsApp pode incluir, se disponível, **dados básicos (como nome, data de início do serviço, data da informação visto por último, endereço IP e endereço de e-mail) e dados da conta (como recado, foto do perfil, dados de grupos e lista de contatos)**(...)

Vale ressaltar, ainda, que o WhatsApp tem se manifestado no sentido de que "o efetivo cumprimento de ordem judicial pressupõe o recebimento da mídia impugnada, pelo próprio aplicativo Whatsapp, em uma conta específica criada para empresa para tanto, a fim de que se confirme o teor da mídia a ser bloqueada". Assim, o envio da mídia deve ser feito **via encaminhamento**, para que a empresa tenha acesso aos *metadados* do *upload* original.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



A revelação da identidade da pessoa por detrás do envio (*upload*) da mídia não significa, necessariamente, que foi esta quem a produziu, entretanto, cabe a esta desincumbir-se da imputação que lhe for feita.

Antes de solicitar dados de algum usuário do WhatsApp, pela via Judicial, é importante consultar a FAQ do aplicativo "Informações para as autoridades policiais"[20]. Dentre as informações disponíveis, destacamos:

> **Respostas às solicitações das autoridades policiais**
> Além dessas diretrizes, as autoridades policiais poderão entrar em contato com o WhatsApp com perguntas ou situações de emergência, conforme detalhado abaixo. Pedimos que as autoridades policiais não enviem solicitações ao Suporte do WhatsApp nem a qualquer outro canal não destinado para tanto.
>
> **Preservação da conta**
> Tomaremos as medidas necessárias para preservar os registros das contas relacionadas a investigações criminais oficiais por 90 dias, mediante recebimento do processo judicial formal. Você pode enviar rapidamente solicitações formais de preservação pelo Sistema de solicitações online para autoridades públicas, conforme descrito abaixo.
>
> **Solicitações emergenciais**
> Ao responder a uma situação que envolva risco iminente para uma criança, ou risco de morte ou de danos físicos graves para qualquer pessoa e que exija a divulgação imediata de informações, as autoridades policiais poderão usar o Sistema de solicitações online para autoridades públicas para enviar uma solicitação. Para que possamos processar esses pedidos com rapidez, recomendamos que você escreva a palavra "EMERGENCY" no campo de assunto da sua mensagem. Saiba mais sobre solicitações de dados de usuários por autoridades governamentais neste artigo.
>
> **Envio de solicitações**
> Online
> Os agentes das autoridades policiais podem usar o Sistema de solicitações online para autoridades públicas para enviar, monitorar e processar solicitações. É necessário ter um endereço de e-mail oficial para acessar o Sistema de solicitações online para autoridades públicas.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



Brito (2021)[21] esclarece que nas requisições de dados sobre endereços IPs é importante incluir as "portas lógicas" destes, quando o IP for nateado (compartilhado).

Jorge Júnior *et all* (2021)[22] descreve os passos para retirada de conteúdo ofensivo através de pedido formulado diretamente às plataformas digitais, como o Facebook, Instagram e WhatsApp.

Caselli (2019)[23] explica que até mesmo os *metadados* constantes das próprias mídias compartilhadas na rede, como data de criação, título ou autor, localização geográfica, resumo, palavras chaves, etc, podem subsidiar a identificação dos seus autores.

## 3.1 Operação Hastag

Uma questão foi levantada quando da operação Hastag, da PF, em julho de 2016: como a Polícia Federal teve acesso ao conteúdo do WhatsApp dos suspeitos? Em entrevista coletiva, o ministro da Justiça, à época, Alexandre de Moraes, confirmou o acesso às mensagens trocadas, no entanto, não explicou como isso se deu.

> Qualquer mecanismo de investigação não deve ser falado numa entrevista coletiva para avisar um suposto terrorista sobre como se investiga. Há a necessidade de uma regulamentação geral para que a Justiça consiga informações online, interceptações e dados do WhatsApp, porque isso facilitaria. Só que as investigações têm outros meios também", explicou Moraes.

O portal Oficina da Net[24] esclarece que "outros meios" de investigação policial podem ter sido adotados na operação Hastag, como a utilização de "Vírus no celular ou computador dos suspeitos, Uso de backup das conversas, Infiltração de agentes em grupos, Clonagem de números de celular e Uso de *metadados*, especificando em que consiste cada um destes métodos.

## 4. Considerações finais

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



O presente trabalho trata de um tema atual, ainda não pacificado no Direito brasileiro. De um lado temos uma empresa que prega não se responsabilizar por mensagens trocadas entre seus usuários. Do outro, temos o Judiciário que, no exercício da sua missão, tenta buscar criminosos que atuam livremente na plataforma de mensagens instantâneas.

A empresa argumenta que faz uso de criptografia de ponta-a-ponta, conforme estabelece o art. 13, IV, do Decreto 8.771/2016[25] (que regulamenta o MCI). Diz que não pode monitorar conteúdo que circula no aplicativo ainda que tais conteúdos estejam em desacordo com a lei, sob pena de incorrer em censura prévia, o que é vedado pela Constituição Federal (art. 220).

No que se refere ao uso da criptografia, temos como uma inciativa louvável. Entretanto, o uso da criptografia não impede o cumprimento das leis brasileiras, em especial do artigo 15 do MCI, até porque não se criptografa endereço IP e, acaso este fosse ocultado (através de um *proxy*, por exemplo), estaríamos diante de uma infração à Lei Federal 12.965/2014.

Apesar da Constituição Federal garantir a livre manifestação do pensamento (art. 220), ela também veda o anonimato (art. 5º, IV). Assim, não é exagero exigir que o WhatsApp mantenha, sob sigilo, em ambiente controlado e de segurança os registros de acesso a aplicações de internet, pelo prazo de 6 meses, nos termos do artigo 15 do Marco Civil da Internet.

## 5. Declaração de direitos

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



## 6. Referências

1. BARRETO, Alesandro Gonçalves. **WhatsApp: como excluir conteúdo viral com cena de sexo envolvendo criança e adolescente**. Delegados.com.br, 2018. Disponível em: https://delegados.com.br/noticia/whatsapp-como-excluir-conteudo-viral-com-cena-de-sexo-envolvendo-crianca-e-adolescente/. Acesso em: 08 mar. 2024.
2. BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Orientação técnica sobre a suspensão de encaminhamentos de arquivo fake news do aplicativo whatsapp**. Brasília-DF. Jan. 2017.
3. [3] BRITO, Jorge Messias de. O uso de "portas lógicas" pelos provedores de internet: uma análise das implicações criminais decorrentes do compartilhamento do endereço IP. **Revista Sociedade Científica**, vol. 6, n.1, p.3323-3357, 2023. https://doi.org/10.61411/rsc95388
4. CASELI, Guilherme. Metadados em whatsapp: uma nova perspectiva de coleta de evidências. **Delegados.com.br**, 2019. Disponível em: https://delegados.com.br/noticia/metadados-em-whatsapp-uma-nova-perspectiva-de-coleta-de-evidencias/. Acesso em: 08 mar. 2024.
5. FREITAS, Miguel. **CPMI - Fake News**: sobre a rastreabilidade do envio de mídias na plataforma Whatsapp para o combate de crimes digitais. 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/655c4226-698e-47fe-9deb-71e178bef7a5. Acesso em: 07 mar. 2024.
6. JORGE JÚNIOR, Hélio Molina *et all*. **Fake news e eleições**: o guia definitivo. Salvador: JusPodivm, 2021.
7. https://www.statista.com/topics/7731/whatsapp-in-brazil/. Acesso em: 07/03/2024.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



8. https://www.tecmundo.com.br/mercado/154215-whatsapp-pay-ameaca-o-pix-banco-central.htm. Acesso em: 07/03/2024. Acesso em: 07/03/2024.
9. https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2020/11/pix-e-lancado-oficialmente-e-esta-disponivel-para-todos-os-clientes-das-734-instituicoes-cadastradas. Acesso em: 07/03/2024.
10. https://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html. Acesso em: 07/03/2024.
11. https://www.tecmundo.com.br/whatsapp/75595-desembargador-derruba-determinacao-suspender-whatsapp-brasil.htm. Acesso em: 07/03/2024.
12. https://gauchazh.clicrbs.com.br/comportamento/noticia/2016/05/o-bloqueio-do-whatsapp-esta-previsto-no-marco-civil-da-internet-5791636.html. Acesso em: 07/03/2024.
13. https://web.archive.org/web/20160722030027/http://jota.uol.com.br/justica-rj-determina-novo-bloqueio-whatsapp. Acesso em: 07/03/2024.
14. https://g1.globo.com/tecnologia/noticia/2016/07/stf-suspende-decisao-da-justica-do-rio-que-bloqueou-whatsapp.html. Acesso em: 07/03/2024.
15. O TJBA foi um dos primeiros tribunais do país a regulamentar a Res. CNJ 345/2020, permitindo a prática de atos processuais por meio de aplicativos de mensagens, conforme se observa do Ato Normativo Conjunto TJBA nº 07/2022 (art. 8º, §2º)
16. https://atos.cnj.jus.br/atos/detalhar/3512. Acesso em: 07/03/2024.
17. https://legis.senado.leg.br/sdleg-getter/documento/download/655c4226-698e-47fe-9deb-71e178bef7a5. Acesso em: 07/03/2024.
18. https://support.google.com/youtube/answer/9288567. Acesso em: 07/03/2024.
19. https://support.google.com/youtube/answer/3244015. Acesso em: 07/03/2024.
20. https://support.google.com/youtube/answer/7648743. Acesso em: 07/03/2024.

**Scientific Society Journal**
**ISSN: 2595-8402**
**Journal DOI: 10.61411/rsc31879**



21. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07/03/2024.
22. https://delegados.com.br/noticia/whatsapp-como-excluir-conteudo-viral-com-cena-de-sexo-envolvendo-crianca-e-adolescente/. Acesso em: 08/03/2024.
23. BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. Orientação técnica sobre a suspensão de encaminhamentos de arquivo fake news do aplicativo whatsapp. Brasília-DF. Jan. 2017.
24. https://faq.whatsapp.com/808280033839222/. Acesso em: 18/02/2024.
25. https://faq.whatsapp.com/444002211197967/?locale=pt_BR. Acesso em: 08/03/2024.
26. https://show.scientificsociety.net/2023/12/o-uso-de-portas-logicas-pelos-provedores-de-internet-uma-analise-das-implicacoes-criminais-decorrentes-do-compartilhamento-do-endereco-ip/. Acesso em: 08/03/2024.
27. https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/9448/2021_jorgejunior_fake_news_eleicoes.pdf. Acesso em: 08/03/2024.
28. https://delegados.com.br/noticia/metadados-em-whatsapp-uma-nova-perspectiva-de-coleta-de-evidencias/. Acesso em: 08/03/2024.
29. https://www.oficinadanet.com.br/post/16937-como-o-governo-brasileiro-monitorou-o-whatsapp-de-supostos-terroristas. Acesso em 08/03/2024.
30. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 08/03/2024.