GUILHERME
CASELLI

MANUAL DE INVESTIGAÇÃO DIGITAL

4ª edição
revista, atualizada
e ampliada

2024

EDITORA
*jus*PODIVM
www.editorajuspodivm.com.br

inclusive, em uma balança de ponderação ao dever de empresa particular, o cumprimento de ordem judicial[3].

Contudo, a má utilização deste aplicativo pode vir a acarretar resultados nefastos à sociedade. O resultado é, assim, uma potencial repercussão direta em diversos ramos do direito, como: na esfera penal, a execução de crimes realizados e publicizados através de seus serviços; na esfera trabalhista, advindo justa causa e a consequente rescisão de contrato de trabalho; na esfera da família, ocasionando separações; na esfera cível, derivando em danos morais a serem indenizados; a disseminação de *fake news*, que resulta em instabilidade social; entre outros.

2. FUNCIONAMENTO DO APLICATIVO E SEGURANÇA DO *WHATSAPP*

Diversos estudos realizados para detalhar o funcionamento e a segurança do aplicativo de mensageria eletrônica *WhatsApp* (e.g.,[4-5]) apontam que todas as mensagens trocadas entre os usuários e o servidor são protegidas por

3. TILT, De. 80% dos brasileiros usa *WhatsApp* pelo menos uma vez por hora, diz pesquisa... – Veja mais em https://www.uol.com.br/tilt/noticias/redacao/2019/10/31/80-dos-brasileiros-usa-whatsapp-pelo-menos-uma-vez-por-hora.htm?cmpid=copiaecola. Internet: UOL, 31 out. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/10/31/80-dos-brasileiros-usa-whatsapp-pelo-menos-uma-vez-por-hora.htm. Acesso em: 20 maio 2020.
4. Paul Rösler, Christian Mainka, Jörg Schwenk (2018). More is Less: On the End-to-End Security of Group Chats in Signal, *WhatsApp*, and Threema. 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018). Disponível: https://eprint.iacr.org/2017/713.
5. Sukhodolskiy, Ilya & Zapechnikov, Sergey. (2020). Analysis of Secure Protocols and Authentication Methods for Messaging. Procedia Computer Science. 169. 407-411. 10.1016/j.procs.2020.02.237.

criptografia na camada de transporte. Já na camada de aplicação, o envio de mensagem utiliza criptografia ponta a ponta, ou seja, do momento em que sai do emissor até o instante em que chega no destinatário. Especificamente, o conteúdo das mensagens é cifrado e tem sua integridade protegida pelo mecanismo de *symmetric ratchet*, em conversas realizadas em grupo e, em conversas individuais, pelo mecanismo *Double Ratchet (DR)* com chaves simétricas estabelecidas entre remetente e destinatário renovadas continuamente. [6-7]

No caso específico de conversas em grupo, foi verificado[8] que o servidor do *WhatsApp* tem a capacidade de influenciar no gerenciamento do grupo (e.g., adicionando usuários sem que haja uma ação dos administradores do grupo pedindo tal inclusão). A forma de distribuição de mensagens em grupo também tem algumas peculiaridades. Especificamente, apurou-se que cada mensagem enviada por um remetente R gera um único texto cifrado para todos os membros do grupo, protegido por uma chave simétrica K_R e assinado com a chave de assinatura de R. Os membros receptores podem calcular K_R para decifrar a mensagem usando um mecanismo similar ao *double ratchet*, que também envolve a renovação contínua das chaves K_R utilizadas. Além do texto cifrado, a transcrição para o servidor também contém identificadores do grupo e da mensagem. O servidor adiciona o *ID* do remetente, um nome legível do remetente e

6. Sukhodolskiy, Ilya & Zapechnikov, Sergey. (2020). Analysis of Secure Protocols and Authentication Methods for Messaging. Procedia Computer Science. 169. 407-411. 10.1016/j.procs.2020.02.237.

7. *WhatsApp*. "Whatsapp encryption overview". Technical white paper. [Online]. Disponível: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

8. Paul Rösler, Christian Mainka, Jörg Schwenk (2018). More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018). Disponível: https://eprint.iacr.org/2017/713.

um carimbo de data e hora com a mensagem para os receptores, e replica para estes últimos o mesmo texto cifrado.

Quanto ao protocolo de troca de chaves públicas autenticadas, necessário para o estabelecimento dessas chaves simétricas, o *WhatsApp* utiliza o *X3DH*[9]. Neste protocolo, as chaves de cada usuário são assinadas usando o esquema de assinatu-ra digital *XEdDSA*[10]. A chave privada do par de chaves de longo prazo do mesmo usuário é usada como chave de assinatura. A chave secreta compartilhada gerada é então usada por eles de forma síncrona como a semente inicial do conjunto de chaves para implementar o mecanismo de *double ratchet*.

Ainda no tocante à proteção dos dados, a prática investigatória comprovou que os arquivos de *backup* não são protegidos por mecanismos de criptografia ponta a ponta, conforme também é informado na documentação oficial do aplicativo[11-12]. Assim, é possível acessá-los de maneira remota, sem a proteção da criptografia. Os detalhes sobre este último ponto são discutidos no Capítulo 3.

2.1. Utilização do algoritmo *symmetric ratchet* e *double ratchet*

Conforme mencionado anteriormente, as comunicações no *WhatsApp* utilizam chaves secretas que são constantemente atualizadas. O objetivo desse procedimento

9. Marlinspike M. The X3DH key agreement protocol / M. Marlinspike, T. Perrin. 2016. 11 pp. *URL*: https://signal.org/docs/specifications/x3dh/x3dh.pdf.
10. Perrin T. The XEdDSA and VXEdDSA Signature Schemes. Rev. 1. 14 pp. *URL*: https://signal.org/docs/specifications/xeddsa/.
11. WhatsApp. "FAQ – About *Google* Drive backups". [Online] https://faq.whatsapp.com/android/chats/about-google-drive-backups/.
12. WhatsApp. "FAQ – How to back up to iCloud". [Online] https://faq.whatsapp.com/iphone/chats/how-to-back-up-to-icloud.

é prover a propriedade de *forward secrecy* ("segurança futura", em uma tradução livre), o que significa basicamente que a descoberta da chave utilizada para proteção de uma mensagem (e.g., ao invadir um aparelho) não permite deci-frar mensagens enviadas anteriormente a essa descoberta. O *WhatsApp* usa dois modelos na execução de seus servi-ços[13]: o *symmetric ratchet* ("catraca simétrica", em uma tradu-ção livre) e o *double ratchet* ("catraca dupla", em uma tradu-ção livre), sendo que este último é considerado mais robusto do que o primeiro.

Em linhas gerais, após o estabelecimento de uma chave inicial usando o mecanismo *X3DH*, o *symmetric ratchet* atua-liza a chave de proteção de cada mensagem por meio de uma função de derivação de chaves (*key derivation function – KDF*). Assim, se um usuário enviar várias mensagens em sequência para um destinatário qualquer, cada uma delas será diferente, criando uma cadeia de chaves com as saídas do *KDF*. Como *KDFs* são algoritmos não reversíveis, a descoberta de uma de chave qualquer gerada como parte desse processo não permite determinar chaves anteriores.

O *double ratchet*, por sua vez, adiciona um procedimento extra de atualização ao *symmetric ratchet*: cada mensagem recebida por um usuário contém uma chave pública Diffie-Hellman efêmera do remetente, o que permite uma nova execução do protocolo de acordo de chaves; a chave resultante desse protocolo é então combinada com a chave simétrica existente, atualizando-a. Como resultado, um atacante que comprometa um dispositivo apenas momentaneamente seria incapaz de descobrir

13. Sukhodolskiy, Ilya & Zapechnikov, Sergey. (2020). Analysis of Secure Protocols and Authentication Methods for Messaging. Procedia Computer Science. 169. 407-411. 10.1016/j.procs.2020.02.237.

chaves futuras atualizadas com o *double ratchet*, por não conseguir descobrir o resultado das novas execuções do protocolo de acordo de chaves. Em outras palavras, para conseguir obter as chaves atualizadas de cada mensagem, um atacante precisaria ter acesso privilegiado contínuo à memória do dispositivo alvo, obtendo cada uma das chaves privadas efêmeras empregadas no mecanismo de *double ratchet*. Esse procedimento é ilustrado na Figura 1.

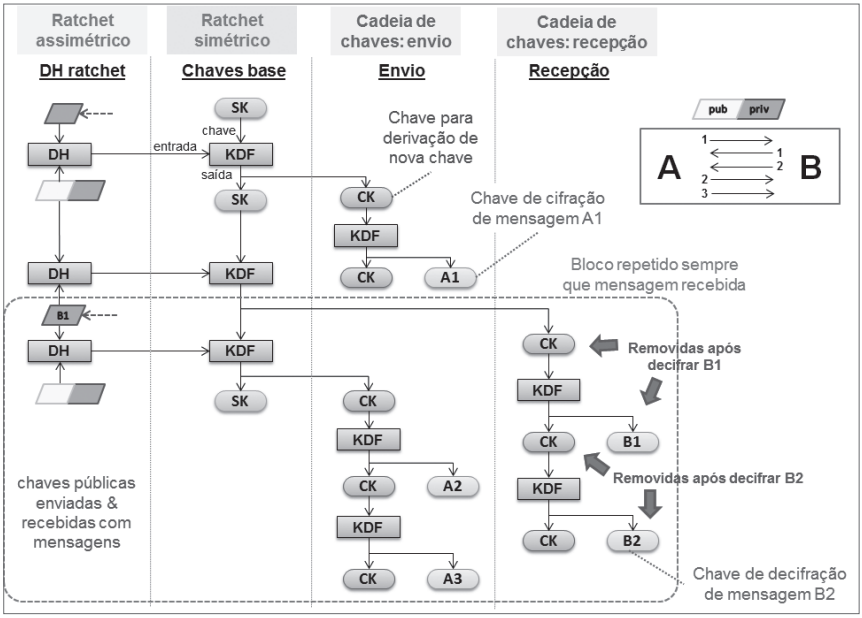

Figura 1 – Ilustração do mecanismo de *double ratchet* no aparelho de usuário A, comunicando-se com usuários B: mensagens carregam chaves públicas efêmeras para execução do protocolo Diffie Hellman (DH); chaves de cifração/decifração de mensagens são atualizadas por função de derivação de chaves (KDF), no procedimento simétrico do double ratchet, e também com chave obtida do DH, na sua porção assimétrica. Fonte: autor, com base em Analysis of Secure[14].

14. Sukhodolskiy, Ilya & Zapechnikov, Sergey. (2020). Analysis of Secure Protocols and Authentication Methods for Messaging. Procedia Computer Science. 169. 407-411. 10.1016/j.procs.2020.02.237.

3. OPERACIONALIZAÇÃO DAS INVESTIGAÇÕES ENVOLVENDO O *WHATSAPP*

Sob a ótica da polícia investigativa, seja no nível Civil ou Federal, uma investigação tendo por elemento tão somente um arquivo de mídia encaminhado via *WhatsApp* acaba sendo bastante complexa. Nesses casos, um dos poucos recursos possíveis cinge-se à simples análise reversa das imagens em serviços de buscadores da *web*. O resultado, em grande parte, é infrutífero, haja vista que o arquivo de mídia analisado pode não estar presente em qualquer base de dados indexável – como um servidor *web*, por exemplo.

3.1. Dados fornecidos pelos servidores do *WhatsApp*

No ano de 2017, foi realizada audiência pública no STF[15] para discutir o bloqueio judicial do *WhatsApp* e o 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. Ele também foi instado a se manifestar especificamente sobre a coleta e disponibilização

15. 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.

de metadados nos arquivos transitados em seus servidores. Embora na ocasião pouca informação nesse sentido tenha sido fornecida, é da experiência do autor que atualmente é possível requerer judicialmente que a empresa forneça:

1) Dados cadastrais: são as informações autodeclaráveis fornecidas pelo próprio usuário quando da criação da conta.
2) Histórico de acesso: trata-se do registro de conexões utilizadas pela conta *WhatsApp* para acessar a *Internet*. Em investigação digital, o histórico de endereços IP é um dos principais elementos buscados, pois concede a possibilidade de rastreabilidade do investigado.
3) Agenda de contatos: apontamento de todas as contas que interagiram com a conta alvo. Essa modalidade de coleta probatória é extremamente importante para destacar membros de eventual organização criminosa que se relacionam com o investigado.
4) Grupos: os grupos dos quais o investigado faz parte, que é outra informação muito valiosa disponível para as investigações. O *WhatsApp* também fornece os dados cadastrais acompanhados dos números telefônicos das contas que compõem cada grupo.
5) Extrato de mensagens: recentemente, o *WhatsApp* implementou a possibilidade de coleta de extrato de mensagens realizada entre a conta alvo e demais interlocutores. Não se trata de acesso ao conteúdo das conversas, mas apenas se houve alguma comunicação e quando isso ocorreu.

Desta forma, caso o investigado realize uma chamada via *VoIP*, é gerado um extrato do início e fim dessa chamada, o

tipo de contato estabelecido (no caso em questão, uma chamada via voz), a conexão *IP* da conta alvo e do interlocutor, assim como a porta lógica *TCP/IP* utilizada para acesso.

3.2. Dados fornecidos pelo serviço de *backup*

Como serviço acessório, o *WhatsApp* permite que seus usuários realizem *backup* dos arquivos multimídia recebidos ou produzidos pelos usuários. Ainda, é possível o envio e armazenamento do bloco das conversas realizadas via mensagem de texto.

Os blocos de conversação são arquivados nos serviços de *backup*, atualmente no formato de criptografia *crypt14*, que são protegidos pelo algoritmo criptográfico *AES*[16] e uma chave armazenada apenas no dispositivo celular do usuário. Desta forma, em princípio não é possível obter o conteúdo das conversas durante uma investigação policial. A exceção a essa regra se dá quando o próprio investigado se dispõe a auxiliar[17] devendo para tanto se autenticar junto ao serviço *Google Drive* utilizado para realizar o *backup*, baixar o conteú-do armazenado, decifrá-lo e acessá-lo normalmente.

Já os arquivos multimídia, conforme discutido mais profundamente no Capítulo de estudo de caso são armazenados sem a aplicação de criptografia. Assim, todos esses dados sincronizados e armazenados nos serviços de nuvens podem

16. CRYPT12 EXTENSÃO de arquivo. Internet, 1 jun. 2019. Disponível em: https://filememo.info/extension/crypt12. Acesso em: 13 maio 2020.

17. EXTRACT and Decrypt Android WhatsApp Backups from Google Account. Internet, 24 jan. 2018. Disponível em: https://blog.elcomsoft.com/2018/01/extract-and-decrypt-whatsapp-backups-from-google/. Acesso em: 11 maio 2020.

ser acessados pelas Autoridades de Segurança Públicas. Isso requer o auxílio dos provedores de serviço de nuvem, o que é possível mediante instauração do devido procedimento investigatório.

3.3. Dados não fornecidos pelo servidor do *WhatsApp*

Com base em uma classificação técnico-jurídica, pode-se dizer que a empresa *WhatsApp* fornece para autoridades de investigação elementos formais, compostos por dados qualificativos e logs de conexão. Quanto a elementos materiais, assim entendidos o conteúdo produzido pelos usuários, como mensagens e mídias, a empresa declara em seus termos de serviço[18] que não possui acesso ao conteúdo das mensagens produzidas pelos usuários e, portanto, tampouco permite a terceiros tal acesso:

Suas mensagens são suas e nós não podemos lê-las. Implementamos privacidade, criptografia de ponta-a-ponta e outras ferramentas de segurança no *WhatsApp*. Nós não mantemos suas mensagens após o envio das mesmas. Quando elas estão criptografadas de ponta a ponta, nós e terceiros, não podemos lê-las de maneira alguma.

Outro dado útil para investigações, mas que não é fornecido pelos servidores do *WhatsApp*, é a identidade do usuário que gerou certo conteúdo de mídia que venha a ser julgado como ilícito. Ao menos em parte, essa não identificação de autoria parece estar relacionada à ausência no *WhatsApp* de serviços de deduplicação de arquivos, expediente que

18. WhatsApp. Dados Jurídicos do WhatsApp. Internet, 28 jan. 2020. Disponível em: https://www.whatsapp.com/legal/#key-updates. Acesso em: 23 jun. 2020.

assegura que somente uma cópia de um arquivo anexado e enviado a diversos usuários seja armazenada. Este é quase um pré-requisito para backup, arquivamento e qualquer outra forma de armazenamento secundário em que a velocidade de acesso seja menos importante do que a redução do volume de dados: ao identificar e eliminar dados repetidos em diferentes locais, reduz-se a necessidade de armazenamento em até 90%[19]. A implementação de deduplicação, em conjunto com estruturação de um serviço de histórico de logs, serviria para indicar o primeiro usuário do *WhatsApp* que disponibilizou a mídia com o conteúdo ilícito apontado e, via de consequência, meios de se chegar a que registrou o evento criminal.

Em complemento à lista de dados técnicos que não são fornecidos pelos servidores do *WhatsApp* para autoridades públicas destacam-se os chamados metadados[20].

Em uma linguagem objetiva, metadados são definidos como "dados relativos a outros dados", ou seja, informações que são fornecidas sobre um determinado arquivo e que exercem a função descritiva. Estruturalmente, metadados podem ser organizados em ao menos três tipos[21-22]:

---

19. L. SCHEIER, ROBERt. Cinco maneiras de reduzir o storage: Saiba qual das técnicas para reduzir o volume de dados armazenados é a mais indicada para a sua empresa. Computerworld, [S. l.], p. 1-2, 1 dez. 2010. Disponível em: https://computerworld.com.br/2010/12/01/cinco-maneiras-de-reduzir-o-storage/. Acesso em: 10 maio 2020.
20. 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.
21. 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.
22. PARTE I: o que são metadados?. Icann.org, [S. l.], p. 1, 11 maio 2016. Disponível em: https://www.icann.org/news/blog/parte-i-o-que-sao-metadados. Acesso em: 10 maio

- METADADOS DESCRITIVOS incluem informações como pontos de contato, palavras-chave usadas para destacar um arquivo, uma localização geográfica ou até mesmo uma explicação sobre o método de captura ou transmissão dos dados. Esses dados são úteis para descobrir, coletar ou agrupar recursos de acordo com as características por eles compartilhadas.

- METADADOS ESTRUTURAIS explicam como um recurso é composto ou organizado.

- METADADOS ADMINISTRATIVOS são usados para gerenciar um recurso. Datas de criação, direitos ou proveniência, ou diretrizes para disposição, como retenção ou remoção. Metadados semelhantes seriam relevantes para um administrador de banco de dados ou para administradores responsáveis por capturar fluxos de tráfego de telecomunicações de dados, ou um log de segurança e dados de eventos.

A rigor, durante as investigações policiais realizadas so-bre crimes ocorridos no cenário virtual, os metadados descri-tivos e administrativos são os mais utilizados, pois ensejam a busca por evidências e fornecem elementos indicadores de autoria. Por ser tratar de meio de coleta probatória, este re-curso não se atém somente à seara penal, podendo ser utili-zado em qualquer ramo do direito.

É interessante notar que, conforme estudos práticos realizados e discutidos na sessão Estudo de Caso deste título, os arquivos de mídia que ficam armazenados nos serviços de *backup* usados pelo *WhatsApp* muitas vezes preservam seus metadados. Entretanto, conforme já indicado, curiosamente essa indicação de coleta e preservação expressa de metadados não aparece no documento oficial contendo a "política de

privacidade" do *WhatsApp*. A provável razão para tal omissão é que metadados desse tipo não estão diretamente relacionados aos serviços de comunicação fornecidos pelo aplicativo.

3.4. Análise reversa de mídias

O *WhatsApp* recentemente disponibilizou em sua versão Beta 2.19.73 a opção de busca reversa de imagens usando a ferramenta correspondente fornecida pelo *Google*. Assim, ao receber uma imagem no *WhatsApp*, o usuário poderia realizar buscas de imagens semelhantes diretamente pelo aplicativo, fortalecendo o combate às *fake news*.

Na seara investigativa, a análise reversa de imagem é apenas um dos possíveis recursos que podem ser usados por investigadores. Porém, a praxe investigatória aponta ser mais eficaz na apuração de ilícitos a extração e análise de metadados, pois possibilita meios para indicar o autor da mídia (imagem, vídeo ou áudio) produzida de maneira criminosa.

A título exemplificativo, caso noticiado ao Delegado de Polícia que um arquivo de áudio está sendo disseminado via *WhatsApp*, a utilização de busca reversa por imagens não teria qualquer utilidade. Também, os demais elementos de persecução disponibilizados pela empresa pouco serviriam para indicar a autoria do áudio.

3.5. Da lista de bloqueio de mídias ilícitas nos servidores do *WhatsApp*

No ano de 2018, o *WhatsApp* disponibilizou as atualizações 2.18.106 e 2.18.110. Dentre outras melhorias, estas

atualizações passaram a permitir que os usuários pudessem baixar novamente as mídias recebidas e acidentalmente apagadas da galeria do dispositivo móvel. Assim, contanto que preservado o caminho da mídia recebida no aplicativo, pas-sou a ser possível baixar mídias recebidas em uma margem temporal de 30 dias pretéritos.

Com base nesta atualização, peritos e profissionais da Segurança Pública que atuam na repressão de crimes ocorri-dos nos meios digitais constataram que o *WhatsApp* passou a adotar como política "sempre armazenar" tais conteúdos, mesmo que já tenham sido entregues e mesmo que não se-jam eles classificados como "conteúdo popular"[23].

Até a implementação da criptografia ponta-a-ponta, era possível visualizar de maneira direta a *url* que individualizava a mídia às claras, com indicação da extensão do tipo de ar-quivo como *jpg*, *mp4*. Após a implementação da criptografia ponta-a-ponta, no entanto, isso não é mais possível. Assim, conforme estudo de caso apresentado no item 4.2 deste tra-balho, quando se identifica que uma mídia contém material ilícito, o método empregado consiste em utilizar um navega-dor de Internet em modo desenvolvedor para se localizar a *url* deste arquivo cifrado (com a extensão ".enc"). Esta *url* é então fornecida ao provedor de aplicação do *WhatsApp*, que é inti-mado a colocar qualquer arquivo cifrado com esse *hash* em uma lista de proibição, impedindo sua propagação. Evidente-mente, essa técnica não se presta a excluir mídias com con-teúdo ilícito dos dispositivos móveis, mas apenas se presta a evitar sua propagação em massa.

23. WHATSAPP. Informação Legal. Terms of Service. Disponível em: <https://www.WhatsApp.com/legal/#Privacy>. Acesso: 10 maio. 2020.

3.6. Coleta de dados pelo *WhatsApp*

São raros os documentos oficiais produzidos pela empre-sa *WhatsApp* sobre a coleta de dados de mídia e de usuários que utilizam seus serviços. Um dos poucos, voltado às Auto-ridades Públicas, é o intitulado "Informações para as autori-dades policiais"[24], que é parte integrante do conjunto de per-guntas frequentes.

De acordo com esse documento, é possível que o servidor do *WhatsApp* disponibilize os 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;* e 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 segue:

> É necessária uma ordem judicial emitida conforme o Código dos Estados Unidos, título 18, seção 2703(d), para forçar a divulgação de determinados registros ou de outras informações relacionadas à conta, excluindo-se o 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 multimídia (áudio, foto ou vídeo) via *WhatsApp* e tente buscar por seus

24. WHATSAPP. Informação Legal. Terms of Service. Disponível em: <https://www.WhatsApp.com/legal/#Privacy>. Acesso: 10 maio. 2020.