A Impossibilidade Técnica de Interceptação de Comunicações de Áudio e Vídeo via WhatsApp: Uma Análise Pericial no Contexto do Caso ORUAN

Por Leandro Morales (*Leandro Morales é perito digital especializado em investigações forenses de dispositivos móveis e análise de evidências digitais. Atua há mais de 20 anos na área de perícia digital, prestando consultoria técnica para escritórios de advocacia e órgãos do sistema de justiça.***), Dellano Sousa (Advogado) e Alexandre Morais da Rosa (Juiz de Direito do TJSC e Professor da UNIVALI, doutor em Direito alexandremoraisdarosa@gmail.com)**

Figura 1: Criptografia de Ponta a Ponta

Introdução

O recente caso envolvendo o cantor de funk ORUAN (Mauro Davi dos Santos Nepomuceno), preso em fevereiro de 2025 e classificado como detento de "alta periculosidade", trouxe novamente à tona uma questão técnica fundamental que gera confusão entre operadores do direito: a alegada possibilidade de interceptação de comunicações de áudio e vídeo realizadas através do aplicativo WhatsApp [1].

A imprensa tem divulgado amplamente que as autoridades policiais teriam interceptado conversas de áudio e vídeo do artista através do popular aplicativo de mensageria. Contudo, do ponto de vista técnico e pericial, a afirmação significa desconhecimento ou confusão quanto ao funcionamento dos sistemas de criptografia de ponta a ponta implementados pelo WhatsApp, bem como sobre as limitações tecnológicas inerentes aos processos de interceptação digital.

Este artigo tem por objetivo esclarecer, de forma técnica e didática, de modo acessível aos profissionais do direito, os aspectos fundamentais que tornam tecnicamente impossível a interceptação direta de comunicações de áudio e vídeo realizadas por meio do WhatsApp, abordando os conceitos de criptografia, as diferenças entre os tipos de comunicação digital e os métodos realmente viáveis para acesso a essas informações no contexto da perícia digital e das investigações criminais.

A compreensão adequada desses aspectos técnicos é essencial para que advogados, membros do Ministério Público, juízes, policiais e demais operadores do direito possam avaliar corretamente as provas digitais apresentadas em processos judiciais, evitando equívocos que podem comprometer a qualidade da prestação jurisdicional e a própria segurança jurídica (erros evitáveis).

1. Comunicadores de Mensagem: Fundamentos Tecnológicos

Figura 2: Aplicativos de Mensageria

Para compreender adequadamente a impossibilidade técnica de interceptação de comunicações via WhatsApp, é fundamental primeiro entender o que são e como funcionam os comunicadores de mensagem instantânea. Os aplicativos de mensageria representam uma evolução significativa dos sistemas de comunicação digital, diferindo substancialmente dos métodos tradicionais de telecomunicações.

Os comunicadores de mensagem, como WhatsApp, Telegram, Signal e Threema, são aplicações de software que permitem a troca de mensagens, arquivos, chamadas de voz e videochamadas através da internet. Diferentemente das chamadas telefônicas convencionais, que trafegam através das redes de telecomunicações tradicionais (circuito comutado), essas comunicações utilizam protocolos de internet (IP) e são processadas como dados digitais, atendendo a parâmetros de ordem eletrônica-digital [2].

1.1 Arquitetura dos Sistemas de Mensageria

A arquitetura fundamental dos modernos sistemas de mensageria instantânea baseia-se em três componentes principais: o cliente (aplicativo instalado no dispositivo do usuário), os servidores intermediários (responsáveis pelo roteamento das mensagens) e os protocolos de comunicação (que definem como as informações são formatadas e transmitidas).

No modelo tradicional de telecomunicações, as operadoras mantêm controle direto sobre o conteúdo das comunicações que, com autorização judicial, podem implementar sistemas de interceptação com o fim de capturam as conversas no momento da transmissão. O modelo é possível porque as comunicações trafegam em formato não criptografado ou com criptografia controlada pela própria operadora. (Exemplo o SMS)

Os aplicativos de mensageria modernos, no entanto, implementam um paradigma completamente diferente (meio distinto). O conteúdo das comunicações é criptografado no dispositivo de origem antes mesmo de ser transmitido para os servidores, e apenas o dispositivo de destino possui as chaves necessárias para descriptografar e acessar o conteúdo. Os servidores intermediários funcionam apenas como retransmissores de dados criptografados, sem capacidade de acessar o conteúdo das mensagens.

Em termos mais cotidianos, considere que você quer enviar uma carta para um amigo. No modelo tradicional, você entrega a carta aberta ao carteiro, que pode lê-la durante o caminho. Se alguém com permissão especial quiser, pode pedir ao carteiro que mostre o conteúdo antes de entregá-lo. Esse modelo é similar ao modelo tradicional de telecomunicação, em que as operadoras (os "carteiros") têm acesso ao conteúdo das comunicações, e, com autorização, podem "ler" ou interceptar as mensagens. Agora, imagine que, em vez de entregar a carta aberta, você cola um selo ou lacre no envelope. O selo ou lacre só pode ser aberto por seu amigo, nem mesmo o carteiro pode vê-lo, ainda que tente. Nos sistemas modernos de mensageria instantânea, a "carta" (sua mensagem) é "selada/lacrada" com criptografia no seu dispositivo (o "remetente") antes mesmo de ser enviada e os servidores intermediários atuam como “carteiros” que só encaminham o envelope, sem jamais saber o que está dentro.

1.2 Diferenças Fundamentais entre Mensageria e Telefonia Tradicional

A distinção entre os sistemas de mensageria instantânea e a telefonia tradicional é relevante para compreender as possibilidades e limitações técnicas da interceptação do conteúdo. Na telefonia convencional, as operadoras possuem acesso direto ao conteúdo das comunicações, permitindo a implementação de sistemas de interceptação mediante autorização judicial. O áudio das chamadas trafega pelos equipamentos da operadora, que pode capturar e gravar essas comunicações.

Nos aplicativos de mensageria com criptografia de ponta a ponta, altera-se completamente a dinâmica. As empresas desenvolvedoras dos aplicativos (como a Meta, proprietária do WhatsApp) não possuem acesso ao conteúdo das comunicações de seus usuários. Os servidores das empresas recebem apenas dados criptografados, que são matematicamente

impossíveis de decifrar sem as chaves específicas geradas pelos dispositivos dos usuários (pelo menos por enquanto).

A diferença arquitetural tem implicações profundas para as investigações criminais e para a aplicação da lei. Enquanto as autoridades podem solicitar às operadoras de telefonia a interceptação de chamadas convencionais, no regime dos aplicativos de mensageria que implementam criptografia de ponta a ponta robusta, a solicitação é tecnicamente impossível.

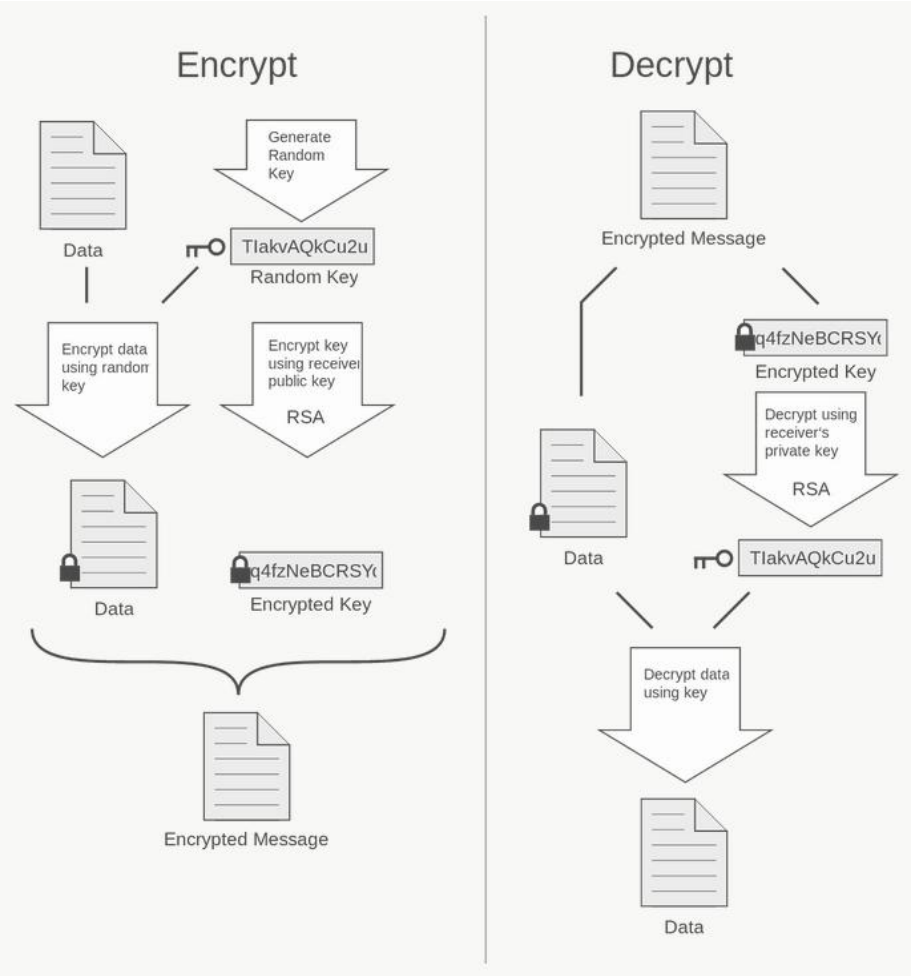

Figura 3: Processos de Criptografia e descriptografia

1.3 Evolução da Segurança em Comunicações Digitais

A implementação de criptografia de ponta a ponta em aplicativos de mensageria representa uma resposta natural à crescente preocupação com a privacidade digital e a segurança das comunicações. A evolução das camadas de segurança e privacidade foi impulsionada por diversos fatores, incluindo o aumento dos crimes cibernéticos, a exposição de programas de vigilância governamental e a crescente conscientização dos usuários sobre a importância da proteção de seus dados pessoais.

O WhatsApp implementou a criptografia de ponta a ponta em 2016, utilizando o protocolo Signal, desenvolvido pela Open Whisper Systems. A implementação foi um marco na democratização da criptografia forte, tornando-a acessível a bilhões de usuários sem necessidade de conhecimento técnico especializado [3].

A adoção massiva desses sistemas de comunicação segura criou um novo paradigma para as investigações criminais, exigindo que as autoridades desenvolvam novas metodologias e técnicas para obtenção de evidências digitais, sempre respeitando os limites técnicos e legais impostos pela tecnologia de criptografia.

2. Criptografia e Segurança Digital: Conceitos Fundamentais

Figura 4: Criptografia Digital

A criptografia constitui o alicerce tecnológico que torna impossível a interceptação direta de comunicações via WhatsApp. Para compreender adequadamente a impossibilidade técnica, é essencial dominar os conceitos fundamentais da criptografia moderna e suas aplicações em sistemas de comunicação digital.

2.1 O Que é Criptografia

Criptografia é a ciência e arte de escrever em códigos, transformando informações legíveis (texto claro) em informações aparentemente aleatórias (texto cifrado) através de algoritmos matemáticos complexos. O objetivo fundamental da criptografia é garantir que apenas pessoas autorizadas possam acessar o conteúdo original das informações, mesmo que terceiros interceptem os dados durante a transmissão [4].

Em termos cotidianos, considere que que você tem um cofre onde guarda todas as suas coisas mais valiosas, contendo uma fechadura especial que só pode ser aberta com uma combinação secreta que você conhece. Se alguém encontrar o cofre, não conseguirá abri-lo sem a combinação certa — mesmo que seja um interessado ou especialista.

No contexto das comunicações digitais, a criptografia serve a quatro propósitos principais: confidencialidade (garantir que apenas destinatários autorizados possam ler a mensagem), integridade (assegurar que a mensagem não foi alterada durante a transmissão), autenticidade (confirmar a identidade do remetente) e não-repúdio (impedir que o remetente negue ter enviado a mensagem).

A força de um sistema criptográfico é medida pela dificuldade computacional necessária para quebrar a criptografia sem conhecer as chaves apropriadas. Os sistemas modernos utilizam chaves de tamanhos que tornariam necessários milhares de anos de processamento computacional para serem quebradas por força bruta (tentativa e erro), mesmo utilizando os computadores mais poderosos disponíveis atualmente.

2.2 Comunicação em Texto Claro versus Comunicação Criptografada

A diferença entre comunicação em texto claro e comunicação criptografada é fundamental para compreender as limitações da interceptação digital. Na comunicação em texto claro, os dados e as informações trafegam pela rede em formato legível, permitindo que qualquer pessoa com acesso aos canais de transmissão possa ler o conteúdo das mensagens.

Historicamente, muitos sistemas de comunicação digital operavam em texto claro ou utilizavam criptografia fraca, facilmente quebrada pelas autoridades. Emails não criptografados, mensagens SMS e chamadas telefônicas convencionais são exemplos de comunicações que podem ser interceptadas e compreendidas diretamente pelas autoridades competentes, mediante autorização judicial.

A comunicação criptografada, por outro lado, transforma o conteúdo original em dados aparentemente aleatórios antes da transmissão. Mesmo que um interceptador capture esses dados durante a transmissão, ele verá apenas sequências de caracteres sem sentido, matematicamente impossíveis de decifrar sem as chaves apropriadas.

No caso específico do WhatsApp, todas as mensagens, chamadas de voz e videochamadas são automaticamente criptografadas no dispositivo do usuário antes de serem enviadas através da internet. Os servidores da Meta (empresa proprietária do WhatsApp) recebem apenas esses dados criptografados e os retransmitem para o destinatário, sem nunca ter acesso ao conteúdo original das comunicações.

2.3 A Implementação da Criptografia no WhatsApp

O WhatsApp utiliza o protocolo Signal, considerado o padrão-ouro em criptografia de ponta a ponta para comunicações instantâneas. O protocolo foi desenvolvido por criptógrafos renomados e passou por extensas auditorias de segurança realizadas por especialistas independentes [5].

A implementação da criptografia no WhatsApp ocorre de forma completamente transparente para o usuário. Quando uma pessoa instala o aplicativo, o dispositivo gera automaticamente um par de chaves criptográficas únicas: uma chave privada (mantida em segredo no

dispositivo) e uma chave pública (compartilhada com outros usuários para permitir a comunicação criptografada).

Cada conversa no WhatsApp possui suas próprias chaves de sessão, geradas dinamicamente e alteradas regularmente através de um processo chamado "forward secrecy" ou segurança progressiva. Isso significa que mesmo se uma chave de sessão for comprometida, ela não permitirá o acesso a mensagens anteriores ou futuras da mesma conversa.

O processo de criptografia e descriptografia ocorre inteiramente nos dispositivos dos usuários. Quando uma pessoa envia uma mensagem, seu dispositivo criptografa o conteúdo usando as chaves apropriadas antes de transmitir os dados pela internet. O dispositivo do destinatário recebe os dados criptografados e os descriptografa localmente, exibindo o conteúdo original apenas para o usuário autorizado.

Em termos cotidianos, a partir do exemplo da carta. Considere que que você deseja enviar uma mensagem muito importante para um amigo, mas você não quer que ninguém mais a leia, nem mesmo os funcionários da empresa que entrega as cartas. Para garantir que só o seu amigo possa abrir a carta, você decide usar um sistema de chaves secretas (cadeado no selo ou lacre), contendo duas chaves. Assim como você tem uma chave para abrir sua casa, o WhatsApp usa um par de chaves criptográficas para proteger suas mensagens. A primeira é a chave pública, equivalente a uma chave que você dá a todos os seus amigos. Qualquer um pode usá-la para "trancar" uma mensagem para você, mas... A segunda é a chave privada, um tipo de chave especial que só você tem. É a única chave que pode "destrancar" as mensagens enviadas por seus amigos. O processo de envio: (a) Quando você escreve uma mensagem no WhatsApp, é como colocar a carta em um envelope. Antes de enviar, o aplicativo "tranca" o envelope usando a chave pública do seu amigo (cadeado ou selo); (b) Mesmo que alguém intercepte o envelope pelo caminho, não conseguirá abri-lo sem a chave privada do seu amigo; (c) A entrega é segura porque o O envelope viaja pela internet, passando por muitas "mãos", mas ninguém pode lê-lo; e, (d) Quando chega ao destino, o seu amigo usa sua chave privada para "destrancar" o envelope e ler a mensagem. O motivo é que para cada conversa no WhatsApp funciona como uma nova caixa forte e quando você começa uma conversa, uma nova chave de sessão é criada, modificando-se de modo dinâmico. Equivale a trocar a fechadura da porta a cada visita. Ainda que alguém descubra a combinação atual, torna-se inútil na próxima visita. No caso do whatsapp a implementação acontece de forma automática, sem que você precise pensar. É como se o seu dispositivo tivesse um assistente invisível que cuida de todas as chaves e trava as mensagens antes de enviá-las. Assim como você confia que as chaves da sua casa estão seguras, o protocolo Signal foi testado por especialistas para garantir a confiança, atestando que se alguém tentar "quebrar" o sistema, com os recursos existentes, a tentativa será impossível, diante da matemática forte e complicada que suporta os cálculos.

2.4 Implicações Legais e Técnicas da Criptografia Forte

A implementação de criptografia forte em aplicativos de comunicação tem implicações significativas para o sistema de justiça criminal. Do ponto de vista técnico, a criptografia de

ponta a ponta torna impossível para as empresas desenvolvedoras dos aplicativos fornecer às autoridades o conteúdo das comunicações de seus usuários, mesmo mediante ordem judicial.

A limitação técnica não representa uma escolha deliberada das empresas para obstruir investigações criminais, representando uma consequência inevitável da arquitetura de segurança implementada. As empresas literalmente não possuem as chaves necessárias para descriptografar as comunicações de seus usuários, pois essas chaves são geradas e mantidas exclusivamente nos dispositivos dos usuários.

Do ponto de vista legal, essa realidade técnica tem gerado debates intensos sobre o equilíbrio entre privacidade individual e segurança pública. Alguns países têm proposto legislações que exigiriam que as empresas implementem "backdoors" ou “portas do fundo” em seus sistemas de criptografia, permitindo acesso governamental ao conteúdo das comunicações. Em termos cotidianos, a pretensão seria a de criar uma "porta dos fundos" na “fechadura” utilizada no exemplo anterior, como uma espécie de chave mestra que o governo pode usar para abrir qualquer porta, com os riscos associados à privacidade, segurança e manipulação, além do risco de cair em mãos erradas, comprometendo todo o sistema de segurança.

A comunidade técnica internacional é praticamente unânime em afirmar que a implementação de backdoors compromete fundamentalmente a segurança de todos os usuários, criando vulnerabilidades que podem ser exploradas não apenas por governos, mas também por criminosos e agentes maliciosos [6].

No contexto brasileiro, é fundamental que os operadores do direito compreendam essas limitações técnicas para evitar expectativas irrealistas sobre as capacidades de interceptação digital e para desenvolver estratégias investigativas adequadas às realidades tecnológicas contemporâneas.

3. Criptografia Simétrica e Assimétrica: Fundamentos dos Sistemas de Chaves

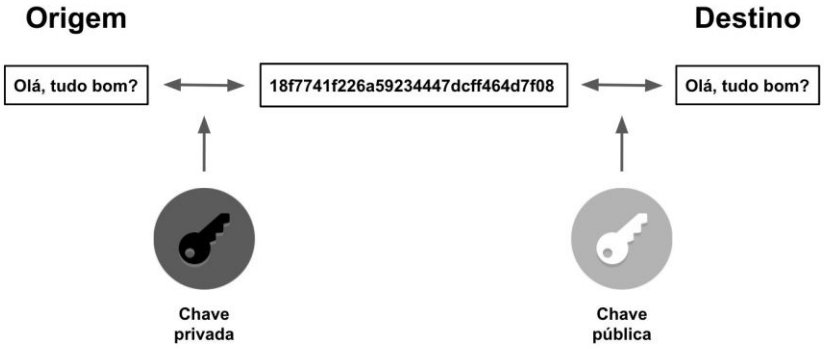

Figura 5: Chaves Criptográficas Simétricas

A compreensão dos diferentes tipos de sistemas criptográficos é essencial para entender como o WhatsApp e outros aplicativos de mensageria implementam a segurança de ponta a ponta. Existem dois paradigmas fundamentais na criptografia moderna: a criptografia simétrica e a criptografia assimétrica, cada uma com características específicas que influenciam diretamente na impossibilidade de interceptação das comunicações.

3.1 Criptografia Simétrica: O Sistema de Chave Única

A criptografia simétrica, também conhecida como criptografia de chave secreta, utiliza a mesma chave tanto para criptografar quanto para descriptografar as informações. É o método mais antigo e, em termos de processamento computacional, o mais eficiente para criptografar grandes volumes de dados [7].

No sistema simétrico, tanto o remetente quanto o destinatário devem possuir a mesma chave secreta. O remetente utiliza essa chave para criptografar a mensagem, e o destinatário usa a mesma chave para descriptografá-la. A segurança do sistema depende inteiramente do sigilo dessa chave compartilhada.

O principal desafio da criptografia simétrica é a distribuição segura das chaves. Como remetente e destinatário precisam compartilhar a mesma chave secreta, surge o problema fundamental: como transmitir essa chave de forma segura sem que ela seja interceptada? Historicamente, isso exigia canais de comunicação previamente seguros ou encontros presenciais para troca de chaves.

Exemplos clássicos de algoritmos de criptografia simétrica incluem o AES (Advanced Encryption Standard), utilizado amplamente em aplicações comerciais e governamentais, e o ChaCha20, empregado em algumas implementações do protocolo Signal. Esses algoritmos são extremamente eficientes e seguros quando as chaves são adequadamente protegidas.

3.2 Criptografia Assimétrica: O Sistema de Chaves Públicas

A criptografia assimétrica, também conhecida como criptografia de chave pública, revolucionou a segurança digital ao resolver o problema da distribuição de chaves. Neste sistema, cada usuário possui um par de chaves matematicamente relacionadas: uma chave pública (que pode ser compartilhada livremente) e uma chave privada (que deve ser mantida em absoluto sigilo) [8].

O funcionamento da criptografia assimétrica baseia-se em funções matemáticas de mão única: operações que são fáceis de calcular em uma direção, mas computacionalmente impossíveis de reverter sem conhecimento da chave privada. Os algoritmos mais comuns incluem RSA, baseado na dificuldade de fatorar números primos grandes, e ECDH (Elliptic Curve Diffie-Hellman), baseado no problema do logaritmo discreto em curvas elípticas.

Na prática, se Alice deseja enviar uma mensagem criptografada para Bob, ela utiliza a chave pública de Bob para criptografar a mensagem. Uma vez criptografada com a chave pública de Bob, apenas a chave privada correspondente (que só Bob possui) pode descriptografar a

mensagem. Mesmo que a chave pública de Bob seja conhecida por todos, isso não compromete a segurança da comunicação.

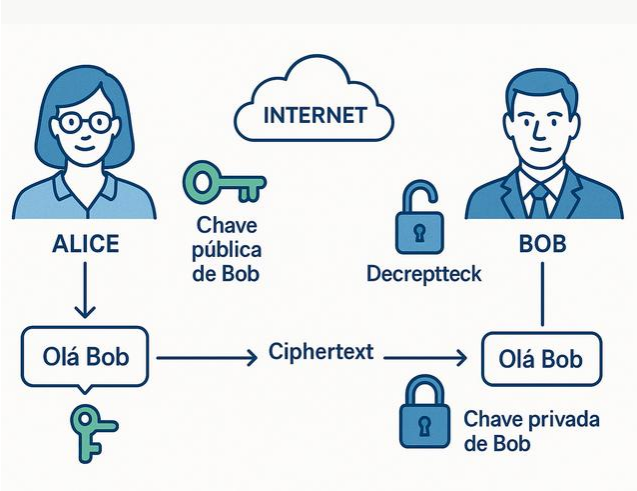

Figura 6: Chaves Criptográficas Assimétricas

A criptografia assimétrica também permite a implementação de assinaturas digitais, onde o remetente usa sua própria chave privada para "assinar" uma mensagem, permitindo que qualquer pessoa verifique a autenticidade da mensagem usando a chave pública do remetente.

3.3 Sistemas Híbridos: Combinando o Melhor dos Dois Mundos

Os sistemas de comunicação modernos, incluindo o WhatsApp, utilizam abordagens híbridas que combinam as vantagens da criptografia simétrica e assimétrica. Essa combinação é necessária porque, embora a criptografia assimétrica resolva o problema da distribuição de chaves, ela é computacionalmente muito mais lenta que a criptografia simétrica para processar grandes volumes de dados.

No modelo híbrido, a criptografia assimétrica é utilizada para estabelecer um canal seguro e trocar chaves simétricas. Uma vez que as chaves simétricas são estabelecidas de forma segura, toda a comunicação subsequente utiliza criptografia simétrica, que é mais eficiente para processar mensagens, arquivos, chamadas de voz e videochamadas.

O protocolo Signal, utilizado pelo WhatsApp, implementa um sistema híbrido sofisticado que inclui várias camadas de segurança. Inicialmente, os dispositivos utilizam criptografia assimétrica para estabelecer chaves de sessão simétricas. Essas chaves de sessão são então utilizadas para criptografar o conteúdo real das comunicações.

3.4 Troca de Chaves e Estabelecimento de Sessões Seguras

O processo de troca de chaves no WhatsApp é automatizado e transparente para o usuário, mas envolve uma complexa dança criptográfica que garante a segurança das comunicações.

Quando dois usuários iniciam uma conversa, seus dispositivos executam um protocolo de acordo de chaves que estabelece chaves de sessão únicas para aquela conversa específica.

O processo utiliza o protocolo X3DH (Extended Triple Diffie-Hellman), que combina chaves de longo prazo (associadas à identidade do usuário) com chaves efêmeras (geradas especificamente para cada sessão). O resultado é um conjunto de chaves de sessão que são únicas para cada conversa e que são regularmente renovadas através do protocolo Double Ratchet.

O protocolo Double Ratchet garante duas propriedades de segurança cruciais: forward secrecy (segurança progressiva) e backward secrecy (segurança regressiva). A forward secrecy assegura que, mesmo se uma chave de sessão for comprometida, ela não permitirá o acesso a mensagens futuras. A backward secrecy garante que uma chave comprometida não permitirá o acesso a mensagens passadas.

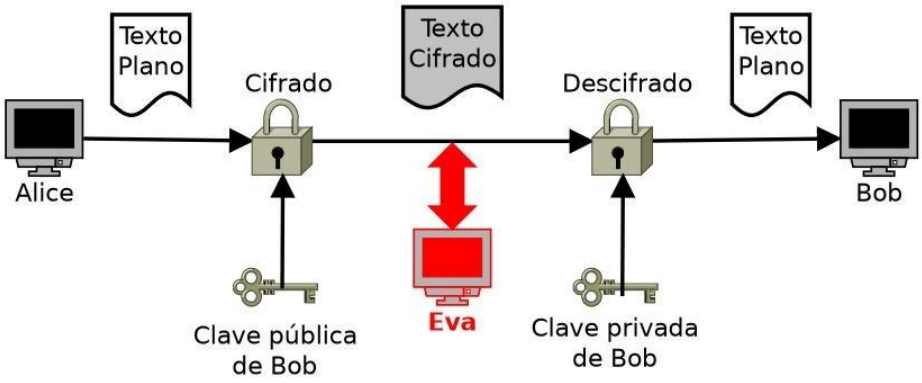

Figura 7: Sistema de Chaves

3.5 Implicações para a Interceptação

A combinação desses sistemas criptográficos torna a interceptação direta das comunicações WhatsApp tecnicamente impossível. Para que uma autoridade pudesse interceptar e decifrar uma comunicação, ela precisaria ter acesso simultâneo a:

1. As chaves privadas de longo prazo de ambos os usuários

2. As chaves efêmeras específicas da sessão

3. O estado interno do protocolo Double Ratchet no momento da comunicação

As informações são geradas, armazenadas e processadas exclusivamente nos dispositivos dos usuários, nunca sendo transmitidas em formato não criptografado ou armazenadas nos servidores da Meta. Mesmo que uma autoridade obtivesse acesso aos servidores da empresa, encontraria apenas dados criptografados que são matematicamente impossíveis de decifrar sem as chaves apropriadas.

A nova arquitetura de segurança representa uma mudança fundamental no paradigma das comunicações digitais, transferindo o controle da segurança das empresas de tecnologia para os próprios usuários. É uma evolução tecnológica que reflete a crescente importância da privacidade digital na sociedade contemporânea, mas que também apresenta novos desafios para as investigações criminais e a aplicação da lei.

4. Ligações de Áudio e Vídeo via WhatsApp: Arquitetura Técnica e Implicações para Interceptação

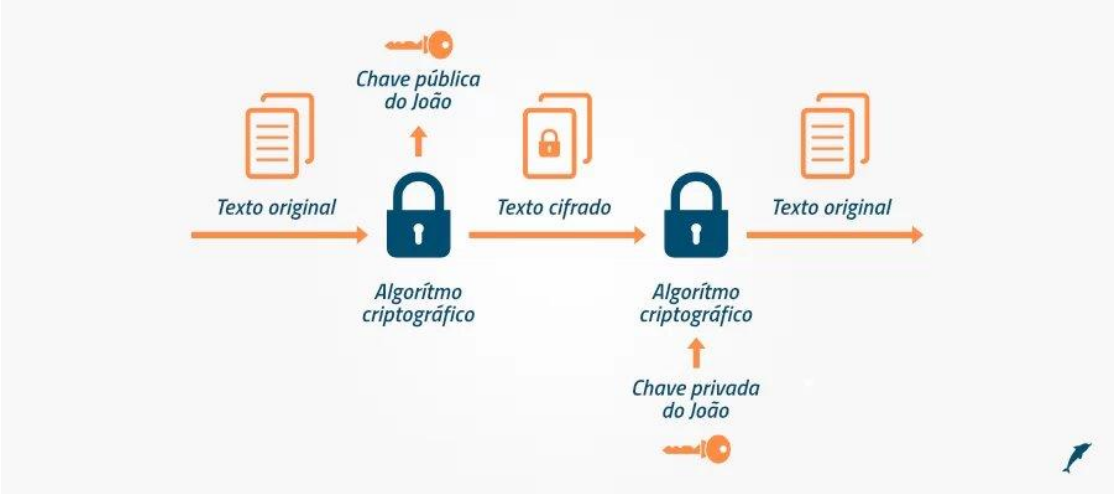

Figura 8: Chamadas WhatsApp

As ligações de áudio e vídeo realizadas através do WhatsApp representam uma das formas mais seguras de comunicação digital disponíveis atualmente. Compreender a arquitetura técnica dessas comunicações é fundamental para entender por que sua interceptação direta é tecnicamente impossível e por que as alegações sobre interceptação no caso ORUAN carecem de fundamento técnico.

4.1 Diferenças Fundamentais entre Ligações e Mensagens de Áudio

Uma das confusões mais comuns entre operadores do direito é a distinção entre ligações de áudio/vídeo e mensagens de áudio enviadas através do WhatsApp. Embora ambas envolvam conteúdo sonoro, suas arquiteturas técnicas são completamente diferentes, com implicações distintas para armazenamento, recuperação e possibilidade de acesso por terceiros.

As mensagens de áudio no WhatsApp são arquivos digitais que são gravados no dispositivo do usuário, criptografados e enviados como anexos através da infraestrutura de mensageria do aplicativo. Os arquivos são armazenados localmente nos dispositivos dos usuários e podem ser reproduzidos repetidamente. Do ponto de vista pericial, mensagens de áudio podem ser recuperadas através de análise forense do dispositivo, porque existem como arquivos armazenados no sistema de arquivos do aparelho/dispositivo.

As ligações de áudio e vídeo, por outro lado, são comunicações em tempo real que utilizam protocolos de streaming de mídia. O conteúdo dessas comunicações é transmitido diretamente entre os dispositivos dos usuários, sem ser armazenado como arquivos permanentes. Uma vez que a ligação termina, o conteúdo da conversa não existe mais em nenhum local, a menos que tenha sido especificamente gravado por um dos participantes [9].

Esta distinção é relevante para compreender as limitações da perícia digital. Enquanto mensagens de áudio podem ser recuperadas através de análise forense de dispositivos, o conteúdo de ligações de áudio e vídeo só pode ser acessado se houver gravações específicas realizadas pelos próprios usuários ou por software instalado nos dispositivos.

4.2 Diferenças Fundamentais entre Prints que são tirados e armazenados e a interceptação dos dados em tempo real

Uma das principais fontes de confusão em casos como o ORUAN é a distinção entre screenshots (capturas de tela) e interceptação real de comunicações. Frequentemente, alegações de "interceptação de áudio e vídeo via WhatsApp" referem-se, na realidade, a screenshots e gravações de tela encontrados durante perícia forense de dispositivos apreendidos.

Screenshots são criados pelo próprio usuário através de combinações de teclas no dispositivo, capturando uma imagem estática do que está sendo exibido na tela. Os arquivos ficam armazenados localmente na galeria do dispositivo e podem ser recuperados posteriormente através de perícia forense, desde que não tenham sido deletados ou o dispositivo não tenha sido formatado.

A interceptação real, por outro lado, envolveria capturar comunicações durante sua transmissão pela internet, o que é tecnicamente impossível devido à criptografia de ponta a ponta do WhatsApp. Quando autoridades apresentam "evidências de conversas WhatsApp", o método real de obtenção geralmente foi:

1. Apreensão legal do dispositivo
2. Perícia forense para extração de dados
3. Recuperação de screenshots armazenados na galeria
4. Análise e apresentação das imagens como evidência

Implicações jurídicas importantes: Screenshots podem ser facilmente editados ou manipulados, apresentam apenas momentos seletivos das conversas e não possuem a mesma força probatória de dados extraídos diretamente do banco de dados do aplicativo. Operadores do direito devem questionar especificamente o método de obtenção das evidências e solicitar esclarecimentos técnicos sobre a metodologia dos screenshots ou dados extraídos através de outros métodos.

4.3 Protocolos de Comunicação em Tempo Real

As ligações de WhatsApp utilizam protocolos especializados para comunicação em tempo real, incluindo variações do protocolo RTP (Real-time Transport Protocol) e SRTP (Secure Real-time Transport Protocol). Os protocolos são otimizados para minimizar a latência e garantir a qualidade da comunicação, mesmo em condições de rede adversas.

O protocolo SRTP adiciona uma camada de criptografia específica para comunicações de mídia em tempo real, complementando a criptografia de ponta a ponta já implementada pelo protocolo Signal. Isso significa que o áudio e vídeo das ligações são criptografados duas vezes: primeiro pela camada de aplicação (protocolo Signal) e depois pela camada de transporte (SRTP).

Durante uma ligação, os dispositivos estabelecem uma conexão direta (peer-to-peer) sempre que possível, ou utilizam servidores de retransmissão (relay servers) quando conexões diretas não são viáveis devido a configurações de rede. Em ambos os casos, o conteúdo da comunicação permanece criptografado de ponta a ponta, sendo descriptografado apenas nos dispositivos dos participantes da ligação.

4.4 Estabelecimento de Chamadas e Negociação de Parâmetros

O processo de estabelecimento de uma ligação WhatsApp envolve uma complexa negociação de parâmetros técnicos entre os dispositivos participantes. O processo inclui a troca de chaves de criptografia específicas para a sessão de mídia, a negociação de codecs de áudio e vídeo, e o estabelecimento de canais de comunicação seguros.

Quando um usuário inicia uma ligação, seu dispositivo envia uma solicitação criptografada através da infraestrutura de mensageria do WhatsApp. O dispositivo de destino recebe essa solicitação e, se o usuário aceitar a ligação, os dispositivos iniciam um processo de handshake criptográfico para estabelecer as chaves de sessão específicas para aquela ligação.

Uma vez estabelecidas as chaves de sessão, os dispositivos podem iniciar a transmissão de mídia criptografada. Todo o áudio e vídeo é processado em tempo real: capturado pelos sensores do dispositivo, criptografado, transmitido pela rede, recebido pelo dispositivo de destino, descriptografado e reproduzido. Este processo ocorre continuamente durante toda a duração da ligação, sem que o conteúdo seja armazenado em qualquer ponto intermediário.

4.5 Infraestrutura de Servidores e Limitações de Acesso

A infraestrutura de servidores do WhatsApp serve apenas como facilitadora para o estabelecimento de ligações e, quando necessário, como retransmissora de dados criptografados. Os servidores da Meta não possuem as chaves necessárias para descriptografar o conteúdo das ligações, funcionando apenas como "tubulações" por onde passam dados criptografados.

Mesmo que autoridades obtivessem acesso completo aos servidores da Meta, encontrariam apenas metadados sobre as ligações (horário de início, duração, participantes) e dados de

sinalização criptografados. O conteúdo real das conversações nunca está disponível nos servidores em formato descriptografado.

A arquitetura é fundamentalmente diferente da telefonia tradicional, onde as operadoras mantêm controle sobre o conteúdo das chamadas e podem implementar sistemas de interceptação mediante autorização judicial. No caso do WhatsApp, a empresa literalmente não possui capacidade técnica para interceptar ou gravar o conteúdo das ligações de seus usuários.

4.6 Qualidade de Serviço e Otimizações de Rede

As ligações WhatsApp implementam diversos mecanismos de otimização para garantir qualidade de serviço mesmo em condições de rede adversas. Os mecanismos incluem codificação adaptativa de áudio e vídeo, correção de erros, e ajuste dinâmico da qualidade baseado na largura de banda disponível.

As otimizações são implementadas de forma que preservem a segurança da comunicação. Por exemplo, quando a qualidade da rede é baixa, o sistema pode reduzir a resolução do vídeo ou a qualidade do áudio, mas nunca compromete a criptografia de ponta a ponta. A redução de qualidade ocorre após a descriptografia no dispositivo de destino, não durante a transmissão.

Figura 9: Arquitetura de Chamadas

4.7 Implicações para Investigações Criminais

A arquitetura técnica das ligações WhatsApp tem implicações diretas para investigações criminais. Do ponto de vista pericial, é importante compreender que:

1. Não há armazenamento central: O conteúdo das ligações não é armazenado nos servidores da Meta ou em qualquer outro local centralizado.

2. Não há capacidade de interceptação em tempo real: A criptografia de ponta a ponta torna impossível a interceptação do conteúdo das ligações durante sua transmissão.

3. Metadados limitados: Apenas informações básicas sobre as ligações (participantes, horários, duração) estão disponíveis nos servidores, e mesmo essas informações estão sujeitas às políticas de privacidade e retenção de dados da empresa.

4. Dependência de acesso aos dispositivos: Qualquer investigação que necessite do conteúdo de ligações WhatsApp deve focar no acesso aos dispositivos dos participantes, onde pode haver gravações locais ou outros vestígios digitais.

Em consequência, a realidade técnica exige que as autoridades desenvolvam novas estratégias investigativas que sejam compatíveis com as limitações impostas pela criptografia de ponta a ponta, sempre respeitando os direitos fundamentais dos indivíduos e os limites legais estabelecidos pelo ordenamento jurídico.

5. A Impossibilidade Técnica da Interceptação: Análise da Troca de Chaves e Barreiras Criptográficas

Figura 10: Segurança Digital

A impossibilidade técnica de interceptar comunicações de áudio e vídeo via WhatsApp transcendo a questão de política empresarial ou escolha tecnológica, incluindo a consequência matemática inevitável da arquitetura de segurança implementada. Este tópico

analisa detalhadamente os mecanismos que tornam essa interceptação impossível e esclarece por que alegações em contrário carecem de fundamento técnico.

5.1 O Processo de Troca de Chaves: Fundamento da Segurança

O protocolo de troca de chaves utilizado pelo WhatsApp é baseado no algoritmo X3DH (Extended Triple Diffie-Hellman), que estabelece um segredo compartilhado entre dois dispositivos sem que esse segredo seja jamais transmitido pela rede. O processo é fundamentalmente diferente dos sistemas de comunicação tradicionais, em que as chaves de criptografia podem ser conhecidas ou controladas por intermediários.

Quando dois usuários iniciam uma conversa no WhatsApp, seus dispositivos executam um protocolo criptográfico que combina múltiplas chaves: a chave de identidade de longo prazo de cada usuário, chaves pré-assinadas que são periodicamente renovadas, e chaves efêmeras geradas especificamente para aquela sessão de comunicação. O resultado deste processo é um conjunto de chaves de sessão que são matematicamente impossíveis de reproduzir sem acesso físico aos dispositivos envolvidos [10].

O aspecto importante do processo é que as chaves de sessão são derivadas através de operações matemáticas realizadas independentemente em cada dispositivo, utilizando dados/informações que nunca são transmitidas em formato não criptografado. Mesmo que um atacante intercepte toda a comunicação entre os dispositivos durante o processo de estabelecimento da sessão, não conseguirá derivar as chaves necessárias para descriptografar o conteúdo das comunicações (vimos antes no exemplo cotidiano).

5.2 Forward Secrecy e Backward Secrecy: Proteção Temporal

O protocolo Double Ratchet, implementado pelo WhatsApp através do protocolo Signal, garante propriedades de segurança que vão além da simples criptografia de ponta a ponta. A forward secrecy (segurança progressiva) assegura que, mesmo se uma chave de sessão for comprometida, ela não permitirá o acesso a comunicações futuras. A backward secrecy (segurança regressiva) garante que uma chave comprometida não permitirá o acesso a comunicações passadas.

As propriedades são implementadas através da renovação contínua das chaves de criptografia. A cada mensagem enviada ou recebida, o protocolo gera novas chaves derivadas das anteriores, mas matematicamente independentes. A consequência é a de que cada mensagem, chamada de áudio ou videochamada é protegida por chaves únicas que são automaticamente descartadas após o uso.

Para um interceptador hipotético, o efeito é que mesmo se conseguir quebrar a criptografia de uma comunicação específica (o que já é computacionalmente impossível com os recursos atuais), a conquista não lhe daria acesso a nenhuma outra comunicação da mesma conversa. Cada comunicação permaneceria protegida por suas próprias chaves únicas.

5.3 Impossibilidade Matemática da Interceptação Remota

A segurança das comunicações WhatsApp baseia-se em problemas matemáticos que são considerados computacionalmente intratáveis, mesmo para os computadores mais poderosos disponíveis atualmente. Os algoritmos utilizados (incluindo curvas elípticas e funções hash criptográficas) são baseados em problemas que exigiriam milhares de anos de processamento para serem resolvidos por força bruta.

Mais importante ainda, a arquitetura do sistema é projetada de forma que inexistam "chaves mestras" ou backdoors que permitiriam acesso privilegiado ao conteúdo das comunicações. Cada conversa é protegida por suas próprias chaves únicas, geradas e mantidas exclusivamente nos dispositivos dos participantes. Nem mesmo a Meta, empresa proprietária do WhatsApp, possui capacidade técnica para acessar o conteúdo das comunicações de seus usuários.

A impossibilidade não é teórica, mas prática e verificável. Organizações de segurança governamentais de diversos países, incluindo agências de inteligência com recursos computacionais praticamente ilimitados, têm reconhecido publicamente a impossibilidade de quebrar a criptografia implementada por aplicativos como o WhatsApp através de métodos de interceptação remota.

5.4 Métodos Reais de Acesso: Malware e Acesso Físico

Figura 11: Malware e Spyware

Embora a interceptação remota das comunicações WhatsApp seja tecnicamente impossível, existem métodos alternativos que podem permitir o acesso ao conteúdo das comunicações. Os métodos, no entanto, longe de quebrar a criptografia, significam o acesso ao conteúdo antes da criptografia ou após a descriptografia nos dispositivos dos usuários.

O método mais comum utilizado por investigadores e, infelizmente, também por criminosos, é a instalação de malware ou spyware nos dispositivos-alvo. Software malicioso como o "Bruno Espião" e outras ferramentas similares funcionam capturando o conteúdo das comunicações diretamente no dispositivo do usuário, antes que seja criptografado para envio ou após ser descriptografado para exibição. Daí uma das causas da confusão.

Os programas maliciosos podem capturar telas, gravar áudio ambiente, interceptar toques no teclado e até mesmo gravar chamadas de áudio e vídeo diretamente no dispositivo. Entretanto, a instalação requer acesso físico ao dispositivo ou a exploração de vulnerabilidades específicas do sistema operacional, sendo que a operação pode ser detectada por software de segurança adequado.

5.5 MALWARE - PEGASUS

Uma das ferramentas de malware mais sofisticadas que realmente permite acesso às comunicações WhatsApp é o Pegasus, desenvolvido pela empresa israelense NSO Group. Diferentemente das alegações impossíveis de interceptação remota, o Pegasus representa um método tecnicamente viável de acessar essas comunicações, sendo considerado pela comunidade de segurança digital como uma das armas cibernéticas mais avançadas já desenvolvidas. O software tem sido utilizado por diversos governos ao redor do mundo, incluindo casos documentados em países como México, Índia, Hungria e até mesmo alegações de uso contra jornalistas e ativistas de direitos humanos.

O Pegasus é instalado diretamente no dispositivo da vítima através de múltiplos vetores de ataque altamente sofisticados. Os exploits zero-day, que exploram vulnerabilidades desconhecidas em sistemas iOS e Android, representam o método mais avançado, permitindo infecção sem qualquer interação da vítima. Por exemplo, em 2021 foi descoberto que o Pegasus podia infectar iPhones através de uma vulnerabilidade no iMessage, simplesmente enviando uma mensagem que era processada automaticamente pelo sistema, sem que o usuário precisasse abrir ou visualizar qualquer conteúdo. Outros métodos incluem ataques de spear-phishing personalizados, onde a vítima recebe links maliciosos via SMS ou WhatsApp que parecem vir de contatos confiáveis, e até mesmo infecções por proximidade através de torres de celular falsas (IMSI catchers) que se fazem passar por antenas legítimas da operadora.

Uma vez instalado, o Pegasus obtém privilégios de administrador no dispositivo, realizando um processo conhecido como "jailbreak" em iPhones ou "root" em dispositivos Android, permitindo acesso irrestrito a todos os dados e funções do sistema operacional. Esta escalação de privilégios é fundamental para suas capacidades extensivas de monitoramento.

O spyware pode ativar remotamente a câmera e o microfone do dispositivo, capturar screenshots automaticamente em intervalos regulares, registrar todas as teclas digitadas (keylogging), acessar a localização GPS em tempo real, e extrair todos os arquivos armazenados, incluindo fotos, vídeos, documentos e bancos de dados de aplicativos. Um exemplo prático seria a capacidade de gravar secretamente uma videochamada do WhatsApp enquanto ela acontece, capturando tanto o áudio quanto o vídeo da conversa sem que os participantes tenham qualquer conhecimento da vigilância.

O aspecto mais importante para compreender é que o Pegasus não quebra a criptografia de ponta a ponta do WhatsApp (continua sendo matematicamente impossível mesmo para esta ferramenta avançada). Em vez disso, o software acessa o conteúdo nos pontos onde a criptografia não se aplica: antes da criptografia no dispositivo de origem ou após a descriptografia no dispositivo de destino. Por exemplo, quando uma pessoa digita uma mensagem no WhatsApp, o Pegasus pode capturar o texto através de keylogging antes mesmo que seja criptografado para envio. Da mesma forma, quando uma mensagem chega ao dispositivo de destino e é descriptografada para exibição na tela, o Pegasus pode capturar o conteúdo através de screenshots ou gravação de tela. Durante uma chamada de vídeo, o malware pode gravar diretamente o que está sendo exibido na tela e o áudio que está sendo reproduzido pelos alto-falantes, obtendo assim uma cópia completa da comunicação.

O Pegasus é projetado para operar de forma completamente invisível e persistente no dispositivo infectado. Não aparece na lista de aplicativos instalados, não possui ícone visível, consome recursos mínimos de bateria e processamento para evitar detecção, e pode se camuflar como processos legítimos do sistema operacional. O software possui capacidades de auto-atualização remota, permitindo que seus operadores instalem novas funcionalidades ou corrijam vulnerabilidades sem acesso físico ao dispositivo. Além disso, inclui mecanismos de auto-destruição que podem ser ativados remotamente para eliminar todas as evidências de sua presença, dificultando investigações forenses posteriores. Um exemplo da sofisticação do sistema é sua capacidade de detectar se está sendo executado em um ambiente de análise (como máquinas virtuais usadas por pesquisadores de segurança) e se comportar de forma diferente para evitar detecção e análise.

Alguns governos utilizavam o Pegasus para investigações de segurança nacional e combate ao terrorismo, sempre teoricamente com autorização judicial apropriada. Casos documentados incluem o uso pela polícia mexicana para investigar cartéis de drogas, pelas autoridades indianas em casos de terrorismo, e por agências europeias em investigações de crimes organizados. No entanto, o software também tem sido controversamente utilizado para vigilância de jornalistas, ativistas de direitos humanos, advogados e opositores políticos, levantando sérias questões sobre abuso de poder e violação de direitos fundamentais. O projeto Pegasus, uma investigação jornalística internacional de 2021, revelou uma lista de mais de 50.000 números de telefone que foram potenciais alvos do spyware, incluindo jornalistas do The Guardian, Financial Times e CNN, além de ativistas como os advogados de Jamal Khashoggi.

5.6 WhatsApp Web e Desktop: Vetores de Acesso Alternativos

As versões web e desktop do WhatsApp representam outro possível vetor de acesso ao conteúdo das comunicações. Estas versões funcionam como "espelhos" do aplicativo móvel, exibindo o mesmo conteúdo que está disponível no dispositivo principal do usuário.

Para utilizar o WhatsApp Web ou Desktop, o usuário deve escanear um código QR com seu dispositivo móvel, estabelecendo uma conexão criptografada entre o dispositivo móvel e o computador. Uma vez estabelecida essa conexão, o computador pode exibir e enviar mensagens, bem como participar de chamadas de áudio e vídeo.

Do ponto de vista investigativo, se as autoridades tivessem acesso físico ao computador de um suspeito e este computador estivesse conectado ao WhatsApp Web, seria possível acessar o conteúdo das comunicações através dessa interface. Contudo, isso ainda requereria acesso físico aos dispositivos do usuário e não constituiria interceptação remota das comunicações, e sim acesso por meios tendencialmente oportunistas.

5.7 Limitações e Considerações Éticas dos Métodos de Acesso

É importante ressaltar que todos os métodos reais de acesso ao conteúdo das comunicações WhatsApp envolvem acesso físico aos dispositivos dos usuários ou a instalação de software não autorizado. Estes métodos levantam questões éticas e legais significativas sobre privacidade, proporcionalidade e limites da investigação criminal.

No contexto brasileiro, a instalação de malware em dispositivos de suspeitos sem autorização judicial apropriada pode constituir violação de direitos fundamentais e tornar as evidências obtidas inadmissíveis em processos judiciais. É fundamental que as autoridades operem dentro dos limites legais estabelecidos e respeitem os direitos constitucionais, sendo vedado o aproveitamento direto de meios de prova criados para o mundo analógico, como a busca e apreensão (CPP, art. 240), para o mundo digital.

Figura 12: Perícia Digital

5.8 Acesso aos Dispositivos: O Caminho Legítimo para a Perícia Digital

O acesso físico aos dispositivos permanece o método mais eficaz e legalmente apropriado para obtenção de evidências digitais relacionadas a comunicações WhatsApp. Através de técnicas de perícia forense digital, é possível recuperar mensagens, arquivos de mídia e outros vestígios digitais armazenados nos dispositivos.

A perícia forense de dispositivos móveis é uma disciplina técnica especializada que utiliza ferramentas e metodologias específicas para extrair, preservar e analisar evidências digitais. O processo pode recuperar não apenas comunicações ativas, mas também dados que foram aparentemente "deletados" pelos usuários.

No entanto, é importante compreender que mesmo a perícia forense tem limitações quando se trata de comunicações WhatsApp. Mensagens que foram completamente removidas dos dispositivos, comunicações que ocorreram em dispositivos que foram posteriormente destruídos ou reformatados, e o conteúdo de ligações de áudio e vídeo que não foram gravadas localmente podem não estar disponíveis para recuperação.

A perícia digital representa o equilíbrio apropriado entre as necessidades investigativas legítimas e o respeito aos direitos fundamentais, operando dentro do espaço de conformidade estabelecidos pelos limites técnicos e legais claros, evitando o fornecimento às autoridades de acesso a evidências relevantes, abrangidos no âmbito de incidências das justas expectativas de privacidade e segurança de toda a coletividade, inclusive elevado à condição de garantia individual (CR, art. 5º, XXXIII).

6. Considerações sobre Casos Jurídicos e Alegações Infundadas

Figura 13: Interceptação Digital

O caso ORUAN não é isolado na jurisprudência brasileira. Diversas informações na mídia sobre processos judiciais, têm apresentado alegações sobre interceptação de comunicações via WhatsApp que carecem de fundamento técnico. O tópico analisa alguns desses casos e esclarece por que tais alegações são tecnicamente impossíveis, contribuindo para uma melhor compreensão dos limites e possibilidades da investigação digital.

6.1 Análise de Casos Jurisprudenciais

O Superior Tribunal de Justiça (STJ) já se manifestou em diversas ocasiões sobre a impossibilidade de interceptação direta de comunicações via WhatsApp. Em julgamento paradigmático, o tribunal estabeleceu que "não há analogia entre interceptação telefônica e espelhamento de conversas no WhatsApp", reconhecendo as diferenças técnicas fundamentais entre esses dois tipos de investigação [11].

A Corte reconheceu que, enquanto a interceptação telefônica tradicional permite a captura de comunicações em tempo real através da infraestrutura das operadoras, o acesso a comunicações WhatsApp requer métodos completamente diferentes, que não se enquadram na definição legal de interceptação telefônica estabelecida pela Lei 9.296/96.

Diversos tribunais estaduais têm seguido esse entendimento, estabelecendo que alegações de interceptação direta de comunicações WhatsApp devem ser analisadas com extremo ceticismo técnico. Casos em que agentes estatais afirmam ter interceptado comunicações de áudio e vídeo via WhatsApp frequentemente revelam, sob análise técnica detalhada, que se tratavam de outros tipos de evidência digital.

6.2 O Problema das Alegações Sensacionalistas

A busca por repercussão midiática tem levado alguns profissionais da área jurídica e policial a fazer alegações tecnicamente impossíveis sobre capacidades de interceptação digital. As alegações, frequentemente amplificadas pela imprensa em busca de manchetes impactantes, contribuem para a desinformação pública sobre as reais capacidades e limitações da investigação digital.

No caso específico do ORUAN, as alegações sobre interceptação de comunicações de áudio e vídeo via WhatsApp seguem um padrão comum: são apresentadas sem detalhamento técnico sobre como tal interceptação teria sido realizada, ignoram as barreiras criptográficas existentes, e são desacompanhadas de evidências técnicas que comprovem a viabilidade do método alegado (não se teve acesso aos autos originais; as considerações decorrem do informado ao público).

É fundamental que operadores do direito desenvolvam ceticismo técnico apropriado ao avaliar tais alegações. Afirmações extraordinárias requerem evidências extraordinárias, e a alegação de interceptação de comunicações criptografadas de ponta a ponta certamente se enquadra nesta categoria.

6.3 Impacto na Credibilidade das Investigações

Alegações tecnicamente impossíveis sobre capacidades de interceptação digital indicam desconhecimento técnico, além de comprometer a credibilidade de investigações legítimas. Quando autoridades fazem afirmações que são facilmente refutadas por especialistas em segurança digital, uma das consequências possíveis e a de gerar desconfiança pública sobre a competência técnica das instituições de controle social.

Mais grave ainda, as alegações podem levar à apresentação de evidências falsas ou mal interpretadas em processos judiciais. Se uma investigação afirma ter interceptado comunicações WhatsApp quando é tecnicamente impossível, surge a questão sobre a origem real das evidências apresentadas e sobre a integridade do processo investigativo (cadeia de custódia, p.ex.).

6.4 A Necessidade de Educação Técnica

A crescente importância das evidências digitais na justiça criminal torna essencial que operadores do direito desenvolvam conhecimento técnico básico sobre tecnologias de comunicação e criptografia. Não significa que todos os profissionais do direito devem se tornar especialistas em tecnologia, exigindo-se, pelo menos, o vocabulário específico, o entendimento e a compreensão dos limites e possibilidades das ferramentas digitais utilizadas em investigações.

Programas de educação continuada para operadores do direito deveriam incluir módulos sobre tecnologia digital, criptografia e perícia forense, especialmente quanto as provas digitais são cada vez mais empregadas em investigações e processos judiciais. A educação é fundamental para garantir que decisões judiciais sejam baseadas em compreensão técnica adequada e não em alegações sensacionalistas ou tecnicamente impossíveis.

7. Conclusões e Recomendações para a Prática Jurídica

Figura 14: Perícia Forense

Com base na análise técnica apresentada neste artigo, é possível estabelecer conclusões claras sobre a impossibilidade de interceptação direta de comunicações de áudio e vídeo via WhatsApp, bem como apresentar recomendações práticas para operadores do direito que lidam com evidências digitais.

7.1 Conclusões Técnicas Fundamentais

A interceptação direta de comunicações de áudio e vídeo via WhatsApp é tecnicamente impossível devido à implementação de criptografia de ponta a ponta baseada no protocolo

Signal. A impossibilidade não é uma questão de política empresarial ou escolha tecnológica, mas uma consequência matemática inevitável da arquitetura de segurança implementada.

As chaves de criptografia necessárias para descriptografar essas comunicações são geradas, armazenadas e processadas exclusivamente nos dispositivos dos usuários, nunca sendo transmitidas em formato não criptografado ou armazenadas nos servidores da Meta. Mesmo que autoridades obtivessem acesso completo à infraestrutura da empresa, encontrariam apenas dados criptografados que são matematicamente impossíveis de decifrar.

O conteúdo de ligações de áudio e vídeo não é armazenado em nenhum local após o término das comunicações, existindo apenas durante a transmissão em tempo real entre os dispositivos dos participantes. Logo, impossível a recuperação posterior dessas comunicações através de métodos de interceptação remota.

7.2 Métodos Legítimos de Investigação Digital

Embora a interceptação direta seja impossível, existem métodos legítimos e tecnicamente viáveis para obtenção de evidências relacionadas a comunicações WhatsApp. O acesso físico ou ao backup de nuvem dos dispositivos dos usuários, mediante autorização judicial apropriada, permite a realização de perícia forense que pode recuperar mensagens, arquivos de mídia e outros vestígios digitais.

A perícia forense de dispositivos móveis é uma disciplina técnica especializada que opera dentro de limites legais e técnicos claros. O método representa o equilíbrio apropriado entre as necessidades investigativas legítimas e o respeito aos direitos fundamentais dos cidadãos.

Técnicas de investigação tradicional, como vigilância física, análise de metadados de comunicação e correlação com outras fontes de evidência, continuam sendo fundamentais para investigações que envolvem comunicações digitais criptografadas.

7.3 Recomendações para Operadores do Direito

Para Magistrados: Desenvolvam ceticismo técnico apropriado ao avaliar alegações sobre interceptação de comunicações criptografadas, exigindo a entrega dos dados brutos, inclusive para que a defesa possa exercer o contraditório digital efetivo, com o detalhamento técnico específico sobre métodos alegados e consulta a especialistas independentes, se necessário.

Para membros do Ministério Público: Suporte em em evidências tecnicamente viáveis e legalmente obtidas, evitando afirmações sensacionalistas tecnicamente insustentáveis, com possível comprometimento da credibilidade e validade de toda a investigação.

Para Defensores: Questionem tecnicamente alegações de interceptação impossível, solicitando o detalhamento sobre métodos utilizados, além dos dados brutos e prova pericial independente sobre a viabilidade técnica dos métodos alegados.

Para Peritos Digitais: Mantenham-se atualizados sobre desenvolvimentos em criptografia e segurança digital, apoiando operadores do direito sobre limitações técnicas e possibilidades reais da perícia digital.

7.4 A Importância da Precisão Técnica

A precisão técnica em alegações sobre capacidades de investigação digital é uma questão de democracia processual, com implicações diretas no exercício de direitos fundamentais. Alegações tecnicamente impossíveis podem levar à apresentação de evidências falsas, comprometer a credibilidade das instituições de justiça e violar direitos e garantias constitucionais.

É fundamental que o sistema de justiça criminal adapte-se às realidades tecnológicas contemporâneas, desenvolvendo métodos de investigação que sejam tanto tecnicamente viáveis quanto legalmente apropriados. Para tanto, impõe-se a alocação de investimento em educação técnica, desenvolvimento de expertise especializada e estabelecimento de protocolos claros para lidar com evidências digitais.

7.5 Considerações Finais

O caso ORUAN serve como um lembrete importante sobre a necessidade de precisão técnica em investigações digitais. Alegações genéricas sobre interceptação de comunicações WhatsApp, quando tecnicamente impossíveis, indicam desconhecimento sobre as tecnologias envolvidas, além de possibilitar a contestação, associada ao comprometimento e a integridade da prova obtida durante o processo investigativo, exigindo-se conformidade nas informações transmitidas ao público em geral.

A criptografia de ponta a ponta representa uma evolução fundamental na proteção da privacidade digital, ampliando os desafios das investigações criminais. A resposta apropriada aos desafios exclui alegações tecnicamente impossíveis, enfraquecimento da criptografia, devendo se orientar pelo desenvolvimento de métodos de investigação que sejam compatíveis com as realidades tecnológicas contemporâneas.

Sobre o caso concreto ORUAN, não podemos nos manifestar diante da ausência de dados e informações da investigação realizada. No entanto, podemos afirmar que as notícias divulgadas quanto à interceptação do whatsapp são tecnicamente inválidas.

O futuro da justiça criminal em um mundo digital depende da capacidade das instituições de justiça de compreender e se adaptar às tecnologias emergentes, sempre respeitando os limites técnicos e legais que protegem os direitos fundamentais. Somente através de uma abordagem tecnicamente informada e legalmente responsável será possível manter a efetividade das investigações criminais sem comprometer a segurança e privacidade de toda a sociedade. Em resumo, conhecimento técnico reduz a margem de afirmações inválidas e tecnicamente impossíveis.

Referências

[1] G1 Rio de Janeiro. "Oruam: Rapper é classificado como de 'alta periculosidade' no RJ". Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2025/07/24/oruam-classificado-preso.ghtml

[2] WhatsApp FAQ. "Sobre a criptografia de ponta a ponta". Disponível em: https://faq.whatsapp.com/820124435853543/?locale=pt_BR/

[3] Tecnoblog. "Como funciona a criptografia de ponta a ponta do WhatsApp". Disponível em: https://tecnoblog.net/responde/como-funciona-a-criptografia-de-ponta-a-ponta-do-whatsapp/

[4] Mailfence Blog. "Criptografia simétrica e assimétrica: Qual a diferença?". Disponível em: https://blog.mailfence.com/pt/criptografia-simetrica-x-assimetrica-qual-e-a-diferenca/

[5] Signal Protocol Documentation. Disponível em: https://signal.org/docs/

[6] ÉPOCA. "Como a polícia pode dar a volta na criptografia do WhatsApp". Disponível em: https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/como-policia-pode-dar-volta-na-criptografia-do-whatsapp.html

[7] TOTVS Blog. "Criptografia simétrica e assimétrica: confira a diferença". Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/criptografia-simetrica-e-assimetrica/

[8] Universidade Java. "Criptografia de chave pública ou assimétrica". Disponível em: https://www.universidadejava.com.br/

[9] Dizer o Direito. "A polícia pode se valer da utilização do espelhamento do Whatsapp". Disponível em: https://www.dizerodireito.com.br/2024/06/a-policia-pode-se-valer-da-utilizacao.html

[10] Silva e Silva Advogados. "DA IMPOSSIBILIDADE DE INTERCEPTAÇÃO JUDICIAL DAS CONVERSAS VIA WHATSAPP". Disponível em: https://silvaesilva.com.br/da-impossibilidade-de-interceptacao-judicial-das-conversas-via-whatsapp/

[11] JusBrasil. "STJ: não há analogia entre interceptação telefônica e espelhamento de conversas no WhatsApp". Disponível em: https://www.jusbrasil.com.br/artigos/stj-nao-ha-analogia-entre-interceptacao-telefonica-e-espelhamento-de-conversas-no-whatsapp/696005504