Ao Excelentíssimo Senhor Fabiano Contarato

Presidente da Comissão Parlamentar de Inquérito do Crime Organizado,

Senado Federal

Assunto: Esclarecimentos complementares à oitiva realizada em 24/02/2026, na 9ª Reunião da Comissão Parlamentar de Inquérito sobre o Crime Organizado

O Facebook Brasil agradece a oportunidade de participar da audiência realizada em 24/02/2024, dedicada à discussão de formas de colaboração entre os setores público e privado para a proteção de brasileiros contra crimes praticados no ambiente digital, especialmente fraudes e golpes.

Durante o encontro, os Excelentíssimos Membros da Comissão apresentaram questionamentos relevantes sobre temas adjacentes, conforme detalhado abaixo:

- **Exmo. Senador Alessandro Vieira:**
  - Aplicação das políticas do WhatsApp diante da criptografia de ponta-a-ponta, com especial atenção à atividades ilegais e exploração e abuso infantil (Notas taquigráficas, 10:24 e seguintes; 10:39 e seguintes).
  - Alcance da criptografia de ponta-a-ponta nos demais produtos da Meta (Notas taquigráficas, 10:47).
  - Notícia sobre a implementação da criptografia ponta-a-ponta no Messenger (Notas Taquigráficas, 10:43)
- **Exmo. Presidente Senador Fabiano Contarato:**
  - Cooperação do WhatsApp com as autoridades, Poder Judiciário e disponibilidade de dados (Notas taquigráficas, 10:51).
- **Exmo. Senador Eduardo Girão:**
  - Parcerias institucionais da Meta relacionadas ao combate à desinformação, moderação de conteúdo, monitoramento de usuários ou envolvimento da USAid (Notas taquigráficas, 11:03).
- **Exmo. Senador Sérgio Moro:**
  - Recomendação de conteúdo político (Notas taquigráficas, 11:15)

No espírito de colaboração e transparência, o Facebook Brasil passa a apresentar as respostas aos questionamentos acima, buscando contribuir de forma construtiva para o debate e para o aprimoramento das políticas de proteção digital no Brasil.

1. WhatsApp e a Aplicação de suas Políticas

O WhatsApp foi projetado para ajudar as pessoas a se comunicarem de forma privada e segura, sendo a segurança dos usuários uma prioridade central para o serviço.

Como parte desse compromisso, o WhatsApp proíbe o uso de seu serviço para o compartilhamento ou participação em atividades ilegais, conforme estabelecido em suas Diretrizes de Mensagens. Para mensagens privadas, isso inclui: conteúdo de apoio a organizações ou indivíduos designados como terroristas; e conteúdo de organização ou coordenação de crimes violentos ou violência contra outras pessoas, como conteúdo que constitua uma ameaça crível à segurança pública ou pessoal. O WhatsApp não permite que organizações ou indivíduos designados como terroristas, traficantes de drogas, ou indivíduos/organizações que representem ou apoiem tais partes tenham presença no aplicativo. Empresas que usem os produtos de mensagens do WhatsApp Business precisam aderir à Política de Mensagens do WhatsApp Business, que proíbe a venda, promoção ou de qualquer outro modo facilite a transação de bens e serviços ilegais por meio da plataforma. O serviço antecipa e se adapta continuamente a novos riscos, fornecendo ferramentas para proteger seus usuários. Para isso, o WhatsApp conta com uma equipe de integridade líder no setor e mecanismos de detecção capazes de identificar danos em seu produto e a seus usuários. Essas ferramentas permitem a aplicação efetiva das Diretrizes de Mensagens, Termos de Serviço e outras políticas aplicáveis.

Para garantir a aplicação efetiva das políticas, o WhatsApp utiliza diversos mecanismos. Quando um usuário denuncia outro usuário em uma conversa individual ou em grupo, o WhatsApp recebe até cinco das últimas mensagens enviadas pela conta denunciada ou no grupo denunciado. Os usuários também podem denunciar uma mensagem única, seja em conversas individuais ou em grupo, selecionando essa única mensagem para que seja enviada ao WhatsApp. Sistemas automatizados, incluindo classificadores, revisam informações não-criptografadas, como mensagens denunciadas e dados de grupos e comunidades, para identificar contas potencialmente violadoras de políticas. Essas ferramentas determinam a probabilidade de violação dos termos ou políticas do WhatsApp, podendo resultar em medidas automáticas, revisão humana adicional ou até banimento da conta. Sempre que o WhatsApp toma conhecimento de conteúdo ilegal ou violação de políticas, seja por detecção automatizada, denúncias de usuários ou encaminhamentos de terceiros, adota medidas para proteger a integridade do serviço.

O WhatsApp tem tolerância zero para exploração e abuso infantil, contando com recursos, controles e uma equipe dedicada de especialistas em segurança online, aplicação da lei, investigações e tecnologia. Quando toma conhecimento de compartilhamento de conteúdos que exploram ou colocam crianças em risco, o WhatsApp bane os usuários envolvidos e denuncia casos ao National Center for Missing and Exploited Children (NCMEC), que coordena ações com autoridades de todo o mundo.

Junto com o trabalho de detecção proativa, o WhatsApp incentiva as pessoas a reportarem conteúdo problemático para o WhatsApp, inclusive por meio de avisos no aplicativo quando um

usuário é contatado pela primeira vez, ou é adicionado a um grupo por alguém que não está em seus contatos salvos. Os usuários também podem bloquear ou denunciar uma conta individual ou grupo a qualquer momento e denunciar todo e qualquer conteúdo de mensagens e status, incluindo conteúdo efêmero. O WhatsApp oferece várias formas de denúncia, e o processo de denúncia é simples e anônimo para outros usuários na plataforma.

Os métodos de detecção do WhatsApp incluem o uso de tecnologias automatizadas avançadas, como a associação de fotos e vídeos, para escanear proativamente informações não-criptografadas (por exemplo, fotos de perfil, imagens de grupos e denúncias de usuários) e detectar imagens exploratórias já identificadas. O WhatsApp também trabalha com outras tecnologias para detectar novas imagens exploratórias que ainda não foram identificadas. Classificadores com tecnologia de aprendizado de máquina fazem uma varredura superficial de textos (como perfis de usuários e descrições de grupos) e avaliam os dados de grupos e os comportamentos suspeitos ligados ao compartilhamento de imagens de exploração infantil.

Usando essas tecnologias, o WhatsApp aplica as medidas cabíveis a centenas de milhares de contas todos os meses por suspeita de compartilhamento de imagens de exploração infantil, banindo contas violadoras da plataforma.

O WhatsApp também trabalha com provedores de lojas de aplicativos para prevenir a proliferação de aplicativos que contenham imagens de exploração infantil ou que tentem conectar pessoas interessadas em compartilhar esse tipo de conteúdo por meio de links de convite de grupo. O WhatsApp restringe a indexação de listas de links de convite de grupo em ferramentas de busca populares.

A criptografia faz parte de como o WhatsApp apoia a privacidade, segurança e proteção das pessoas que utilizam o serviço. Ela já é amplamente utilizada por outros grandes serviços de mensageria para ajudar a proteger as mensagens privadas das pessoas e fornecer a privacidade e segurança que elas esperam ao enviar mensagens para amigos e familiares. Por isso, o WhatsApp continuará mantendo a criptografia, ao mesmo tempo em que implementa outros recursos para ajudar a manter as pessoas seguras. O WhatsApp está comprometido em liderar a luta contra a exploração infantil online e continuará a dedicar atenção e recursos de forma significativa a esses esforços.

---

2. WhatsApp, Criptografia de Ponta-a-Ponta e Cooperação com Autoridades

Além das políticas de segurança e mecanismos de proteção mencionados, a criptografia de ponta-a-ponta é um elemento central do WhatsApp, especialmente no contexto de comunicações privadas. Quando um usuário conversa com outro pelo WhatsApp, as mensagens são protegidas por criptografia de ponta-a-ponta, o que significa que apenas os dispositivos de remetente e do destinatário possuem as chaves necessárias para descriptografar o conteúdo. O WhatsApp não

tem acesso ao conteúdo dessas comunicações, pois a criptografia e a descriptografia delas ocorrem inteiramente no dispositivo dos usuários, e as chaves mudam a cada mensagem enviada.

Devido a essa arquitetura, não é possível quebrar ou contornar a criptografia sob demanda, mesmo em resposta a ordens judiciais. O WhatsApp não possui a capacidade técnica de descriptografar mensagens ou chamadas, e não mantém "chaves mestras" que permitiriam acesso ao conteúdo das mensagens e introduzir uma “porta dos fundos" comprometeria a segurança de todos usuários, criando vulnerabilidades exploráveis por agentes mal-intencionados.

Essa impossibilidade técnica é reconhecida por especialistas e respaldada por decisões do Superior Tribunal de Justiça e de tribunais federais brasileiros, que afastam sanções quando o cumprimento é materialmente impossível. Ministros do Supremo Tribunal Federal, no âmbito dos votos já proferidos na ADI 5527 e ADPF 403, apontam a criptografia de ponta-a-ponta como um direito fundamental e reconhecem a incapacidade técnica do WhatsApp de acessar conteúdo sem enfraquecer as proteções de privacidade.

Apesar dessas limitações técnicas, o WhatsApp coopera plenamente com investigações criminais, em estrita conformidade com a legislação brasileira. Por meio de um Sistema Online de Solicitações para Autoridades, disponível 24h, todos os dias da semana, o WhatsApp fornece informações disponíveis, como informações básicas de usuário, 6 meses de registro de acesso para contas de DDI+55, foto de perfil, histórico de alteração de número, agenda de contatos e dados de grupos e canais. Além disso, em resposta a ordens de interceptação, também pode começar a coletar e fornecer, por até quinze (15) dias, informações relativas a como a conta-alvo interage com outras pessoas usando o serviço WhatsApp. Oferecemos, também, tratamento expedito a demandas de autoridades, em casos de emergência, com risco iminente à vida ou lesão física grave.

O WhatsApp recebe regularmente feedback das autoridades policiais e judiciais brasileiras de que sua cooperação tem sido útil no avanço de investigações e no apoio a resultados concretos de casos, evidenciando que mesmo diante das limitações técnicas impostas pela criptografia ponta-a-ponta, o WhatsApp mantém uma postura de colaboração contínua e eficaz, em total conformidade com a legislação nacional, sem comprometer a segurança das comunicações privadas dos usuários.

---

3. Criptografia de Ponta-a-Ponta em Outros Produtos da Meta

Em atenção à extensão da criptografia ponta-a-ponta nos produtos Meta e WhatsApp, gostaríamos de retificar a informação apresentada na reunião anterior, após checagem com equipes internas especializadas, e esclarecer que a Meta implementa criptografia de ponta-a-ponta em outros produtos de mensagens, em diferentes estágios e configurações, conforme detalhado abaixo:

WhatsApp. A criptografia de ponta-a-ponta está habilitada para chats individuais com outros usuários, chats em grupo com outros usuários, chamadas de voz/vídeo com outros usuários, mídia, status publicados por usuários e grupos de anúncios de comunidades, e ela é mantida em dispositivos vinculados. Os backups estão desativados por padrão; os usuários podem optar por backups na nuvem com a opção de criptografia de ponta-a-ponta disponível.

Instagram. A criptografia de ponta-a-ponta foi disponibilizada como recurso opcional no Direct do Instagram, não definido por padrão, para mensagens privadas. Para ativá-la é preciso ir nas configurações das conversas com cada pessoa e optar pela criptografia ponta-a-ponta.

Messenger (incluindo mensagens pessoais do Facebook). A criptografia de ponta-a-ponta está habilitada por padrão para mensagens pessoais individuais no Messenger e no Facebook, e funciona da mesma forma seja quando o usuário envia mensagens pelo aplicativo do Messenger ou pelo aplicativo do Facebook. A implementação da criptografia de ponta-a-ponta para chats em grupo está em andamento. Todo o texto, mídia, chamadas de voz e vídeo dentro de chats criptografados de ponta-a-ponta também são criptografados.

As preocupações específicas relacionadas ao caso do Novo México foram levantadas em 2019 e representam a razão pela qual a Meta desenvolveu uma série de novos recursos de segurança para ajudar a detectar e prevenir abusos, todos projetados para funcionar em conjunto aos chats criptografados. Antes de migrar para a criptografia por padrão para conversas pessoais Messenger, engenheiros da Meta, criptógrafos, designers, especialistas em políticas e gerentes de produto da Meta trabalharam incansavelmente para introduzir novos recursos de privacidade, segurança e controle. Isso inclui controles de entrega de mensagens, que permitem que as pessoas escolham quem pode enviar mensagens para elas, bem como o “app lock” que usa as configurações de privacidade do celular, como biometria ou reconhecimento facial, para destravar o aplicativo por senha, além de recursos de segurança já existentes como denúncia, bloqueio e solicitações de mensagem. A Meta trabalhou em estreita colaboração com especialistas externos, acadêmicos, ativistas e governos para identificar riscos e construir mitigações para garantir que privacidade e segurança caminhassem juntas.

É importante ressaltar que a implementação da criptografia no Messenger não prejudica o compromisso da Meta de cooperar com as autoridades policiais, nem significa que a Meta parou de reportar conteúdo prejudicial ao NCMEC. De fato, a Meta passou mais de uma década desenvolvendo políticas e tecnologias para ajudar a manter os jovens seguros e impedir que predadores tentem usar os serviços para se conectar uns com os outros. O compromisso abrangente da Meta inclui uso extensivo de tecnologia para prevenir, detectar, remover e denunciar violações de suas políticas que proíbem a exploração infantil. A Meta trabalha com profissionais, colabora com a indústria e coopera com as autoridades em todo o mundo para combater a exploração online de crianças. Por exemplo, a Meta responde a solicitações proferidas no escopo de investigações criminais, fornecendo dados de usuários às autoridades no Brasil de acordo com a legislação brasileira.

Além disso, a Meta utiliza ferramentas de inteligência artificial que podem ajudar a detectar proativamente contas envolvidas em padrões de comportamento potencialmente maliciosos com base em indicadores não-criptografados, uma capacidade que ajuda a Meta a identificar e resolver problemas em seus serviços. Adicionalmente, a tecnologia de aprendizado de máquina da Meta pode analisar informações não-criptografadas de suas plataformas, como informações de conta e fotos carregadas em espaços públicos, para detectar atividades potencialmente suspeitas e abuso. Para ajudar a Meta a responder rapidamente a violações de suas políticas, a Meta também incentiva as pessoas a reportarem mensagens tanto em serviços criptografados quanto não-criptografados. A Meta tornou suas ferramentas de denúncia mais fáceis de encontrar e passou a incentivar adolescentes a denunciar em momentos relevantes, como quando bloqueiam alguém.

4. Parcerias Institucionais e Recomendação de Conteúdo Político

A Meta mantém relações institucionais com autoridades brasileiras, sempre pautadas pela transparência e pelo apoio a objetivos legítimos de interesse público. Entre as iniciativas divulgadas publicamente, destacam-se a adesão aos esforços do Supremo Tribunal Federal no Programa de Combate à Desinformação, para desenvolver iniciativas e projetos de combate à desinformação, de promoção da educação a parceria com o Ministério da Justiça e a Secretaria Nacional de Segurança Pública (SENASP) para oferecer o programa Amber Alert[1]. Durante o ciclo eleitoral, a Meta também firmou acordo com o Tribunal Superior Eleitoral (TSE), que perdurou até, até 31 de dezembro de 2024, incluindo mensagens informativas sobre as eleições, canal oficial no WhatsApp, transparência na biblioteca de anúncios e recebimento de denúncias sobre conteúdos e contas suspeitas de disparo em massa, sem implicar nenhuma obrigação de tomada de ação que não estivesse em linha com as políticas da empresa.

Importante ressaltar que a Meta não firmou qualquer parceria, financiou, forneceu cooperação técnica ou participou de projetos no Brasil envolvendo a USAID (Agência dos Estados Unidos para o Desenvolvimento Internacional) ou entidades financiadas pela USAID relacionados a combate à desinformação, moderação de conteúdo ou integridade da informação.

A liberdade de expressão é um direito humano internacionalmente consagrado e, como tal, integralmente observado pela Meta. Entre 2021 e 2024, a Meta fez mudanças para reduzir a quantidade de conteúdo cívico que as pessoas viam — posts sobre eleições, política ou questões sociais — com base no feedback dos seus usuários, que disseram querer ver menos desse tipo de conteúdo. Mas essa foi uma abordagem bastante direta e que não considerou nuances. Desde o início deste ano, a Meta retomou a recomendação desse tipo de conteúdo no Facebook, Instagram e Threads de forma mais personalizada, para que as pessoas que desejam ver mais conteúdo político em seus feeds possam fazê-lo.

[1] Por meio do Amber Alert, o MJ/SENASP consegue divulgar rapidamente alertas verificados sobre crianças desaparecidas para pessoas na região envolvida através das plataformas da Meta, possibilitando a rápida localização dessas crianças.

Em 2025, a Meta passou a tratar o conteúdo cívico de perfis e Páginas que usuários seguem no Facebook de forma semelhante a qualquer outro conteúdo do feed, classificando e mostrando esse conteúdo com base em sinais explícitos (por exemplo, curtir um conteúdo) e sinais implícitos (como visualizar posts), que nos ajudam a prever o que é significativo para os usuários. Também passamos a recomendar mais conteúdo político com base nesses sinais personalizados e ampliar as opções para que as pessoas possam controlar quanto desse conteúdo desejam ver.

Com isso, reiteramos que a Meta está atenta ao impacto que suas regras e sistemas têm na capacidade de as pessoas fazerem suas vozes serem ouvidas, e disponível para ajustar sua abordagem quando necessário.

Considerações Finais

O Facebook Brasil reafirma seu compromisso com o diálogo transparente e construtivo junto à Comissão e nos colocamos à disposição para esclarecer dúvidas, fornecer informações adicionais e colaborar com futuras discussões.

gov.br
Documento assinado digitalmente
YANA DUMARESQ SOBRAL ALVES
Data: 06/03/2026 18:41:01-0300
Verifique em https://validar.iti.gov.br

Atenciosamente,

Yana Dumaresq Sobral Alves

Facebook Serviços Online do Brasil Ltda.