

Conectando juventudes à segurança digital: Criptografia e literacia em foco



Conectando juventudes à segurança digital: Criptografia e literacia em foco

AUTORIA

Luiza Correa de Magalhães Dutra
Paulo Rená da Silva Santarém
Wilson Guilherme Dias Pereira

REVISÃO INTERNA

Ana Bárbara Gomes Pereira

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO

Felipe Duarte
Imagens: Freepik

PRODUÇÃO EDITORIAL

IRIS - Instituto de Referência em Internet e Sociedade

COMO REFERENCIAR EM ABNT

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva. **Conectando juventudes à segurança digital: Criptografia e literacia em foco**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2025. Disponível em <<https://bit.ly/41sq0Zz>>. Acesso em: dd mmm. aaaa.

Esta publicação é financiada pela Meta. Todos os projetos do IRIS são realizados de forma independente, de acordo com parâmetros de ética em pesquisa como replicabilidade, cientificidade e aqueles descritos no estatuto do IRIS. Todos os resultados são publicados e disponíveis de forma livre e gratuita e não têm qualquer intervenção ou, sob nenhuma hipótese, aprovação prévia da instituição financiadora.





INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Ana Bárbara Gomes

Paloma Rocillo

MEMBROS

Felipe Duarte | Coordenador de Comunicação

Fernanda Rodrigues | Coordenadora de Pesquisa e Pesquisadora

Júlia Caldeira | Pesquisadora

Júlia Tereza Koole | Estagiária de pesquisa

Luisa Melo | Estagiária de pesquisa

Luiza Correa de Magalhães Dutra | Pesquisadora

Paulo Rená da Silva Santarém | Pesquisador

Thais Moreira | Analista de comunicação

Vitória Santos | Pesquisadora

Wilson Guilherme | Pesquisadore

irisbh.com.br

Sumário

| | |
|---|-----------|
| APRESENTAÇÃO | 5 |
| AGRADECIMENTOS | 7 |
| 1. INTRODUÇÃO | 9 |
| 2. METODOLOGIA DO ENCONTRO | 10 |
| 3. APRESENTAÇÃO DOS RESULTADOS | 11 |
| 3.1. Premissas gerais do encontro | 11 |
| 3.2. Estação 1: Engajamento dos adolescentes nas práticas de segurança da informação e criptografia | 13 |
| 3.3. Estação 2: Engajamento nas discussões e construção de tecnologias | 18 |
| 3.4. Estação 3: Diversidade e representatividade | 22 |
| 4. RECOMENDAÇÕES | 27 |

Apresentação

O IRIS é um centro de pesquisa independente e interdisciplinar dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, além de defender e fomentar políticas públicas que avancem os direitos humanos na área digital. Assim, sua atuação busca trazer insumos científicos aos usuários da internet e aos diferentes setores que compõem a sociedade: governo, sociedade civil, setor privado, comunidade técnica e acadêmica.



Na área de criptografia e segurança digital, desenvolvemos dois principais projetos de pesquisa intitulados: “Comunicações privadas, investigações e direitos” e “Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL”.

No primeiro estudo, focamos em oferecer subsídios confiáveis para o debate político e jurídico sobre investigações em comunicações privadas no Brasil, buscando equilibrar a segurança das tecnologias da informação com a proteção dos direitos humanos e das garantias democráticas. A análise envolveu a avaliação de impactos e riscos, a sistematização do conhecimento científico e a formulação de recomendações para os setores público e privado. Foram analisados três mecanismos de investigação de comunicações privadas: rastreabilidade de mensagens instantâneas, hacking governamental e varredura no lado do cliente.

Na segunda pesquisa, nosso foco foi direcionado para crianças e adolescentes. O objetivo principal foi analisar o campo de debate político e jurídico sobre os campos de combate à violência sexual contra crianças e adolescentes e a defesa da criptografia como tecnologia de proteção ao direito à privacidade. Ambas as questões frequentemente são apresentadas como incompatíveis, com o argumento de que a criptografia forte seria conivente com

as violências sexuais online. O projeto, assim, visou analisar as propostas normativas e tecnológicas desenvolvidas nos países do MERCOSUL, sistematizando os conhecimentos e discursos gerados nesses territórios.

Os resultados destes estudos foram as produções de relatórios de pesquisa, policy papers, textos de blog e um site interativo, conforme resumidamente elencado abaixo:

- Relatório final [“Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas”](#);¹
- Relatório final [“Varredura pelo lado do cliente: uma revisão de literatura”](#);²
- Relatório final [“Hacking Governamental: uma revisão sistemática”](#);³
- Policy paper [“Recomendações sobre privacidade das comunicações, investigações e direitos digitais”](#);⁴
- Guia Informativo [“Artefatos Normativos Sobre Direitos de Crianças e Adolescentes em Ambientes Digitais no MERCOSUL”](#);⁵
- Relatório Final [“Segurança Da Informação E Proteção De Crianças E Adolescentes: Discursos E Propostas Regulatórias No MERCOSUL”](#);⁶
- Policy paper [“Recomendações sobre a proteção de crianças e adolescentes em ambientes com criptografia no MERCOSUL”](#).⁷

1 RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em: <<https://bit.ly/3yLlb0P>>

2 PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Varredura pelo lado do cliente: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022.

3 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Hacking Governamental: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <<https://bit.ly/3YdVcIL>>

4 DUTRA, Luiza Correa de Magalhães; GOMES, Ana Bárbara; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva. Recomendações sobre privacidade das comunicações, investigações e direitos digitais. Belo Horizonte: Instituto de Referência em Internet e Sociedade, dezembro de 2022. Disponível em: <<http://bit.ly/3ViK38I>>.

5 DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigue; PEREIRA, Wilson Guilherme Dias. Guia Informativo: Artefatos Normativos Sobre Direitos de Crianças e Adolescentes em Ambientes Digitais no MERCOSUL. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/3VsxQzz>.

6 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Segurança Da Informação E Proteção De Crianças E Adolescentes: Discursos E Propostas Regulatórias no MERCOSUL. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/3BEsMI9>.

7 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva. Recomendações sobre a proteção de crianças e adolescentes em ambientes com criptografia no

A partir dos indícios de que a falta de participação de adolescentes no debate sobre criptografia pode ensejar soluções ineficazes e perpetuar um baixo letramento digital, promovemos, agora, o encontro “**Conectando juventudes à segurança digital: Criptografia e literacia em foco**”, que proporcionou a reunião de especialistas de abordagem multidisciplinar para discutir propostas de como avançar os temas de segurança e criptografia para adolescentes . Este relatório, portanto, apresenta os seus resultados, bem como sua metodologia e referências.

Agradecimentos

A equipe de pesquisa do projeto “Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL” expressa sua profunda gratidão a todos os participantes do encontro “**Conectando juventudes à segurança digital: Criptografia e literacia em foco**”. Suas contribuições foram inestimáveis e fundamentais para o enriquecimento das discussões realizadas. Cada um de vocês trouxe uma perspectiva única e valiosa que ajudou a ampliar nossos horizontes e a aprofundar nosso entendimento sobre os temas abordados.

Agradecemos por dedicarem seu tempo e esforço para participar e fazer desta experiência uma oportunidade de aprendizado e troca de ideias. Que possamos continuar a cultivar essa colaboração e compartilhamento de conhecimento no futuro.

Nominalmente, gostaríamos de agradecer às pessoas participantes que permitiram a divulgação do seu nome neste relatório:⁸

- Ana Claudia Cifali - Instituto Alana
- Marcos Cesar - IPREc
- Ariel Pimentel - Rede Transfeminista
- Violeta Cunha - Rede Transfeminista
- Catharina Vilela - InternetLab
- Jade Lopes - Serenas
- Guilherme Klafke - FGV

MERCOSUL. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em <https://bit.ly/4dGvJiE>.

⁸ As opiniões e perspectivas compartilhadas pelas pessoas participantes no workshop não necessariamente refletem as políticas e posicionamentos oficiais das instituições a que estão vinculadas.

- Júlia Fernandes de Mendonça - Data Privacy Brasil
- Anna Flora Werneck - Childhood
- Paula Bernardi - ISOC Global
- Lucas Lago - Instituto Aaron Swartz
- Leandro Mendonça - ASEc Brasil
- Débora Mate Mendes - UNIFAP (Universidade Federal do Amapá)
- George Augusto Valença Santos - UFRPE (Universidade Federal Rural de Pernambuco)

1. Introdução

No debate mundial sobre o uso da criptografia forte na proteção de comunicações privadas, surgem propostas de enfraquecimento a fim de facilitar a investigação e a persecução penal. Uma das questões emergentes é a proteção de crianças e adolescentes, com foco especial nos riscos de violências sexuais cometidas com o auxílio da tecnologia.

Em nosso relatório *Segurança Da Informação E Proteção De Crianças E Adolescentes: Discursos E Propostas Regulatórias no MERCOSUL*,⁹ Identificamos que falta debate público amplo sobre a conexão entre direitos de crianças e adolescentes e a segurança da informação, em particular em ambientes com criptografia. Mesmo as propostas normativas de segurança online desse público não contam com previsões expressas sobre criptografia. Em termos geográficos, verificamos uma concentração em interesses e questões do Norte Global, confirmada pela incipiente produção normativa sobre o tema no MERCOSUL. Dando um passo além, com inspiração no multissetorialismo, detectamos que também há uma baixa ou inexistente participação de crianças e adolescentes no debate, o que se reflete na ausência de reflexões e propostas que levem em conta os seus legítimos interesses.

Nesse cenário, o encontro **Conectando juventudes à segurança digital: Criptografia e literacia em foco** buscou congregiar pessoas de diferentes instituições do Terceiro Setor. Ao todo foram 14 especialistas envolvidos no tema - seja na questão da proteção online de crianças e adolescentes, seja na questão da defesa da criptografia forte. O objetivo foi propor **um ambiente de análise, reflexão e troca, em que especialistas convidados pudessem compartilhar suas visões, conceitos e perspectivas sobre os desafios e oportunidades presentes na promoção da participação de adolescentes nas discussões sobre criptografia**. Avaliando as dificuldades e as oportunidades, buscamos construir em conjunto **propostas práticas** que pudessem ser implementadas, a fim de impulsionar um novo caminho para a harmonização entre a proteção de direitos de crianças e adolescentes e o uso da criptografia forte.

A partir dos resultados desse encontro, buscaremos fortalecer uma rede de especialistas em torno da intersecção entre os temas, envolvendo técnicos e tomadores de decisão. Como primeiro passo, registramos neste relatório as estratégias cocriadas durante o evento.

9 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues. *Segurança Da Informação E Proteção De Crianças E Adolescentes: Discursos E Propostas Regulatórias no MERCOSUL*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/3BEsMl9>. Acesso em: 13 jan. 2025.

2. Metodologia do encontro

A organização do debate online foi baseada na metodologia [World Café](#). Nosso objetivo foi promover um espaço colaborativo e construtivo, com o intuito de responder coletivamente questões sobre a participação de adolescentes no tema da criptografia.

Antes do evento, fizemos um levantamento das instituições pertinentes e buscamos selecionar uma lista de nomes que pudessem trazer uma gama diversificada de saberes para nossa discussão coletiva, com equilíbrio entre a área de proteção de crianças e adolescentes e a área de segurança da informação. Ao todo, foram 14 participantes.

O evento, que aconteceu por meio da plataforma *Google Meet*, se iniciou com uma apresentação seguida de uma breve exposição sobre o tema e orientações gerais sobre a dinâmica. Em seguida, as pessoas participantes foram divididas em **três subgrupos** e encaminhadas para três salas virtuais separadas, denominadas estações, cada uma com um recorte temático distinto e uma pessoa da equipe de pesquisa atuando como facilitadora. A função da facilitação foi incentivar a discussão, organizar as atividades e registrar as principais ideias e conclusões em uma lousa interativa compartilhada, por meio da ferramenta *Miro*.

- **Estação 1: Engajamento dos adolescentes nas práticas de segurança da informação e criptografia**
- **Estação 2: Engajamento nas discussões e construção de tecnologias**
- **Estação 3: Diversidade e representatividade**

Para cada estação, preparamos um ponto de partida com premissas hipotéticas sobre o tema e um conjunto de perguntas orientadoras (ver [Apresentação dos resultados](#)), que foram enviados previamente por email ao grupo de especialistas. Em cada estação, as perguntas foram conduzidas levando em conta os acúmulos individuais das pessoas convidadas sobre o assunto, gerando propostas para as correspondentes questões centrais.

As respostas e manifestações das pessoas participantes foram anotadas e dispostas em *post-its* na plataforma *Miro*, criando um mapa visual de soluções e desafios em torno do tema central de cada estação. Seguindo o método do World Café, a cada proposta formulada, indagava-se ao grupo se havia consenso ou dissenso ou se era algo a se aprofundar.

As estações duraram 25 minutos, e, então, os subgrupos foram reorganizados de forma que cada especialista passasse pelos três temas e, também, houvesse rotatividade entre os participantes que dividiram a sala. Nesse segundo momento de discussão, além de serem provocadas reflexões sobre as premissas hipotéticas e as perguntas orientadoras, as pessoas eram incentivadas a considerar e dialogar com as ideias e conclusões do grupo anterior, registradas na lousa digital.

Finalmente, todas as pessoas retornaram à sala principal, onde cada integrante responsável pela facilitação apresentou um resumo dos resultados de cada estação. Dessa forma, foi possível que todo mundo tivesse uma visão global dos resultados, com espaço para eventual compartilhamento complementar de sugestões e reflexões sobre como conectar as juventudes aos debates e ações sobre criptografia.

Neste documento, a partir da síntese textual dos mapas visuais de *post-its*, consolidamos recomendações que buscam exprimir os resultados das atividades propostas elaboradas em conjunto pelo grupo de especialistas.

3. Apresentação dos resultados

Para sistematizar as informações do encontro, foram sumarizados os principais pontos de discussão, apresentando as premissas hipotéticas de cada estação, as perguntas orientadoras, e os pontos trazidos nos debates. Em seguida, apresentamos as recomendações que surgiram sobre as temáticas. Desta forma, propomos organizar as percepções dos participantes sobre os temas relacionados aos campos de segurança digital/criptografia e juventude, para que análises posteriores possam aprofundar as convergências possíveis.

3.1. Premissas gerais do encontro

As premissas iniciais compartilhadas com os participantes antes do encontro tinham como objetivo de justificar a discussão e planificar um ponto de partida comum. Elas foram construídas com base no acúmulo obtido ao longo do desenvolvimento do projeto de pesquisa realizado pelo IRIS e intitulado “[Segurança Da Informação E Proteção De Crianças E Adolescentes: Discursos E Propostas Regulatórias No MERCOSUL](#)”. Veja abaixo:

1. Segundo pesquisa realizada em outubro de 2023 pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação ([Cetic.br](#)),¹⁰ **aproximadamente 84% da população brasileira tem acesso à internet**, o que corresponde a cerca de 156 milhões de pessoas. **Esse índice alcança 95% entre os usuários de 9 a 17 anos**, o que significa que cerca de 25 milhões de crianças e adolescentes estão conectados à rede;
2. Pensando que, segundo Tic Kids 2024, 93% da população brasileira de 9 a 17 anos é usuária de Internet e **29% dos usuários de 9 a 17 anos reportaram ter passado por situações ofensivas, que não gostaram ou chatearam na Internet;**¹¹

10 [CETIC.BR](#) | [NIC.BR](#). Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros - TIC Domicílios 2023. 26 ago. 2024. Disponível em <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2023/>. Acesso em 13 jan. 2025.

11 [CETIC.BR](#). Tic Kids Online Brasil 2024 - Principais Resultados. 13 set. 2024. Disponível em <https://>

3. Levando em consideração que, segundo mesma pesquisa, **30% de crianças e adolescentes já tiveram contato com alguém na internet que não conheciam pessoalmente;**
4. **A implementação de criptografia forte protege dados pessoais e comunicações privadas de crianças e adolescentes, suas famílias e amigos,** tornando-os inacessíveis a terceiros mal-intencionados e dificultando ações de abusadores e exploradores online. Isso reduz riscos como grooming, vazamento de sexting e outras formas de violência sexual digital, funcionando como uma barreira adicional contra violências online;
5. **Inexiste legislação específica sobre a proteção dos direitos de crianças e adolescentes em ambientes digitais com criptografia,** especialmente em relação à violência sexual online, nos países do MERCOSUL;
6. **Os debates legislativos, no MERCOSUL, ainda são raros e incipientes,** sem garantir participação do público-alvo nas políticas públicas, o que limita o reconhecimento de crianças e adolescentes como sujeitos de direitos ativos;
7. **Ausência de normas legais** sobre criptografia na região do MERCOSUL;
8. Dentre os riscos da falta de regulação, pontuamos a possível **restrição desproporcional dos direitos** de cidadania, privacidade e liberdade de expressão, assim como a **possível exposição excessiva** de crianças e adolescentes a conteúdos inadequados devido à falta de medidas de segurança;
9. Esses riscos são agravados pela significativa **falta de letramento digital** e pela inexistência de abordagens discursivas apropriadas para a população jovem;
10. Propostas que enfraqueçam a criptografia ou permitam monitoramento digital excessivo de jovens são vistas como prejudiciais aos seus direitos fundamentais. Contudo, a defesa da criptografia forte não apresenta soluções práticas para equilibrar segurança e proteção contra violações online de crianças e adolescentes, com a **falta de iniciativas específicas** nos países estudados.

A partir destas premissas gerais, foram formuladas algumas hipóteses - visando estimular a conversa entre os especialistas, já que poderiam ser refutadas, contestadas, endossadas, e, enfim, disparar discussões sobre consensos e dissenso entre o grupo. São elas:

3.2. Estação 1: Engajamento dos adolescentes nas práticas de segurança da informação e criptografia

Para esta discussão, consideramos a seguinte **hipótese**:

***Premissa/problema:** há pouco engajamento de adolescentes em práticas de segurança da informação, como a criptografia. Como fazer com que esse debate faça parte da construção da cidadania digital de crianças e adolescentes brasileiros?*

Com base nisso, o objetivo foi de responder às seguintes **perguntas orientadoras**:

- I. Como viabilizar o letramento?
- II. Quais questões podem ser interessantes para adolescentes?
- III. Como fazer uma sensibilização para que a segurança digital e criptografia sejam compreendidas como ferramentas essenciais para proteção individual e coletiva?
- IV. Quais são as abordagens sobre criptografia que podem ser prioritárias a jovens?

Considerando o *Miro* (lousa digital) criado a partir da reunião na sala do *Google Meet*, tanto as premissas quanto as questões foram resumidas na tela da seguinte forma:

Estação 1

Aprofundar

Premissa/problema: Há pouco engajamento de crianças e adolescentes em práticas de segurança da informação, como a criptografia. Como fazer com que esse debate faça parte da construção da cidadania digital de crianças e adolescentes brasileiros?

Discorda da premissa, as juvenudes já estão se preocupando com sua segurança, especialmente no que diz respeito a segurança de sua sexualidade

É preciso construir mais pesquisas sobre o processo de escolhas de tecnologias.

Atrelar o processo de autonomia de crianças e adolescentes a partir da sala de aula, trazer o conteúdo para mais perto do conteúdo que já precisa ser dado.

Trabalhar de maneira melhor e mais técnica sobre as ferramentas de segurança e criptografia, cobrando inclusive de forma mais forte as empresas.

Hacktons, e comitês de participação de adolescentes, rodas de conversas, inserção de alertas de riscos.

Adaptar a linguagem dos avisos, como, por exemplo, o do whats.

Atrelar o conteúdo de criptografia e segurança a outras temáticas que são relevantes, como por exemplo vazemos de nuds.

Dinâmica: simulação de gabinetes de crise

Como viabilizar o letramento?

Traduzir os termos de criptografia para linguagens mais acessíveis, com metodologias que considerem as idades e a autonomia progressiva. Ex.: usar o bilhete como forma de exemplo.

Cuidar para que a tradução de criptografia, não substitua a responsabilidade das plataformas.

Campanhas de comunicação, bonitas, atrativas e convidativas, que valorize a estética, e engajamento de produtores de conteúdos.

É preciso refletir sobre o papel dos influenciadores nesse contexto

Materiais que demonstrem o que é a criptografia, falar sobre a parte mais de matemática também pode ser importante, e seu valor, na prática.

Cuidar para que o processo de letramento não seja adultocentrico

Formatos diferentes. Séries de episódios curtos.

Produção mão na massa das juvenudes.

Articulações de conteúdos, a partir da educação entre pares.

Quais questões podem ser interessantes para adolescentes?

Proteção de sexualidade online

Olhar interseccional para fazer esses diálogos.

ransomware

A violência facilitada pela tec.

Olhar mais pra tensão entre controle parental e criptografia, se for uma tensão...

Perspectivas de maior profissionalização de adolescentes. Mostrar como uma perspectiva profissional

Como fazer uma sensibilização para que a segurança digital e criptografia sejam compreendidas como ferramentas essenciais para proteção individual e coletiva?

Fazer o caminho inverso, olhar o que já aconteceu socialmente para poder fazer as intervenções: reengenharia.

Fazer mais perguntas sociais como: você se protege? de que você se protege? porque?

Como proteger, os adolescentes de conteúdos que eles são estimulados a acessar, como por exemplo, conteúdos de violência.

Como trabalhar a perspectiva da proteção do "lado mau" da criptografia, a criptografia protegendo crimes contra adolescentes

Quais são as abordagens sobre criptografia que podem ser prioritárias a jovens?

Apontar pras juvenudes que elus não precisam saber criar uma criptografia, mas sim, quais apps já usam, para que elus possam escolher. Apontar também estratégias de segurança de sites e afins.

Quais são práticas de criptografia, o que eles entendem, e se eles entendem.

Desse modo, foram encontrados os seguintes resultados:

3.2.1. Como fazer com que o debate sobre criptografia faça parte da construção da cidadania digital de crianças e adolescentes brasileiros?

- A premissa utilizada como base argumentativa de que adolescentes não estão engajados nas pautas de segurança digital e criptografia foi refutada pelas especialistas. **Não houve consenso** sobre tal premissa. Na visão de alguns convidados, pautas como a segurança sexual online de adolescentes, especialmente de corpos feminilizados, já faz parte da rotina das juventudes;
- Houve **consenso** sobre a perspectiva de que é preciso desenvolver mais pesquisas e investigações de como adolescentes e jovens escolhem as tecnologias/plataformas que utilizam. Tal resultado pode ser caminho vital para intervenções sociais;
- Houve **consenso** entre as pessoas especialistas sobre o importante papel que a sala de aula desenvolve no processo de tomada de autonomia tecnológica. Mesmo entendendo que as pessoas educadoras já se encontram com altas demandas de responsabilidades, e por vezes possuem baixo letramento digital, destacaram que um caminho possível seria a interdisciplinaridade do debate;
- A perspectiva da responsabilidade das empresas também foi suscitada de forma **consensual**. É preciso cobrar de forma mais assertiva suas responsabilidades quanto à implementação de técnicas mais avançadas de criptografia;
- Quanto a forma de engajar os adolescentes em discussões sobre criptografia e segurança digital, as pessoas especialistas foram **consensuais** em apontar caminhos possíveis, como a utilização de metodologias que reconheçam o protagonismo do indivíduo e o coloque como parte da solução, como *hackathon*, rodas de conversa, simulações de gabinetes de crise, comitês consultivos de participação de adolescentes e a inserção de alertas de riscos e seguranças com linguagens mais acessíveis;
- Houve **consenso**, ainda, em afirmar que o debate sobre criptografia deve ser atrelado a outras temáticas, como, por exemplo, vazamento de nudes e direitos sexuais online.

3.2.2. Como viabilizar o letramento?

- A tradução dos termos de criptografia para linguagens mais acessíveis, com metodologias que considerem inclusive as idades e a autonomia progressiva, foi um **consenso**. Entretanto, os especialistas indicaram como **ponto a aprofundar** o cuidado que se deve ter em não desresponsabilizar as empresas quando do uso dessas linguagens mais simplificadas;
- No contexto de campanhas, houve **consenso** na perspectiva de que a linguagem

precisa ser atrativa e convidativa, voltada para os jovens. Os especialistas apontaram como **ponto a aprofundar** a participação de influenciadores digitais neste quesito. O ponto de aprofundamento se baseia especialmente pela necessidade de cuidado com outros trabalhos já produzidos, para evitar conflito de posicionamentos;

- Outra abordagem para o letramento em criptografia apontado é a utilização de múltiplas linguagens, inclusive a técnica; isso considera a multiplicidade de interesses e contextos, pois existem adolescentes que são do campo de ciências exatas e podem enxergar na lógica matemática da criptografia um caminho promissor de confiança na técnica. Este apontamento foi **consenso** entre as pessoas especialistas;
- É preciso ter cuidado para que o processo de letramento digital não seja adultocêntrico. É importante, portanto, valorizar estratégias de educação entre pares e de experiências mais práticas de aprendizagem, valorizando diferentes formatos. Esta visão foi **consensual**.

3.2.3. Quais questões podem ser interessantes para adolescentes?

- As pessoas especialistas apontaram de forma **consensual** que o debate sobre direitos sexuais online, especialmente o combate ao vazamento de nudes, pode ser uma tópico potente para introduzir os debates sobre criptografia e segurança digital;
- Além disso, foi também **consensual** a necessidade de se estabelecer um diálogo interseccional que se atente às diversidades da adolescência;
- Outra perspectiva criativa para trabalhar essas temáticas com adolescentes é articulá-las com o direito à profissionalização. Ou seja, houve **consenso** de que o mercado de trabalho de cibersegurança pode ser mais explorado na perspectiva da profissionalização de adolescentes, mostrando inclusive que os aprendizados podem trazer não apenas a sua própria segurança, como também um meio de renda e uma profissão;
- Apesar de não estar diretamente ligado à perspectiva dos adolescentes, três outras questões também foram levantadas neste tópico como **pontos a aprofundar**: o primeiro deles foi a “tensão” entre autonomia e controle, especialmente na perspectiva de que a mediação parental pode ser vista como um confronto à autonomia que se promete para adolescentes a partir da criptografia;
- Os outros dois **pontos a aprofundar** foram os riscos de utilização de ferramentas com criptografia para facilitar a violência sexual online contra crianças e adolescentes, e o risco da utilização de softwares maliciosos como *ransomware* para captação de dados escolares destes grupos, com finalidades comerciais.

3.2.4. Como fazer uma sensibilização para que a segurança digital e criptografia sejam compreendidas como ferramentas essenciais para proteção individual e coletiva?

- Houve **consenso** entre as pessoas especialistas sobre a necessidade de fazermos o caminho inverso: ao invés de olharmos para as tecnologias digitais, olharmos primeiro para o aspecto social para ver quais casos se interconectam com a criptografia, para, assim, usá-los como *cases*. Isso poderia gerar uma espécie de “reengenharia”, explorando mais perguntas e não buscando respostas tão simplistas.

3.2.5. Quais são as abordagens sobre criptografia que podem ser prioritárias aos jovens?

- Quanto às abordagens, tentamos entender coletivamente com as pessoas especialistas quais os principais espaços onde essas criptografias seriam utilizadas no contexto dos adolescentes. A resposta coletiva seguiu de forma **consensual** para apontar o caminho dialógico de conversação com adolescentes, apostando em perguntar mais a esses sujeitos: “onde utilizam?”, “como utilizam?”;
- As pessoas especialistas foram ainda **consensuais** em apontar para o fato de que é importante que a comunicação seja eficiente para que adolescentes saibam que não precisam ser especialistas em segurança digital, mas que é muito importante entender quais as condutas mais seguras na vida online, assim como na vida offline.

3.3. Estação 2: Engajamento nas discussões e construção de tecnologias

Para esta discussão, foi considerado o seguinte par de hipóteses:

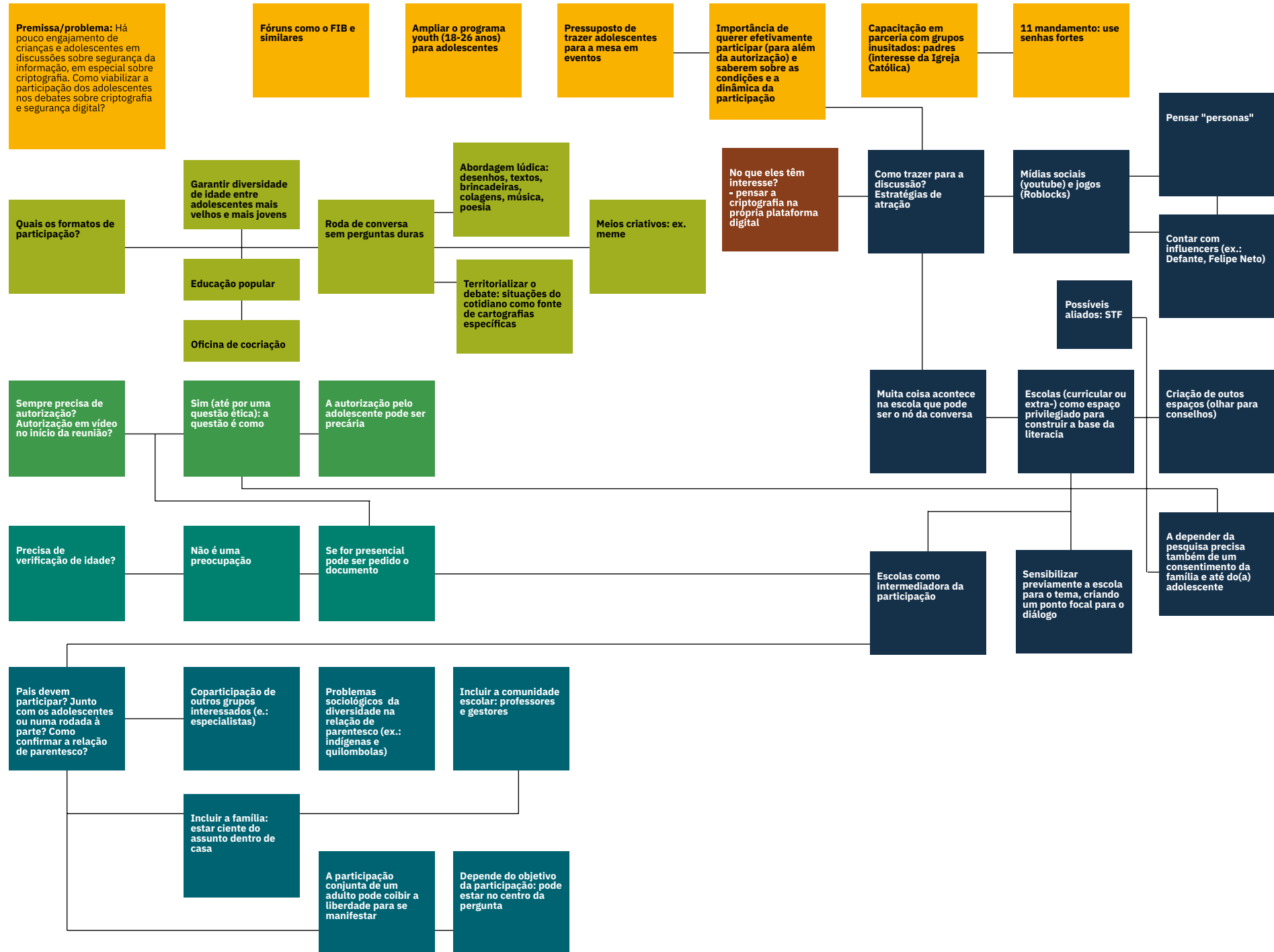
Há pouco engajamento de adolescentes em discussões sobre segurança da informação, em especial sobre criptografia. Como viabilizar a participação dos adolescentes nos debates sobre criptografia e segurança digital?

Com essa base, buscou-se responder às seguintes **perguntas orientadoras**:

- I. Quais os formatos de participação?
- II. Sempre precisa de autorização? Autorização em vídeo no início da reunião?
- III. Precisa de verificação de idade?
- IV. Pais devem participar? Junto com os adolescentes ou numa rodada à parte? Como confirmar a relação de parentesco?

Utilizando-se a lousa digital da plataforma Miro, mediante trocas na reunião online realizada na sala do Google Meet, gerou-se o seguinte mapa mental sintético:

Estação 2



Desse modo, foram construídos os seguintes resultados:

3.3.1. Quais podem ser os espaços de participação?

- Em **consenso**, apontou-se como primeira possibilidade aproveitar espaços como Fórum da Internet no Brasil – FIB, por exemplo, por meio da ampliação do programa *Youth* (que hoje abarca jovens entre 18 e 26 anos) para contemplar adolescentes;
- Em seguida, em **consenso**, reputou-se necessária a presença de adolescentes como um pressuposto para o debate de temas de seu interesse, destacando-se ser importante que haja seu efetivo interesse de participação (para além da autorização e possibilidade de preparação), bem como a devida informação sobre as condições e a dinâmica da participação nesses eventos;
- A fim de viabilizar o fomento e o amadurecimento desse interesse, em **consenso**, citou-se a iniciativa de formar parcerias com organizações que possam atuar na capacitação de adolescentes, incluindo parceiros que tenham como foco de atuação pautas distintas do digital, mas que também estão em contato direto com o público jovem. Neste momento, alguns participantes compartilharam experiências em que outros atores se mostraram disponíveis para aprender e replicar conhecimento sobre o tema (como líderes religiosos, por exemplo).

3.3.2. Como trazer adolescentes para a discussão?

- Houve **consenso** de que um ponto de entrada para atrair os adolescentes para o debate seria investigar os assuntos de seu interesse que se conectam com o tema, por exemplo, pensar a adoção concreta da criptografia nas plataformas digitais que eles usam;
- Em **consenso**, ponderou-se que as mídias sociais (por exemplo, youtube), jogos (Roblocks) e influencers de grande visibilidade (Felipe Neto) seriam exemplos de caminhos para fomentar o engajamento;
- De modo **consensual**, apontou-se que a aproximação deve considerar “personas” diferentes: diferentes estratégias devem ser traçadas para os diferentes tipos de adolescentes, considerando marcadores de raça, classe, idade, gênero, região etc;
- Também houve **consenso** na sugestão de escolas, em especial públicas, como espaço privilegiado para discussão, pois muitos acontecimentos escolares podem viabilizar a conversa, desde que haja uma sensibilização prévia para o tema, com a eventual criação de um ponto focal local para o diálogo. Ainda nesse aspecto, houve **consenso** de que outras instituições poderiam oferecer material de apoio, como o Supremo Tribunal Federal, que tem se dedicado ao tema recentemente;
- Diante do risco de sobrecarga ao ter a escola como intermediadora da participação, apontou-se em **consenso** a necessidade de voltar o olhar para outros espaços, como

os Conselhos de Direitos, integrantes do Sistema de Garantia de Direitos;

3.3.3. Quais os formatos de participação?

- Em **consenso**, foram citadas rodas de conversa sem perguntas duras (do tipo “como você vê a criptografia”) e oficinas de cocriação que permitam abordagens lúdicas por meio de desenhos, textos, brincadeiras, colagens, música, poesia e até memes;
- Também em **consenso**, apontou-se a educação popular como fonte de inspiração;
- Apontou-se, de forma **consensual**, a importância de territorializar o debate, por meio de situações cotidianas como fonte de cartografias específicas;
- Ainda, na construção das formas de participação, sugeriu-se, em **consenso**, garantir diversidade de idade entre adolescentes mais velhos e mais jovens.

3.3.4. Seria necessário obter autorização para a participação de adolescentes?

- Apontou-se em **consenso** ser necessário sempre obter a autorização para a participação, inclusive considerando a proteção de dados pessoais e questões éticas da pesquisa com seres humanos;
- Houve **consenso** de que a autorização dada por adolescentes pode ser precária, mas deve ser vista como um momento de formação;
- Em **consenso**, a escola foi apontada como possível intermediária para obter essa autorização;
- Apontou-se, também em **consenso**, que a questão da verificação de idade não é uma preocupação central e que, caso necessário, basta solicitar a apresentação de um documento oficial.

3.3.5. Qual poderia ser a participação da família?

- De início, em **consenso**, destacou-se a delicadeza e complexidade da questão do parentesco, que pode não ser tão evidente em grupos como indígenas e quilombolas;
- Houve **consenso** de que a presença de pais e mães pode inibir a livre manifestação, de modo que possibilidade dessa participação deve estar restrita a situações em que o objetivo abarque a interação entre os componentes da família, a exemplo de uma terapia de casal;
- Ao mesmo tempo, apontou-se de modo **consensual** que a família deve ser incluída como destinatária do assunto, para que este passe a ser relevante dentro de casa, bem como sendo importante que a comunidade escolar como um todo, incluindo professores e gestores, seja sensibilizada para o tema;

- Também em **consenso**, ressaltou-se a importância de ter cuidado na interação com quaisquer outros grupos de interesse, por exemplo, especialistas, de modo que não haja prejuízos ou deslegitimação durante a participação de adolescentes.

3.4. Estação 3: Diversidade e representatividade

Para esta discussão foi considerada a seguintes **hipótese**:

Há o risco de a eventual participação de adolescentes não alcançar uma diversidade representativa. Como reunir adolescentes em um grupo que seja representativo da diversidade brasileira, em termos de classe, região, inclusão digital, além de raça e gênero, nesses espaços discutidos?

Buscamos responder às seguintes **perguntas orientadoras**:

- I. Como reunir adolescentes em um grupo que seja representativo da diversidade brasileira, em termos de classe, região, inclusão digital, além de raça e gênero, nesses espaços discutidos?
- II. Conectividade significativa: como ouvir quem não tem internet?
- III. Como alcançar periferias e cidades não metropolitanas?
- IV. Como validar uma eventual abordagem restrita?
- V. Como impulsionar o desenvolvimento tecnológico voltado para o fortalecimento da segurança de crianças e adolescentes?

Considerando o Miro (lousa digital) criado a partir da reunião na sala do Google Meet, tanto as premissas quanto as questões foram resumidas na tela da seguinte forma:

Estação 3

| | | | | | | | | |
|--|--|--|--|--|---|---|---|---|
| Premissa/problemas: como reunir adolescentes em um grupo que seja representativo da diversidade brasileira, em termos de classe, região, inclusão digital, além de raça e gênero, nesses espaços discutidos? | Locais onde teriam representação de jovens: igrejas, escolas - como chegar nesses jovens | Escolas como ponto focal + redes de terceiro setor que atuam no território na ponta - forma de continuidade do contato | Pontos focais das organizações para engajar os grupos locais: acesso à diversidade de percepções | Outros formatos de acesso: rádio, TV - formas de chegar nas famílias também Conteúdo em áudio | Preparação da equipe é fundamental (para lidar com riscos, relatos) + considerar particularidade de cada contexto (adequar as conversas) + chamar os adolescentes | Trabalhar com pares - jovens falando com jovens - não colocar um adulto como interlocutor | Contrapartida para os jovens: trocas fora do encontro, perguntar, mostrar interesse - para além de meros objetos de estudos - certificado final | |
| Conectividade significativa: como ouvir quem não tem internet? | Se os adolescentes sabem o que é criptografia - momento de sensibilização sobre o tema | Que seja presencial esses encontros (mas aqui temos que pensar no custo) | Escolas-famílias | Diferença do perfil de uso da internet (ex: celular compartilhado entre a família) | IA na Sala de Aula (DP) | Construção de confiança | | |
| | Contar com movimentos sociais locais | Como avaliar o impacto da campanha? Quais métricas? | Escuta aberta - em um ambiente real | Falta de uma pesquisa qualitativa - parceria | Vans tecnológicas + rádios comunitárias + estimular ferramentas offline | | | |
| Como alcançar periferias e cidades não metropolitanas? | Escolas + terceiro setor: para chegar no público do campo (juventude camponesas) | Igreja como ponto central para acesso aos jovens | Mapeamento de instituições que já trabalham com o tema | Cuidado com a questão do "objeto de estudo" - ideia de "uso" - retorno, devolutiva | Pensar na questão do tempo: campanhas longas com criação de relações - com feedbacks durante o processo + processos práticos | Espaço para jovens participarem de eventos - construção política e possibilidade de viagens | Construir espaços feministas - perspectiva de empoderamento técnico - formas formadoras | |
| Como validar uma eventual abordagem restrita? | Procurar influenciadores que já falam com esse público - acesso com linguagem específica | Que tipo de representatividade estamos buscando? Por quais motivos se interessariam por criptografia? | Não tomar uma pessoa como representante de toda diversidade | Criação de materiais diversos, com conteúdos diversos, a partir de abordagens anteriores | Olimpíadas com prêmios - pensar em algo que estimule a participação | Feiras interativas + oficinas com foco nas realidades locais = forma de maior engajamento | Como produzir ferramentas tecnológicas para sua própria comunidade/- realidade - letramento digital | Construções com educadores diversos, do ensino básico - quem tem acesso direto aos estudantes |
| Como impulsionar o desenvolvimento tecnológico voltado para o fortalecimento da segurança de crianças e adolescentes? | Demanda dos jovens para ensinar o básico sobre cibersegurança | Materiais voltados para adolescentes | Cuidado com adolescentes neurodivergentes + | Termo de assentimento dos adolescentes + termo de consentimento dos pais | Adolescente colocar a "mão na massa" - ensino básico - fomento local | | | |

Desse modo, foram encontrados os seguintes resultados:

3.4.1. Conectividade significativa: como ouvir quem não tem internet? Como alcançar periferias e cidades não metropolitanas? Como reunir adolescentes em um grupo que seja representativo da diversidade brasileira, em termos de classe, região, inclusão digital, além de raça e gênero, nesses espaços discutidos?

- Foi **consenso** a importância de buscarmos locais de convívio social onde teriam representações de jovens em comunidades periféricas, como igrejas e escolas. Foi apontado que esses locais possuem vínculos estabelecidos com as comunidades e podem auxiliar no primeiro e contínuo contato com jovens. Ainda, foi destacado que as escolas e as organizações do terceiro setor que já atuem nesses locais podem, também, ser importantes pontos para continuidade de contato com esse grupo; ou seja, a busca por entidades que já trabalhem e tenham contato com estes jovens é de suma importância;
- Outro ponto apresentado, **mas que necessita ser aprofundado**, foi a possibilidade de uso de tecnologias alternativas para alcançar o público almejado, como conteúdo de áudios através de rádio e televisão. Esses meios alternativos podem auxiliar a chegada do debate sobre segurança digital em espaços com restrição à internet, tanto para os adolescentes, como para suas famílias;
- A busca por jovens para falar com os adolescentes destas comunidades também foi ponto de **consenso**; ou seja, jovens para falar com outros jovens, como forma de aproximação entre pares, afastando os adultos desta interlocução;
- Outro ponto de **consenso** apontado foi a importância de darmos uma contrapartida para os grupos de jovens que tenham contato; em outras palavras, tratá-los não como objetos de estudo, mas como pessoas que possuem questões e problemas reais e merecem ser ouvidas. A demonstração de interesse, as perguntas realizadas, e a escuta ativa foram apontados como caminhos possíveis. Neste sentido, apontaram a importância da preparação da equipe que irá trabalhar com esses jovens para lidar com riscos e relatos do campo, e entender as particularidades de cada contexto social que estão inseridos.
- Também destacaram a possibilidade de criação de campanhas de longa duração com feedbacks durante o processo, assim como a possibilidade destes jovens participarem de eventos do campo da governança da internet já existentes, como FIB e IGF. Esse ponto foi considerado **a ser aprofundado**, pois não se mostrou em total consenso;
- Alguns integrantes da estação trouxeram a importância de buscarmos fazer encontros presenciais com os adolescentes como forma de entendermos e ouvirmos se o tema de segurança digital e criptografia é já uma pauta debatida por esse grupo, para assim

as trocas serem estabelecidas e iniciadas, com a estruturação de confiança que o tema necessita. Considerado **ponto a aprofundar**, pois não se mostrou consenso;

- Na questão de gênero, foi **consenso** a ideia de construção de espaços feministas que tratem do tema de segurança digital a partir da perspectiva de gênero e de um empoderamento técnico, buscando formar meninas que sejam também formadoras sobre o tema em suas comunidades;

3.4.2. Como validar uma eventual abordagem restrita?

- Um dos pontos principais apresentados, em **consenso**, neste questionamento foi a busca por influenciadores digitais que já falem para o público adolescentes, não necessariamente sobre a temática de criptografia e segurança digital, mas que tenham uma linguagem específica e acessível para os jovens, o que facilitaria o diálogo e a escuta;
- Foi destacado o risco e a importância de não se tomar uma pessoa representante de determinada comunidade como a única pessoa representa e a “voz” deste local. Todos os espaços de interações sociais e construção de vínculos são diversos e formados por pessoas com diferentes perspectivas; daí a relevância de se conhecer, primeiro, a comunidade e o local onde se está buscando trabalhar. Ponto de **consenso**;
- Pensar na criação e divulgação de materiais diversos com linguagem acessível para os adolescentes também foi um ponto apresentado e **consensuado**. Ainda, trouxeram exemplos para engajamento dos jovens nestas pautas de segurança digital: olimpíadas com prêmios; feiras interativas; oficinas com foco nas realidades locais, foram algumas das formas apresentadas de engajamento;
- Um de nossos interlocutores apresentou a ideia de como produzir ferramentas tecnológicas nas próprias comunidades e que produzam dados para essas comunidades, buscando trabalhar futuramente e auxiliar em um letramento digital local. Esse ponto foi considerado para **aprofundar**, pois nem todos os participantes deram seu consenso;

3.4.3. Como impulsionar o desenvolvimento tecnológico voltado para o fortalecimento da segurança de crianças e adolescentes?

- Essa questão se iniciou com uma fala, de um de nossos interlocutores, sobre a necessidade de se iniciar ensinando o básico sobre cibersegurança para os adolescentes, apontando a importância de se protegerem em ambientes digitais e demonstrando os riscos ao não se debater sobre criptografia e segurança digital. Ponto de **consenso**;
- Foi apresentado, em **consenso**, a importância de cuidados necessários para com

os adolescentes a partir de suas particularidades: neurodivergentes; populações indígenas; juventude camponesa, entre outras;

- Também foi **consenso** a importância de os adolescentes colocarem “a mão na massa” quando se trata de impulsionamento tecnológico; ou seja, ensinar, com a prática, o que são técnicas de segurança digital nos diferentes aplicativos digitais;
- Por fim, a necessidade da existência de um termo de assentimento dos adolescentes, quando se tratar de alguma pesquisa/trabalho que tenha contato direto com esse grupo, e o termo de consentimento dos pais ou responsáveis desses jovens foi também **consenso** do grupo.

4. Recomendações

A partir das discussões geradas no encontro com especialistas nas áreas de segurança digital, proteção de crianças e adolescentes e cuidados digitais, apresentamos as recomendações abaixo, voltadas aos diferentes setores da sociedade envolvidos no debate..

- I. Recomenda-se às empresas** que utilizam serviços e aplicações com criptografia e que tenham entre seu público de utilização, crianças e/ou adolescentes, que desenvolvam pesquisas de/com usuários para identificar as percepções, os conhecimentos e as principais abordagens nas quais crianças e adolescentes utilizam seus serviços;
- II. Recomenda-se às empresas** que adequem a linguagem de seus produtos, especialmente daqueles de segurança e privacidade, conforme a idade declarada da pessoa usuária, para permitir o reconhecimento da autonomia progressiva de adolescentes e jovens;
- III. Recomenda-se às empresas** que tenham como premissa a presença de crianças e adolescentes em suas plataformas e atuem para a sua proteção, mesmo que as suas ferramentas não os tenham como público alvo;
- IV. Recomenda-se ao Comitê Gestor da Internet no Brasil (CGI.br)** a criação de espaços no Fórum da Internet ou em outros programas, como o Youth BR¹², para a inclusão de adolescentes, ampliando sua participação sobre tecnologias no Brasil;
- V. Recomenda-se às organizações, empresas e instituições em geral que queiram desenvolver projetos e ações com adolescentes sobre criptografia e segurança digital** que respeitem suas condições de autonomia e desenvolvimento, que evitem falas e atitudes discriminatórias, adultocêntricas, ou que ponha em risco o bem-estar de crianças e adolescentes. **Recomenda-se**, ainda, o cuidado ético com seus posicionamentos enquanto sujeitos e não meros objetos de investigação ou ensino. É preciso que estas aproximações sejam feitas de forma qualificada e sensível às especificidades do grupo.
- VI. Recomenda-se às empresas** que desenvolvam, apliquem ou financiem projetos de letramento digitais voltados para adolescentes e que tais projetos tenham como base o ensino sobre cibersegurança e criptografia, a partir de perspectivas teóricas e práticas. É preciso um compromisso com a formação dos jovens usuários da internet para o meio digital, habilitando-os a estar e

12 O programa Youth BR, é um programa de inserção de jovens na governança da internet do Brasil. Desenvolvido pelo [CGI.br](https://cgi.br), desde 2015 o programa seleciona jovens entre 18 a 25 anos para serem capacitados sobre os temas correlatos a internet. Para saber mais acesse: <https://fib.cgi.br/pt-BR/youth#sobre/>

construir uma rede segura para todas as pessoas. Ainda, **é recomendado** que utilizem do direito à aprendizagem previsto no Estatuto da Criança e do Adolescente para capacitar estes jovens ao mundo do trabalho.

VII. Recomenda-se aos organizadores de programas, projetos e eventos que considerem tecer parcerias com escolas que podem ser intermediadoras para sensibilizar, selecionar e convidar adolescentes a participarem de debates multissetoriais sobre temas do interesse direto desse público. Esse movimento pode fomentar ações que desoneram a sobrecarga das escolas e fortalecer uma rede de cuidado voltada aos adolescentes. Para tanto, é preciso observar o cuidado de obter as devidas autorizações de responsáveis e de viabilizar o adequado engajamento nas atividades de discussão, evitando qualquer tipo de tratamento excludente ou condescendente.

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE