

Uso da Tecnologia na Proteção de Crianças e Adolescentes: Uma Análise da Comunicabilidade e da Adequação ao ECA Digital

Monografia de Sistemas de Informação - Pesquisa Científica

Daniele Cássia Silva Diniz

Departamento de Ciência da Computação

Universidade Federal de Minas Gerais

Belo Horizonte, Brasil

danielecassia@ufmg.br

Abstract—A crescente presença digital de crianças e adolescentes os expõe a vulnerabilidades como o cyberbullying e conteúdo inadequado. Ferramentas de controle parental surgem para mitigar esse problema, porém ainda são subutilizadas. Este estudo analisa a comunicabilidade e as estratégias de design das ferramentas AirDroid Parental Control e Google Family Link, avaliando também o grau de conformidade de suas funcionalidades com as diretrizes estabelecidas pela Lei nº 15.211/2025 (ECA Digital). Para isso, utilizamos o Método de Inspeção Semiótica para reconstruir a metacomunicação projetada pelos designers, associada a uma análise qualitativa dos requisitos legais de supervisão parental e monitoramento infantil vigentes no Brasil. Os resultados revelam duas filosofias de controle parental distintas: o AirDroid apoia-se em uma lógica de vigilância ativa, enquanto o Family Link prioriza uma mediação estruturada. Ambas as ferramentas apresentam desafios de comunicabilidade que podem confundir o usuário e exibem lacunas de conformidade legal, especialmente no que tange à identificação de interação com adultos e à ciência do monitoramento por parte do menor.

Index Terms—Controle Parental, Método de Inspeção Semiótica, Engenharia Semiótica, ECA Digital, Monitoramento Infantil, Supervisão Parental, Interação Humano-Computador

I. INTRODUÇÃO

A integração da internet ao cotidiano é uma realidade irreversível, especialmente para crianças e adolescentes, denominados “*nativos digitais*” [1], que estão cada vez mais conectados [2]. Entre os diversos ambientes online, os ambientes digitais interativos emergem como centrais para a sua socialização, construção de identidade e entretenimento. No entanto, essa hiperconectividade ocorre em um ecossistema complexo, no qual as experiências vivenciadas por crianças e adolescentes nem sempre são seguras, podendo expô-las a diferentes tipos de riscos e nem sempre contribuindo de forma positiva para sua formação e desenvolvimento. Esses riscos abrangem desde o contato com conteúdos inapropriados potencialmente danosos (e.g. violência, drogas), como decorrentes de interações sociais (e.g., *cyberbullying*, assédio) e relacionados à privacidade de dados (e.g. coleta

predatória de dados pessoais, publicidade direcionada) a conteúdos pornográficos [3].

Além disso, discussões sobre a exploração e adultização de crianças nas plataformas de mídias sociais estão cada vez mais frequentes [4]. Diante desse cenário, a urgência por mecanismos de salvaguarda tornou-se uma questão não apenas social, mas também de ordem pública e jurídica, com a publicação da Lei nº15.211/2025, presente no Estatuto Digital da Criança e do Adolescente (ECA Digital), que reforçou a obrigatoriedade de políticas de segurança rigorosas em plataformas digitais, elevando a relevância do debate sobre a responsabilidade das empresas e dos tutores [5].

Embora as ferramentas de controle parental, softwares e funcionalidades integradas às plataformas [6]–[8] que permitam que tutores supervisionem, restrinjam e filtrem o acesso e as interações online das crianças e adolescentes, surjam como a resposta técnica primária a esses riscos, observa-se uma lacuna significativa entre a oferta tecnológica e a adoção prática. Estudos [2], [9], [10] destacam o “*paradoxo da abundância*”, que enfatiza que apesar de algumas funcionalidades de supervisão parental estarem nativamente integradas em sistemas operacionais como Android e iOS, a adesão efetiva destas funcionalidades permanece baixa porque muitos usuários as percebem como intrusivas ou redundantes em relação à vigilância física.

Nessa pesquisa, buscamos avaliar a efetividade de ferramentas de controle parental, diretamente influenciada pela qualidade de sua concepção e implementação, um problema central do campo de Interação Humano-Computador (IHC). Para isso, adotamos o Método de Inspeção Semiótica (MIS) [11], investigando quais são os significados projetados pelos designers e como eles estão sendo transmitidos aos usuários. Além disso, queremos verificar a conformidade dessas ferramentas com as diretrizes estabelecidas pelo ECA Digital, realizando um levantamento dos requisitos previstos na legislação e uma análise do grau de aderência das soluções avaliadas.

Para alcançar os objetivos propostos, as ferramentas *AirDroid Parental Control* e *Google Family Link*, amplamente utilizadas e disponíveis em diferentes ecossistemas foram analisadas. Como principais resultados, identificamos que enquanto uma ferramenta se apoia em uma lógica de *vigilância ativa e intrusiva*, a outra prioriza uma *mediação estruturada e orientada a hábitos*, embora ambas apresentem desafios de comunicabilidade que podem confundir o usuário final. Além disso observamos que ambas possuem pontos de atenção em relação a conformidade com o ECA Digital

II. REFERENCIAL TEÓRICO

A vulnerabilidade de crianças e adolescentes no ambiente digital é uma preocupação que se intensificou com a popularização da internet na década de 1990. Foi especificamente em 1994 que surgiu a primeira ferramenta comercial de controle parental, o *Net Nanny*, seguido de perto pelo *SurfWatch* em 1995, desenvolvida para filtrar conteúdos pornográficos e palavras-chave consideradas impróprias [12]. Inicialmente, essas ferramentas tinham como principal funcionalidade o bloqueio reativo de URLs e a filtragem de texto, uma abordagem limitada se comparada à mediação atual.

A recente lei aprovada no Brasil, o ECA Digital [5], reforça a relevância de mecanismos de controle e monitoramento parental modernos e eficazes ao abordar, especificamente no Capítulo V, as ferramentas de “Supervisão Parental” e, no Capítulo IV, os “Produtos de Monitoramento Infantil”. Em ambos os casos, a legislação destaca a importância de instrumentos capazes de auxiliar pais e responsáveis no acompanhamento das atividades digitais de crianças e adolescentes, com o objetivo de promover seu desenvolvimento integral, bem-estar e proteção no ambiente online.

A preocupação com mecanismos de supervisão e proteção digital deste público não se restringe ao contexto brasileiro. Em âmbito internacional, diferentes países e organizações têm avançado em regulamentações e iniciativas voltadas à segurança online de crianças e adolescentes. Na Austrália, o *Online Safety Act* estabelece diretrizes para proteção infantil em ambientes digitais, incluindo mecanismos de supervisão e restrições de acesso para menores [13]. Nos Estados Unidos, a *Children’s Online Privacy Protection Act* (COPPA) [14] exige consentimento parental para a coleta de dados de crianças menores de 13 anos, enquanto propostas mais recentes, como a *Kids Online Safety Act* (KOSA) [15], ampliam o debate sobre supervisão parental e responsabilidades das plataformas na mitigação de riscos online. Na Europa, iniciativas como o programa *Better Internet for Kids* [16] promovem diretrizes continentais para proteção digital infantil, coexistindo com legislações e medidas nacionais mais restritivas adotadas recentemente por países como França e Dinamarca [17], [18].

Nesse contexto, ferramentas de controle parental e monitoramento de crianças e adolescentes têm sido amplamente

investigadas na literatura [7], [19]–[22] devido ao seu potencial para promover experiências digitais mais seguras em plataformas online e de mídias sociais. Tal interesse é impulsionado por diversos estudos que apontam riscos e potenciais danos associados à exposição de crianças e adolescentes a conteúdos inadequados e interações nocivas em plataformas digitais [23]–[27].

Apesar disso, alguns trabalhos na literatura argumentam que abordagens exclusivamente restritivas tendem a ser insuficientes para lidar com a complexidade dos riscos digitais contemporâneos. Estudos indicam que mecanismos baseados apenas em restrições etárias [21] ou centrados predominantemente em vigilância e monitoramento podem comprometer a autonomia, a privacidade e o bem-estar de crianças e adolescentes, especialmente durante a adolescência [19]. Além disso, pais e crianças frequentemente percebem os riscos online de maneiras distintas, reforçando a necessidade de modelos de segurança mais flexíveis, colaborativos e adaptáveis aos diferentes níveis de maturidade, experiências digitais e necessidades do público infantojuvenil [21].

Além das discussões conceituais, alguns estudos têm investigado diferentes aspectos relativos ao projeto e avaliação de ferramentas de controle parental. Com foco no projeto dessas ferramentas, os autores [28] e [29] investigam e identificam requisitos técnicos e padrões de interface, mas não exploram as barreiras comportamentais e o baixo letramento digital que impedem os pais de usar essas ferramentas na prática. Em [30], os autores exploraram com os pais propostas de design de ferramentas de controle parental que levassem em consideração aspectos de autorregulação e comunicação aberta em crianças de diferentes faixas etárias. Além disso, outras pesquisas propõem o desenvolvimento de novas soluções voltadas ao acompanhamento de chamadas, mensagens e contatos, buscando equilibrar supervisão parental, segurança digital e respeito à privacidade infantil [7], [31], [32].

Paralelamente, diversos trabalhos têm focado em investigar como essas ferramentas de controle parental têm sido usadas pelos pais e suas experiências [19], [20], [33]. No entanto, poucos trabalhos foram encontrados que analisam as soluções apresentadas para o controle dos pais [34]. Assim, existe uma lacuna na literatura no que tange a comunicabilidade das principais ferramentas de controle parental, suas estratégias de apoio aos pais e a adequação a legislação brasileira.

III. FERRAMENTAS

As ferramentas *AirDroid Parental Control*¹ e *Google Family Link*² foram selecionadas para avaliação por representarem soluções amplamente utilizadas no contexto contemporâneo [35], [36] apresentarem elevada relevância prática no cotidiano das famílias e por oferecerem diferentes estratégias de mediação parental digital. Enquanto o

¹<https://www.airdroid.com/parental-control/>

²<https://families.google/familylink/>

AirDroid Parental Control oferece mecanismos mais extensivos de monitoramento remoto, incluindo acompanhamento em tempo real de atividades e funcionalidades avançadas de supervisão do dispositivo, o *Google Family Link* está fortemente integrado ao Android e aos serviços da Google, priorizando gerenciamento de contas, controle de tempo de uso e filtragem inicial de conteúdo.

A. *AirDroid Parental Control*

O *AirDroid Parental Control* é um aplicativo que permite aos pais monitorar e gerenciar remotamente o uso de dispositivos pelos filhos, sendo voltado para famílias que desejam acompanhamento completo, tanto *online* quanto *offline*. O app controla localização em tempo real, histórico de rotas e cercas geográficas, além de limite de tempo de tela e gerenciamento de uso por aplicativo. Também oferece acesso remoto à câmera, áudio ambiente e espelhamento de tela (recursos exclusivo para Android), além de monitoramento de notificações, chamadas e SMS. Outras funcionalidades incluem detecção de conteúdo definido como impróprio, filtragem de sites, bloqueio de conteúdos identificados como nocivos, relatórios de atividades e alertas em tempo real.

A ferramenta está disponível globalmente na *Google Play Store*, na *Apple App Store* e em versão web. O dispositivo do tutor funciona com Android 8.0 ou superior, ou iOS 13 ou superior, enquanto o dispositivo da criança ou do adolescente exige o aplicativo complementar *AirDroid Kids*, disponível no site da ferramenta, rodando em Android 8.0+ ou iOS 15+. Atualmente, sinalizando a popularidade da ferramenta, o *AirDroid Parental Control* possui mais de 10 milhões de downloads e mais de 142 mil avaliações na *Google Play Store*.

B. *Google Family Link*

O *Google Family Link* é uma ferramenta de supervisão parental que reúne funcionalidades e salvaguardas tecnológicas destinadas a permitir que tutores legais supervisionem, limitem, configurem e gerenciem o uso de dispositivos e aplicações por crianças e adolescentes. Possui o objetivo de promover segurança, proteção e experiências digitais adequadas ao desenvolvimento desse público. Considerada uma das ferramentas de supervisão parental mais utilizadas atualmente [35], [37], atualmente a ferramenta possui mais de 100 milhões de downloads e mais de 5 milhões avaliações na *Google Play Store*. O *Google Family Link* é um serviço gratuito da Google voltado ao gerenciamento de dispositivos e contas de crianças e adolescentes para todas as idades.

A plataforma oferece funcionalidades como controle do tempo diário de uso e definição de horários de descanso, aprovação ou bloqueio de downloads de aplicativos, geração de relatórios de uso por aplicação, rastreamento de localização em tempo real, bloqueio remoto do dispositivo e aplicação de filtros de conteúdo no *Chrome*, *Pesquisa Google*, *YouTube* e *Google Play Store*. O serviço está disponível em 38 países (inclusive o Brasil) nas lojas *Google Play Store* e *Apple App Store*. O aplicativo utilizado

pelos tutores é compatível com dispositivos Android 7.0 ou superior, iOS 16 ou superior e Chromebooks, enquanto os dispositivos supervisionados exigem Android 7.0 ou superior, mantendo compatibilidade parcial com Android 5.0 e 6.0, ou Chrome OS 71 ou superior. Em dispositivos iPhone e iPad, entretanto, a supervisão é limitada às contas Google, não sendo possível realizar o gerenciamento completo do aparelho. A ferramenta não é universalmente pré-instalada como aplicativo visível, mas em sistemas Android, frequentemente já vem incorporado nativamente às contas Google supervisionadas.

IV. METODOLOGIA

Nesse trabalho aplicamos o Método de Inspeção Semiótica (MIS) [11], [38], um método que nos permite fazer uma análise sistemática de um sistema interativo, gerando a reconstrução da sua proposta de solução e identificando potenciais problemas para os usuários. A partir dos resultados dessa inspeção, avaliamos os sistemas sob a perspectiva do ECA Digital, estabelecendo os requisitos mínimos previstos na legislação e verificando a conformidade de cada sistema em relação a esses requisitos.

A. *Método de Inspeção Semiótica*

O MIS é fundamentado na Engenharia Semiótica, uma teoria da área de IHC que entende a interface como sendo uma comunicação do projetista para o usuário sobre a quem o sistema se destina, que objetivos os usuários podem atingir com o sistema, e como interagir com ele [39]. Nesse contexto, a **comunicabilidade** de um sistema é definida como a propriedade desse sistema de transmitir ao usuário as intenções e princípios de design que orientaram seu desenvolvimento [38]–[40].

Antes de aplicar o MIS, o avaliador deve realizar uma etapa de preparação, na qual executa uma avaliação informal do sistema, delimita o escopo da avaliação e define os cenários a serem usados para guiar a análise. O MIS é então organizado em 5 passos:

- 1) **Inspeção de signos metalinguísticos:** Análise de documentação e signos explicativos (e.g. instruções, mensagens de erro) para captar o discurso explícito do designer e reconstrução da metamensagem baseada nos signos metalinguísticos.
- 2) **Inspeção de signos estáticos:** Análise dos signos estáticos da interface e reconstrução da metamensagem baseada nesses signos.
- 3) **Inspeção de signos dinâmicos:** Análise dos signos dinâmicos, i.e. comportamento do sistema e reconstrução da metamensagem baseada nos signos dinâmicos.
- 4) **Contraste das meta-mensagens:** Análise comparativa das mensagens reconstruídas para identificar inconsistências ou ambiguidades entre as metamensagens relativas a cada classe de signos.

5) **Apreciação global da comunicabilidade:**
Reconstrução final da metamensagem e síntese diagnóstica da qualidade da sua comunicabilidade.

A reconstrução da metamensagem é feita usando o modelo da metacomunicação da teoria da Engenharia Semiótica como base:

- *“Aqui está minha compreensão de quem você é, do que aprendi que você deseja ou precisa fazer, de quais são as formas preferenciais pelas quais pretende fazê-lo e por quê. Este é, portanto, o sistema que projetei para você, e esta é a maneira pela qual você pode ou deve utilizá-lo a fim de cumprir uma série de propósitos que se enquadram dentro dessa visão.” [11]*

A análise dos sistemas com o MIS foi realizada no segundo semestre de 2025, o foco da inspeção foi o uso das funções de Controle Parental pelos responsáveis/tutores com o objetivo de configurar o controle desejado. A análise foi feita utilizando contas criadas para a pesquisa que simulassem contas de crianças e adolescentes, bem como contas de responsáveis. Nenhum dado real de usuário foi utilizado. O cenário definido para guiar a inspeção foi:

“João, pai de Ana (12 anos), começou recentemente a se preocupar com a quantidade de tempo que a filha passa utilizando o celular e acessando redes sociais. Após assistir a uma reportagem sobre riscos digitais envolvendo crianças e adolescentes, João decidiu procurar formas de acompanhar melhor as atividades online da filha. Durante uma conversa com colegas de trabalho, ele ouviu pela primeira vez sobre ferramentas de controle parental e decidiu procurar aplicativos que possam ajudá-lo a trazer mais segurança para sua filha.”

B. Estatuto da Criança e do Adolescente Digital

Após a aplicação do MIS, as ferramentas foram analisadas sob a ótica da Lei para verificar a conformidade de suas funcionalidades com a legislação brasileira.

Com base nas definições do Art. 2º da lei, tanto o *AirDroid Parental Control* quanto o *Google Family Link* enquadram-se simultaneamente como: (i) *produtos ou serviços de tecnologia da informação*, por serem softwares distribuídos por meio eletrônico; (ii) *produtos de monitoramento infantil*, dado que transmitem aos responsáveis dados de localização, tempo de tela e atividades digitais dos menores; e (iii) *mecanismos de supervisão parental*, uma vez que disponibilizam salvaguardas para gerenciar o uso dos dispositivos e o acesso a conteúdos.

A partir desse enquadramento, realizou-se uma análise qualitativa baseada nos Capítulos II, V e VI do estatuto. Os requisitos mínimos, dispostos nos artigos 16, 17, 18 e 19, foram decompostos em sete classificações, são elas:

- 1) **Usabilidade, Transparência e Dados (Art. 16 e 17):** Exige interfaces acessíveis, em língua portuguesa e livres de padrões manipulativos (*dark patterns*) que induzam à desativação de salvaguardas. É obrigatório exibir avisos claros e contínuos quando o monitoramento estiver ativo, além de realizar mapeamento de

riscos e relatórios de impacto à proteção de dados do menor.

- 2) **Configuração Padrão Protetiva (Art. 18):** Determina a adoção nativa do nível máximo de proteção (*privacy by default*), incluindo:
 - Restrição de geolocalização e de comunicação com usuários não autorizados;
 - Bloqueio de recursos indutores de uso excessivo (reprodução automática, notificações excessivas e recompensas por tempo);
 - Opção para gerenciar ou desativar sistemas de recomendação personalizada e funcionalidades de inteligência artificial não essenciais.
- 3) **Saúde e Suporte (Art. 18):** Obrigatoriedade de ferramentas para visualização e limitação imediata do tempo de uso, promoção de ações de educação digital e, quando tecnicamente viável, oferta de recursos de suporte emocional adequados à faixa etária.
- 4) **Controles Operacionais dos Responsáveis (Art. 18):** Prerrogativas técnicas que garantam aos tutores gerenciar privacidade e contas, restringir transações financeiras, acessar métricas consolidadas de tempo e identificar perfis de adultos em comunicação com o menor.
- 5) **Segurança e Inviolabilidade de Dados (Art. 19):** Exige o emprego de mecanismos tecnológicos robustos que garantam a proteção integral e a inviolabilidade de imagens, sons e quaisquer outras informações captadas, armazenadas ou transmitidas aos responsáveis.
- 6) **Transparência e Ciência do Menor (Art. 19):** Determina a inclusão obrigatória de sinalizadores ou alertas que informem claramente as crianças e os adolescentes de que estão sendo monitorados, utilizando linguagem acessível e apropriada à sua faixa etária.
- 7) **Princípio do Melhor Interesse (Art. 19):** Estabelece que a concepção, o desenvolvimento e a aplicação prática das ferramentas de monitoramento devem priorizar o bem-estar do menor e salvaguardar o pleno desenvolvimento de suas capacidades cognitivas e sociais.

A análise da adequação dos sistemas ao ECA Digital foi realizada no primeiro semestre de 2026, com base nos dados levantados por meio da aplicação do MIS, utilizando os mesmos cenários e contas de teste.

V. RESULTADOS

Nesta seção apresentamos os principais resultados obtidos a partir da análise dos sistemas de controle parental presentes nas duas ferramentas apresentada na Seção III.

Para cada um deles, apresentamos a reconstrução da metacomunicação estruturada de acordo com os principais pontos do modelo de metacomunicação (Quem é você?; O que você quer ou precisa fazer? Como você pode ou deve utilizar o sistema?), os principais problemas de comunicabilidade identificados, e suas características de adequação ao ECA Digital.

A. AirDroid Parental Control

A seguir, detalhamos a metamensagem obtida através dos passos relacionados à aplicação do MIS, que seguem o modelo definido:

Q1: Quem é você?

Mãe, pai ou responsável que está preocupado com a segurança do seu filho online, você e seu filho possuem dispositivos próprios. Você está habituado a utilizar aplicativos e já instalou e configurou a parte inicial da supervisão no seu aparelho e no do seu filho.

Q2: O que você quer ou precisa fazer?

Você precisa de uma proteção completa para seu filho e, para isso, está em busca de uma ferramenta que possibilite um monitoramento irrestrito, de forma que te mantenha conectado e informado sobre o que acontece ao redor dele (Fig.1, A-B-F). Você também quer monitorar e detectar conteúdos inadequados em redes sociais e mensagens, acessar a tela, câmera e microfone do celular do seu filho pelo seu aparelho (Fig.1, C), bloquear chamadas e sites indesejados, receber alertas de atividades suspeitas, gerenciar o tempo de uso de tela para ajudar seu filho a ter hábitos digitais saudáveis, saber onde ele está em tempo real e ter acesso às rotas e lugares por onde ele passou. Você fazer o rastreamento de localização do seu filho. Além disso, você quer ter relatórios detalhando o uso do celular pelo seu filho para compreender o comportamento digital dele, e também manter uma comunicação ativa com ele por meio de alertas e mensagens (Fig.1, G). Ademais, você quer esconder o aplicativo de supervisão do celular da criança ou adolescente, de modo que, o monitoramento seja discreto (Fig.1, D).

Q3: Como você pode ou deve utilizar o sistema?

Você pode gerenciar a supervisão em um navegador, em dispositivos Android ou iOS e aplicar essa supervisão tanto em aparelhos Android quanto iOS, sendo que as funcionalidades disponíveis dependem do aparelho utilizado pelo seu filho. Se seu filho possui um dispositivo iOS, é possível programar tempo de inatividade, aplicar restrições de aplicativos, conteúdo e uso, definir limites e gerenciamento de aplicativos, detectar imagens inapropriadas, estabelecer limites e restrições de sites, acessar o serviço de localização e geocercas, receber alertas em tempo real, acessar relatórios de atividades e criar grupos de família. Para crianças com dispositivos Android, você pode acessar todas as funcionalidades disponíveis para iOS e, além disso, contar com recursos adicionais como acesso à câmera remota, espelhamento de tela, áudio unidirecional, sincronização de notificações de aplicativos, detecção de conteúdo social e monitoramento de chamadas e SMS.

Através do menu, você encontrará um aparelho representado pelo label 'Dispositivo' (Fig.2, H), onde você consegue selecionar o aparelho que deseja configurar no momento e ver informações como nível de bateria e a rede conectada no aparelho selecionado (Fig.2, A), acessar o relatório do dia (Fig.2, C), acessar a câmera e o microfone do aparelho do seu filho (Fig.2, D-F), fazer o espelhamento de tela

(Fig.2, E), acessar as notificações que seu filho recebeu e ver informações sobre os aplicativos que seu filho tem instalado (Fig.2, G), bloquear o aparelho de forma imediata, definir tempo de inatividade e configurações padrão (Fig.2, I), definir limite de tempo para os apps, dentre outras funcionalidades (Fig.2, J).

Ao acessar a câmera, você pode mudar a orientação do vídeo e a câmera monitorada (Fig.3, A-B), tanto frontal quanto traseira, pode ouvir o áudio juntamente com o vídeo (Fig.3, C) e acionar o flash da câmera do seu filho (Fig.3, D). Além disso, você pode acessar a funcionalidade de áudio unidirecional, você tem acesso ao microfone do seu filho e consegue ouvir tudo que ele está escutando naquele momento; você também pode gravar o que está sendo escutado (Fig.3, E-F). Outra funcionalidade é o espelhamento de tela, você poderá ver o que seu filho está vendo em tempo real no aparelho; um ícone indicando gravação aparecerá no telefone do seu filho, e juntamente com o espelhamento você também pode acessar o áudio (Fig.3, G).

Além disso, é viável estabelecer um limite de tempo diário que o usuário pode passar em cada aplicativo e no dispositivo (Fig.4, A). Quando o limite diário de uso for atingido, o app ou dispositivo será bloqueado automaticamente. Você pode acessar as notificações dos aplicativos, criar um tempo de atividade onde o telefone da criança só poderá acessar chamadas telefônicas (Fig.4, B). Além disso, você pode acessar o histórico de navegação do seu filho e adicionar sites na lista de sites bloqueados (Fig.4, C).

No menu também temos uma opção relacionada à localização, indicada pelo ícone de Pin (alfinete) e pelo label 'Localização' (Fig.5, D). Nessa parte, você pode acessar a localização atual do seu filho (Fig.5, C) e definir cercas geográficas para receber notificações quando o dispositivo entrar ou sair da área (Fig.5, B-F). Você também pode acessar os lugares que seu filho foi; para isso, basta você selecionar a data em que quer acessar o histórico (Fig.5, A-E).

Ademais, no menu também temos a opção relacionada ao grupo familiar, indicada pelo ícone de casa e pelo label 'Família' (Fig.6, C). Nessa parte, você consegue acessar o grupo, que é um chat de mensagens com todos os dispositivos que você supervisiona (Fig.6, A), bem como um chat individual com cada aparelho (Fig.6, B). Outra funcionalidade é acessar as notificações recebidas no celular da criança ou adolescente (Fig.2, B e Fig.6, F). Além disso, na página que detalha os eventos do dia, podemos observar o tempo total de uso do celular (Fig.6, D) e o tempo utilizado em cada aplicativo (Fig.6, E).

Apreciação

A análise indica que o sistema comunica de forma abrangente e direta seu propósito principal, que é oferecer um controle parental total sobre os dispositivos da criança, com ênfase em vigilância ativa e monitoramento contínuo. A presença de funcionalidades como acesso remoto à câmera, microfone, espelhamento de tela e sincronização de notificações evidencia a possibilidade de uma estratégia de

supervisão intrusiva, voltada para responsáveis que desejam conhecimento detalhado das atividades digitais dos filhos. Contudo, observam-se potenciais rupturas de comunicabilidade: a grande quantidade de recursos e opções pode sobrecarregar usuários menos experientes, gerando dificuldade de identificar as funções essenciais na interface. Além disso, a comunicação sobre o uso de recursos sensíveis, como áudio unidirecional e câmera remota, não esclarece adequadamente as questões éticas e de privacidade associadas a essas funcionalidades, nem os cuidados necessários para seu uso responsável, podendo induzir o responsável a práticas invasivas sem o devido alerta. De modo geral, o sistema oferece muitas possibilidades, mas sua comunicabilidade é comprometida pela complexidade e pela falta de metacomunicação clara sobre os limites apropriados da supervisão.

Adequação ao ECA Digital

A avaliação revela que, embora a ferramenta ofereça recursos robustos de supervisão parental, apresenta defasagens significativas em aspectos cruciais, como proteção nativa, transparência para o menor e governança de dados.

A seguir, detalhamos o grau de aderência da ferramenta a cada um dos sete critérios analisados:

- 1) **Usabilidade, Transparência e Dados (Art. 16 e 17) – Parcial:** A interface é em português e de fácil navegação, sem indícios de *dark patterns* que induzam à redução de segurança. Contudo, a ferramenta falha na transparência contínua por não emitir avisos permanentes de monitoramento (e.g. como localização ou espelhamento) e por oferecer um “Modo Furtivo” que oculta a aplicação. Faltam, ainda, informações públicas sobre Relatórios de Impacto à Proteção de Dados (DPIA) e mapeamento de riscos.
- 2) **Configuração Padrão Protetiva (Art. 18) – Parcial:** A plataforma descumpra a premissa de *privacy by default*. Restrições de localização e bloqueios de aplicativos exigem ativação manual, deixando o dispositivo vulnerável logo após a instalação.
- 3) **Saúde e Suporte (Art. 18) – Parcial:** O aplicativo apresenta excelente desempenho na limitação do tempo de uso, com bloqueios automáticos, pausas programadas e relatórios detalhados. No entanto, não possui promoção de ações de educação digital ativa e carece de recursos voltados ao suporte emocional ou à identificação de sofrimento psicológico da criança.
- 4) **Controles Operacionais (Art. 18) – Parcial:** O AirDroid fornece amplo controle para gerenciar a privacidade, limitar o uso e rastrear a localização do dispositivo. A conformidade é reduzida apenas pela ausência de restrições diretas a transações financeiras e pela falta de sistemas automáticos que identifiquem perfis de adultos interagindo com o menor.
- 5) **Segurança e Inviolabilidade (Art. 19) – Parcial:** Apesar de a desenvolvedora alegar o uso de criptografia e transmissão segura, faltam evidências de mecanismos robustos exigidos pelo ECA Digital. Não há divulgação

de auditorias independentes, detalhamento sobre o gerenciamento de chaves criptográficas ou políticas claras de retenção e exclusão de dados sensíveis.

- 6) **Transparência e Ciência do Menor (Art. 19) – Não Conforme:** Este é o ponto mais crítico da ferramenta. A presença do “Modo Furtivo” e a ausência de alertas contínuos em linguagem acessível violam diretamente o direito da criança de saber que está sendo monitorada.
- 7) **Princípio do Melhor Interesse (Art. 19) – Parcial:** Embora atue na prevenção do uso excessivo e proteja contra certos riscos digitais, suas funções altamente invasivas (e.g. captura remota, espelhamento de tela e áudio unidirecional), quando desacompanhadas de transparência, ameaçam a privacidade, a autonomia e o desenvolvimento saudável do menor. Nesses casos, a proteção passa a depender exclusivamente do bom senso do tutor.

B. Google Family Link

De forma análoga ao que foi feito para o *AirDroid Parental Control*, aplicamos o mesmo procedimento ao *Google Family Link*, cuja metamensagem é apresentada a seguir:

Q1: Quem é você?

Você é um responsável que possui um celular com o aplicativo Family Link instalado e deseja supervisionar e gerenciar o uso do dispositivo móvel de uma criança ou adolescente vinculado à sua família Google. Você e seu filho possuem uma conta Google.

Q2: O que você quer ou precisa?

Você precisa reforçar a proteção da sua família online (Fig.7, B), controlando o uso do aparelho e da conta Google do seu filho. Para isso, busca uma ferramenta que funcione no sistema Android ou iOS (Fig.7, E) e respeite suas escolhas individuais sobre a tecnologia (Fig.7, C), ajude a criar hábitos saudáveis e positivos (Fig.7, D), e possibilite o monitoramento de uso. Essa ferramenta deve permitir bloquear e desbloquear o celular, gerenciar a conta Google da família, restaurar, remover ou excluir a conta do seu filho, e ativar e gerenciar a supervisão nessa conta. Você também deseja que ela tenha funcionalidades para configurar o tempo de uso do aparelho, visualizar limites de tempo e programação, monitorar o uso de aplicativos e, assim, garantir um ambiente digital seguro.

Q3: Como você pode ou deve utilizar o sistema?

Você pode configurar a supervisão de dispositivos Android e ChromeOS da criança ou adolescente, permitindo monitorar o tempo de uso e controlar os aparelhos remotamente. Ao abrir o aplicativo, você é direcionado à tela inicial, identificada pelo ícone de gráfico e pelo label ‘Tempo de tela’ (Fig.8, J). Nessa tela, você consegue visualizar qual criança está selecionada (Fig.8, A), suas notificações, informações sobre a sua própria conta (responsável) (Fig.8, B), o tempo de uso do celular no dia atual (Fig.8, C) e os principais apps utilizados (Fig.8, d), o nome do dispositivo da criança e o tempo restante de uso (Fig.8, E), bem como os

dados referentes ao limite definido (Fig.8, H). A partir daqui, você pode adicionar tempo extra (Fig.8, F) ou bloquear imediatamente o celular (Fig.8, G).

Acessando as configurações do dispositivo da criança, você pode visualizar o nível de bateria e se o celular está conectado a internet (Fig.8, K), editar o nome do aparelho (Fig.8, A), tocar um som no celular dela (Fig.8, M), para ajudar a encontrá-lo ou chamar sua atenção e acessar relatórios de atividades (Fig.8, N). Você também pode definir o que a criança pode ver e utilizar quando o celular estiver bloqueado devido ao limite de tempo, gerenciar permissões de aplicativos e ativar e ajustar o posicionamento de localização via Family Link (Fig.8, O), além de adicionar ou remover outras configurações (Fig.8, P).

Na tela de ‘Limite de tempo’, você pode definir um limite diário total de uso e também limites individuais para cada aplicativo (Fig.9, A-D). Quando o limite diário é ativado, você tem a opção de criar uma programação semanal (Fig.9, C) ou definir um limite específico para o dia atual (Fig.9, B). Nos limites por aplicativo, você pode determinar o tempo máximo de uso para cada app, podendo aplicar filtro para ordenar a lista dos aplicativos mostrados (Fig.9, E), ou até mesmo definir que determinado aplicativo não tenha tempo limite, o que permite acesso mesmo durante horários restritos, como o horário escolar (Fig.9, F). Você também pode bloquear aplicativos específicos. Além disso você tem acesso ao relatório de atividades, que mostra o tempo de uso total do celular (Fig.9, H) e em cada aplicativo (Fig.9, I), você pode filtrar as atividades (Fig.9, G).

Na parte de programações, você pode definir período de ‘Descanso’ e ‘Horário escolar’ (Fig.10, A-B), de modo que, o aparelho será bloqueado durante o descanso e silenciado durante o horário escolar (Fig.10, C). O ‘Descanso’ é voltado para o período de dormir, você pode definir o horário de ir para a cama, podendo fazer uma programação semanal ou ajustar manualmente o dia atual (Fig.10, D-E). Além disso, você pode selecionar quais aplicativos são permitidos durante esse período (Fig.10, F-G). Já o ‘Horário escolar’ tem como objetivo minimizar distrações (Fig.10, B), possui o mesmo padrão de configuração.

Acessando o menu ‘Controles’, identificado pelo ícone de um pai e um filho se abraçando (Fig.11, C), você pode definir configurações da conta da criança e outras restrições (Fig.11, A-B). Para sites e navegadores, você pode configurar filtros, podendo permitir todos os sites, tentar bloquear sites explícitos ou permitir apenas sites aprovados por você, gerenciando listas de sites liberados e bloqueados (Fig.11, D-E). Além disso, há a configuração do ‘SafeSearch’ (Pesquisa Segura) do Google, onde você pode gerenciar conteúdo explícito, como atividade sexual e violência explícita, nos resultados de busca (Fig.11, F). Dentre outras funcionalidades como, restrição de conteúdo no YouTube e gerenciamento da Google Play Store, em que se pode definir desde uma classificação etária até a permissão de compras nos aplicativos (Fig.11, B).

No menu indicado pelo ícone de pin (alfinete) e pelo label ‘Localização’ (Fig.12, B), você consegue ver a localização em tempo real da criança (Fig.12, A-C). Também tem acesso aos ‘Locais da Família’, que são lugares que você salva e define para receber notificações quando a criança chegar, sair ou ambos (Fig.12, A). Para isso, você adiciona um endereço (Fig.12, E), define um raio (Fig.12, D) e escolhe o tipo de notificação (Fig.12, F). Sempre que a criança entrar ou sair daquele local, você será notificado.

Apreciação

A análise indica que o sistema comunica de forma relativamente clara seu propósito principal, que é permitir o controle parental sobre dispositivos de crianças e adolescentes por meio de supervisão remota. A presença de funcionalidades como monitoramento de tempo de uso, bloqueio do dispositivo e gerenciamento de permissões contribui para uma boa compreensão inicial do usuário sobre o que pode ser feito no sistema. Entretanto, observa-se limitações de comunicabilidade, como por exemplo a dependência de conhecimento prévio sobre contas Google e estrutura familiar digital, o que pode representar uma barreira para usuários menos experientes. A comunicação sobre ações críticas, como remoção ou restauração da conta da criança, também pode não evidenciar claramente suas consequências, gerando riscos de uso indevido. De modo geral, o sistema apresenta boa comunicabilidade em relação às suas funções principais.

Adequação ao ECA Digital

A análise indica que a ferramenta atendeu à maior parte dos princípios definidos pela lei, oferecendo recursos voltados para a transparência, a segurança dos dados e a proteção da privacidade da criança e do adolescente. No entanto, apresenta limitações de identificação de interação entre a conta supervisionada e adultos, detalhados a seguir:

- 1) **Usabilidade, Transparência e Dados (Art. 16 e 17) – Total:** A interface é intuitiva e sem *dark patterns*. O tratamento de dados é explicado nos termos de uso e o menor recebe notificações de acesso aos seus dados (e.g. localização).
- 2) **Configuração Padrão Protetiva (Art. 18) – Parcial:** Possui forte aplicação de *privacy by default* no ecossistema Google, mas limitada fora dele, sem controle sobre algoritmos de terceiros.
- 3) **Saúde e Suporte (Art. 18) – Total:** Oferece funcionalidades abrangentes de gestão de tempo de tela, como limites diários, programações para horário escolar e descanso, e a capacidade de bloquear o dispositivo remotamente. Além de incentivar a equilíbrio e saúde digital.
- 4) **Controles Operacionais (Art. 18) – Parcial:** Os pais têm controle total da conta vinculada, podendo gerenciar permissões, redefinir senhas e excluir a conta. O Family Link permite aprovar ou bloquear compras no Google Play, mas não controla transações em apps de terceiros. Além disso, fornece relatórios de uso com métricas de tempo por aplicativo. Não há função específica para identificar perfis de adultos

nas comunicações, apesar de ser possível filtrar a comunicação por chamadas e SMS.

- 5) **Segurança e Inviolabilidade (Art. 19) – Total:** O Google afirma proteger os dados com criptografia e outras medidas de segurança, além de declarar conformidade com a LGPD. Entretanto, essas alegações precisam ser verificadas por meio de certificações, auditorias e análise das práticas de tratamento de dados, especialmente em relação à proteção de crianças e adolescentes.
- 6) **Transparência e Ciência do Menor (Art. 19) – Total:** A ferramenta cumpre integralmente este requisito, ela é projetada para ser transparente, com uma notificação persistente no dispositivo da criança, fazendo com que a criança sempre saiba que está sendo monitorada, e qualquer tentativa de remover a supervisão notifica os pais.
- 7) **Princípio do Melhor Interesse (Art. 19) – Total:** A ferramenta incentiva a proteção gradual e no desenvolvimento da autonomia digital da criança, mas não limita certas configurações pela idade da criança supervisionada.

VI. CONTRIBUIÇÕES

Os resultados obtidos por meio da aplicação do MIS revelam que o *AirDroid Parental Control* e o *Google Family Link*, embora ambos propostos como ferramentas de supervisão e monitoramento parental, possuem duas abordagens distintas de controle digital: uma centrada na **vigilância ativa e intrusiva** (*AirDroid*) e outra orientada à **mediação e ao estabelecimento de hábitos** (*Family Link*). Essa distinção não é meramente técnica, mas reflete diferentes metagens projetadas pelos designers e, consequentemente, distintos perfis de usuário.

Conforme evidenciado na Seção V-A, o *AirDroid Parental Control*, embora possua uma riqueza de funcionalidades, projeta uma relação de poder assimétrica na qual o responsável tem acesso irrestrito ao dispositivo do menor, incluindo funcionalidades como ativação remota da câmera e do microfone, espelhamento de tela em tempo real e leitura de notificações de aplicativos. Essa abordagem, que denominamos **vigilância ativa**, pressupõe que a segurança digital só é alcançável mediante o monitoramento constante e, em certa medida, encoberto — uma vez que o sistema incentiva o uso em modo invisível (Fig.1, D), que oculta o aplicativo de monitoramento no celular do filho. Apesar de citar brevemente a importância do diálogo entre pais, ou responsáveis/tutores, e filhos (Fig.1, E) em nenhum momento essa mensagem é repassada durante o uso das funcionalidades de vigilância, fazendo com que a mensagem implícita seja de que o menor não precisa ter privacidade ou autonomia digital, e que o responsável precisa verificar ativamente cada ação para prevenir riscos. A metacomunicação não aborda questões associadas a limites éticos da vigilância, o que pode permitir, e talvez até induzir, usos abusivos de suas funcionalidades.

Em contraste, o *Google Family Link* (Seção V-B) adota uma estratégia de **mediação estruturada**. Suas funcionalidades, limites de tempo de tela, programações de descanso e horário escolar, bloqueio remoto e filtros de conteúdo são desenhadas para operar de forma transparente e negociada. A criança ou adolescente recebe notificações claras sobre o tempo restante, e o sistema incentiva diálogos sobre o uso saudável da tecnologia. No entanto, o *Google Family Link* poderia explicitar mais claramente as consequências das ações, como a remoção da conta ou o bloqueio prolongado, melhorando assim sua comunicabilidade.

Para escolher entre as diferentes estratégias, o tutor deveria entender claramente a proposta de cada uma delas. No entanto, a apresentação da estratégia não é claramente comunicada em signos iniciais da interface. Além disso, o *AirDroid Parental Control* requer um conhecimento técnico ou familiaridade maior com tecnologia, uma vez que envolve o acesso direto a elementos do telefone da criança, via seu próprio telefone.

Do ponto de vista “social”, a motivação da escolha entre as ferramentas pode estar associada às estratégias educacionais adotadas pelo responsável, à sua percepção e nível de receio dos riscos digitais, e também nível de confiança nos filhos e autonomia dada aos filhos. Vale ressaltar, que existem estudos que evidenciam a importância de não apenas proteger crianças e adolescentes, mas também prepará-los (em especial adolescentes) para lidar com os desafios de segurança online de forma independente [41].

Em síntese, os resultados indicam que ambas as ferramentas ainda não atendem integralmente às disposições estabelecidas pelo ECA Digital [5] para o contexto brasileiro, especialmente no que se refere à supervisão parental e às soluções de monitoramento infantil. Entre as lacunas observadas, destaca-se o **não atendimento ao disposto no Art. 19, § 1º**, que determina que crianças e adolescentes sejam informados quando estiverem sendo monitorados, **bem como ao Art. 18, § 3º**, que estabelece que ferramentas de supervisão devem permitir aos responsáveis identificar os perfis de adultos com os quais a criança ou o adolescente se comunica.

VII. CONCLUSÃO

Este trabalho analisou a comunicabilidade de duas ferramentas de controle parental, *AirDroid Parental Control* e *Google Family Link*, por meio da aplicação do Método de Inspeção Semiótica e da análise da adequação a legislação brasileira. Os resultados evidenciaram duas estratégias distintas de controle digital: a **vigilância ativa**, característica do *AirDroid Parental Control*, com recursos como acesso remoto à câmera e ao microfone, e a **mediação estruturada**, presente no *Google Family Link*, com foco em limites de tempo, programações e transparência. Ambas, contudo, enfrentam desafios de comunicabilidade, que podem gerar confusão no usuário final, e de conformidade com o ECA Digital.

As estratégias propostas como solução por cada aplicativo refletem não apenas diferentes soluções técnicas, mas também distintas concepções sobre o que significa proteger uma criança no ambiente digital. No atual contexto, cabe aos responsáveis refletirem sobre qual modelo melhor se alinha à construção de um ambiente digital seguro, respeitoso e formativo para seus filhos.

Como contribuição, este trabalho preenche uma lacuna identificada na literatura ao oferecer uma análise comparativa das soluções propostas por duas ferramentas representativas de controle parental, aspecto pouco explorado em estudos anteriores, e a contextualização no cenário brasileiro. Os resultados aqui apresentados interessam especialmente a pesquisadores das áreas de Interação Humano-Computador, segurança digital e áreas afins que buscam compreender como diferentes estratégias de supervisão são comunicadas aos usuários. Além disso, projetistas dessas ferramentas podem se beneficiar das análises aqui realizadas, utilizando os achados sobre desafios de comunicabilidade para orientar o (re)projeto de interfaces mais claras, éticas e alinhadas às reais necessidades de pais e responsáveis.

Apesar dos resultados alcançados, deve-se considerar que a análise limitou-se à inspeção conduzida por uma única avaliadora, ainda que com validação de uma pesquisadora sênior, e restringiu-se à análise de duas ferramentas específicas no contexto do sistema Android. Um trabalho futuro de interesse é ampliar a análise para outras plataformas para investigar se outras estratégias são propostas e como são apresentadas aos responsáveis. Além disso, seria interessante a realização de estudos que incluam a avaliação com usuários reais (pais e crianças/adolescentes), e também uma investigação interdisciplinar que analisasse os impactos psicológicos de diferentes modelos de supervisão na autonomia e privacidade dos menores.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] M. Prensky, "Digital Natives, Digital Immigrants Part 1," *On the Horizon: The International Journal of Learning Futures*, vol. 9, no. 5, pp. 1–6, 09 2001. [Online]. Available: <https://doi.org/10.1108/10748120110424816>
- [2] S. Mann, A. Calvin, A. Lenhart, and M. B. Robb, "The Common Sense Census: Media Use by Kids Zero to Eight, 2025," *Common Sense Media, Tech. Rep.*, Feb. 2025, acessado em 27 maio 2026. [Online]. Available: <https://www.common-sense-media.org/sites/default/files/research/report/2025-common-sense-census-web-2.pdf>
- [3] OECD, *How's Life for Children in The Digital Age?* OECD Publishing, 2025.
- [4] J. A. M. Marcílio and L. M. Santos, "A Adultização de Crianças e Adolescentes À Luz do Direito Penal e do Estatuto da Criança e do Adolescente (ECA)," *Revista Ibero-Americana de Humanidades, Ciências e Educação*, vol. 11, no. 11, pp. 6407–6414, Nov. 2025. [Online]. Available: <https://periodicorease.pro.br/rease/article/view/22366>
- [5] Brasil, "Lei No. 15.211, de 17 de setembro de 2025: Estatuto Digital da Criança e do Adolescente," <https://www.planalto.gov.br/ccivil03/ato2023-2026/2025/lei/l15211.htm>, 2025, acessado : Maio 26, 2026.
- [6] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, "Parental Controls: Safer Internet Solutions or New Pitfalls?" *IEEE Security Privacy*, vol. 19, no. 6, pp. 36–46, 2021.
- [7] M. Stoev and D. K. Sarmah, "Online Protection for Children Using a Developed Parental Monitoring Tool," in *Proceedings of Eighth International Congress on Information and Communication Technology*, X.-S. Yang, R. S. Sherratt, N. Dey, and A. Joshi, Eds. Singapore: Springer Nature Singapore, 2023, pp. 205–215.
- [8] V. Gnanasekaran and K. De Moor, "Usability, Security, and Privacy Recommendations for Mobile Parental Control," in *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*, ser. EICC '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 138–143. [Online]. Available: <https://doi.org/10.1145/3590777.3590800>
- [9] Fast Company Brasil, "Apenas 17% dos Pais Utilizam Ferramentas para Controlar o Acesso das Crianças à Internet," <https://fastcompanybrasil.com/news/penas-17-utilizam-ferramentas-para-controlar-o-acesso-das-criancas-a-internet/>, Aug. 2023, acessado em 27 maio 2026.
- [10] J. Lee, S. Lee, and Y. Shin, "Lack of Parental Control Is Longitudinally Associated with Higher Smartphone Addiction Tendency in Young Children: A Population-Based Cohort Study," *Journal of Korean Medical Science*, vol. 39, no. 34, p. e254, Sep. 2024. [Online]. Available: <https://doi.org/10.3346/jkms.2024.39.e254>
- [11] C. S. de Souza, C. F. Leitão, R. O. Prates, and E. J. da Silva, "The Semiotic Inspection Method," in *Proceedings of VII Brazilian Symposium on Human Factors in Computing Systems*, ser. IHC '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 148–157. [Online]. Available: <https://doi.org/10.1145/1298023.1298044>
- [12] E. Smith, "Why We Won't Stop Trying To Filter The Internet," <https://tedium.co/2025/08/26/internet-content-filters-history/>, 2025, acessado: Maio 26, 2026.
- [13] Australian Government eSafety Commissioner, "Online Safety Act," <https://www.esafety.gov.au/about-us/who-we-are/online-safety-act>, 2021, acessado: Maio 26, 2026.
- [14] Federal Trade Commission, "Children's Online Privacy Protection Rule ("COPPA")," <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>, 2025, acessado: Maio 26, 2026.
- [15] United States Congress, "Kids Online Safety Act (KOSA)," <https://www.congress.gov/bill/118th-congress/senate-bill/1409>, 2025, acessado: Maio 26, 2026.
- [16] European Commission, "Better Internet for Kids (BIK+) Strategy," <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>, 2022, acessado: Maio 26, 2026.
- [17] French Government, "Social Media Restrictions for Minors in France," <https://www.gouvernement.fr>, 2025, acessado: Maio 26, 2026.
- [18] Danish Government, "Digital Protection Measures for Children and Adolescents," <https://digst.dk>, 2025, acessado: Maio 26, 2026.
- [19] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and P. J. Wisniewski, "A Matter of Control or Safety? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–14. [Online]. Available: <https://doi.org/10.1145/3173574.3173768>
- [20] P. Dumar, H. Atashpanjeh, and M. N. Al-Ameen, "'It's Hard for Him to Make Choices Sometimes and He Needs Guidance': Re-orienting Parental Control for Children," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, no. CSCW1, Apr. 2024. [Online]. Available: <https://doi.org/10.1145/3637359>
- [21] R. Panchanadikar, Y. Hu, K. Guo, A. L. Hall, H. Hu, N. Vishwamitra, and G. Freeman, "Beyond Age-Based Restrictions: Rethinking Children's Online Safety Through Comparing Parent-Child Perspectives of Risks in User-Generated Content Games," in *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, ser. CHI '26. New York, NY, USA: Association for Computing Machinery, 2026. [Online]. Available: <https://doi.org/10.1145/3772318.3790868>
- [22] P. Dumar and M. N. Al-Ameen, "'It's Like Educating us Older People...': Unveiling Needs and Expectations Regarding Educational Features within Parental Control Tools," in *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: <https://doi.org/10.1145/3613905.3651113>
- [23] UNICEF Innocenti, "Childhood in a Digital World: Screen Time, Digital Skills and Mental Health," UNICEF Innocenti – Global Office of Research and Foresight, Florence, Italy, Tech. Rep., 2025, acessado: Maio 26, 2026. [Online]. Available: <https://www.unicef.org/innocenti/reports/childhood-digital-world>

- [24] E. Bozzola, G. Spina, R. Agostiniani, S. Barni, R. Russo, E. Scarpato, A. Di Mauro, A. V. Di Stefano, C. Caruso, G. Corsello, and A. Staiano, "The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks," *International Journal of Environmental Research and Public Health*, vol. 19, no. 16, 2022. [Online]. Available: <https://www.mdpi.com/1660-4601/19/16/9960>
- [25] S. I. Alqahtani, W. M. S. Yafooz, A. Alsaedi, L. Syed, and R. Alluhaibi, "Children's Safety on YouTube: A Systematic Review," *Applied Sciences*, vol. 13, no. 6, 2023. [Online]. Available: <https://www.mdpi.com/2076-3417/13/6/4044>
- [26] S. Alshamrani, A. Abusnaina, M. Abuhamad, D. Nyang, and D. Mohaisen, "Hate, Obscenity, and Insults: Measuring the Exposure of Children to Inappropriate Comments in YouTube," in *Companion Proceedings of the Web Conference 2021*, ser. WWW '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 508–515. [Online]. Available: <https://doi.org/10.1145/3442442.3452314>
- [27] R. Armitage, "Social Media Usage in Children: An Urgent Public Health Problem," *Public Health*, vol. 200, pp. e2–e3, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0033350621003589>
- [28] J. V. Assis and G. Valença, "Is My Child Safe Online? - On Requirements for Parental Control Tools in Apps used by Children," *Journal on Interactive Systems*, vol. 15, no. 1, p. 823–838, Aug. 2024. [Online]. Available: <https://journals-sol.sbc.org.br/index.php/jis/article/view/4240>
- [29] Z. Iftikhar, Q. R. u. Haq, O. Younus, T. Sardar, H. Arif, M. Javed, and S. Shahid, "Designing Parental Monitoring and Control Technology: A Systematic Review," in *Human-Computer Interaction – INTERACT 2021: 18th IFIP TC 13 International Conference, Bari, Italy, August 30 – September 3, 2021, Proceedings, Part IV*. Berlin, Heidelberg: Springer-Verlag, 2021, p. 676–700. [Online]. Available: https://doi.org/10.1007/978-3-030-85610-6_39
- [30] P. Dumarú and M. N. Al-Ameen, "One Size Doesn't Fit All: Towards Design and Evaluation of Developmentally Appropriate Parental Control Tool," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, ser. CHI '25. New York, NY, USA: Association for Computing Machinery, 2025. [Online]. Available: <https://doi.org/10.1145/3706598.3713548>
- [31] K. Joshi, R. Trivedi, J. Patel, and R. Karani, "Guardian Eye: Hostile Parental Control Solution," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2024, pp. 1–7.
- [32] G. Wang, J. Zhao, K. Kollnig, A. Zier, B. Duron, Z. Zhang, M. Van Kleek, and N. Shadbolt, "KOALA Hero Toolkit: A New Approach to Inform Families of Mobile Datafication Risks," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, ser. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: <https://doi.org/10.1145/3613904.3642283>
- [33] M. Stoilova, M. Bulger, and S. Livingstone, "Do Parental Control Tools Fulfil Family Expectations for Child Protection? A Rapid Evidence Review of The Contexts and Outcomes of Use," *Journal of Children and Media*, vol. 18, no. 1, pp. 29–49, 2024. [Online]. Available: <https://doi.org/10.1080/17482798.2023.2265512>
- [34] N. Rojas, N. Boettcher, P. P. Játiva, and M. G. Gaitán, "Evaluation of Parental Control Tools Functionalities: The Chilean Context," in *Advanced Research in Technologies, Information, Innovation and Sustainability*, T. Guarda, F. Portela, and M. F. Augusto, Eds. Cham: Springer Nature Switzerland, 2025, pp. 303–314.
- [35] The New York Times Wirecutter, "The Best Parental-Control Apps to Manage Screen Time (and Keep Your Kid Safer Online)," <https://www.nytimes.com/wirecutter/reviews/best-apps-to-manage-your-kids-phone/>, 2025, acessado em: 26 maio 2026.
- [36] The National Parenting Center, "AirDroid Parental Control," <https://nationalparentingcenter.com/airdroid-parental-control/>, 2025, acessado: Maio 26, 2026.
- [37] Common Sense Media, "Parents' Ultimate Guide to Parental Controls," <https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-parental-controls>, Mar. 2021, acessado em: 26 maio 2026.
- [38] C. S. de Souza and C. F. Leitão, *Semiotic Engineering Methods for Scientific Research in HCI*. Morgan & Claypool Publishers, 2009.
- [39] C. S. de Souza, *The Semiotic Engineering of Human-Computer Interaction*. MIT press, 2005.
- [40] R. O. Prates, C. S. De Souza, and S. D. Barbosa, "Methods and Tools: A Method for Evaluating the Communicability of User Interfaces," *interactions*, vol. 7, no. 1, pp. 31–38, 2000.
- [41] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?" in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, ser. CSCW '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 51–69. [Online]. Available: <https://doi.org/10.1145/2998181.2998352>

APÊNDICE

A. AirDroid Parental Control

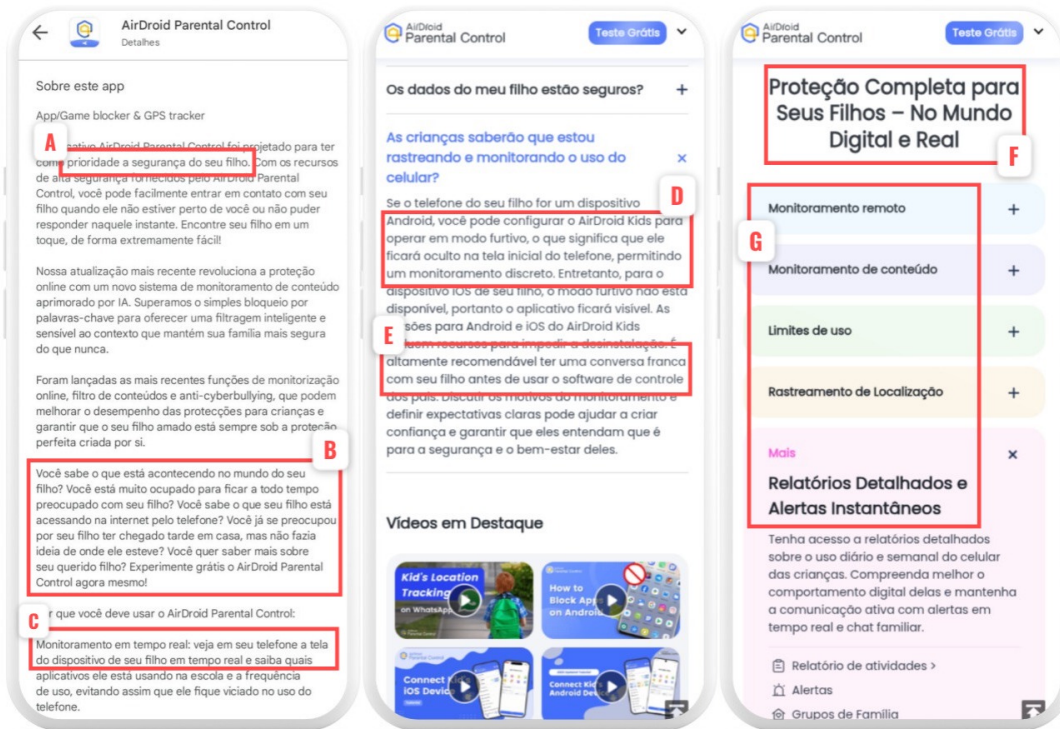


Fig. 1: Essa figura representa partes da documentação disponível sobre o sistema *AirDroid Parental Control*, expostos na *Google Play Store*, no FAQ e no site da ferramenta.

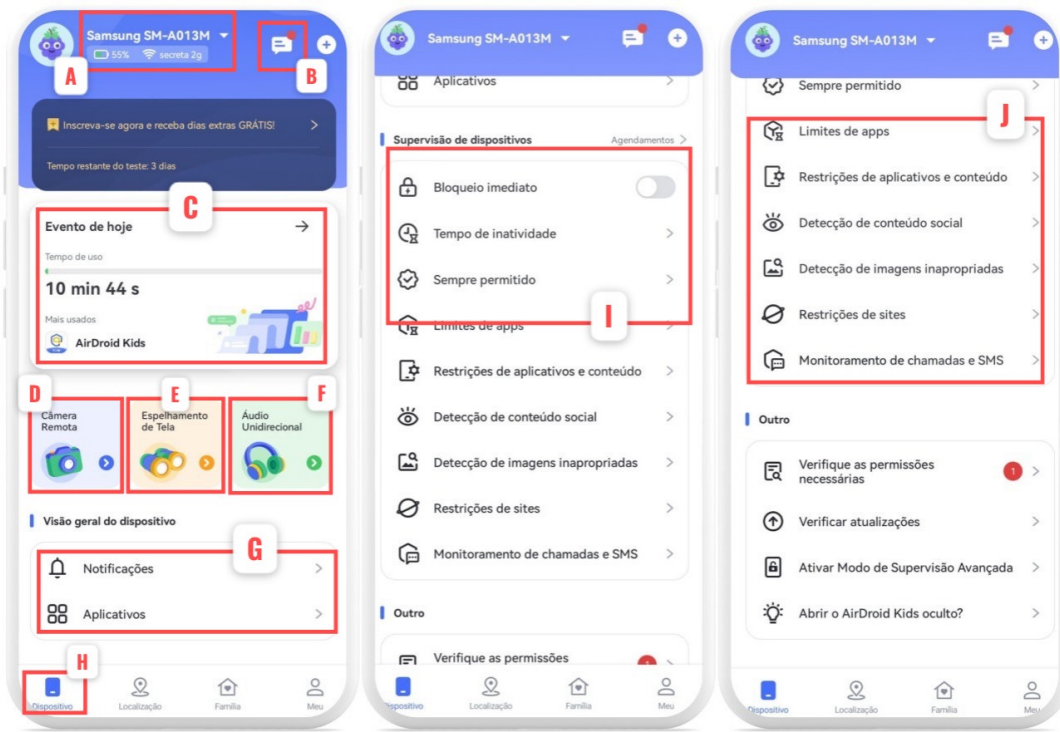


Fig. 2: Essa imagem representa a página inicial do aplicativo com todas as funcionalidades e configurações.

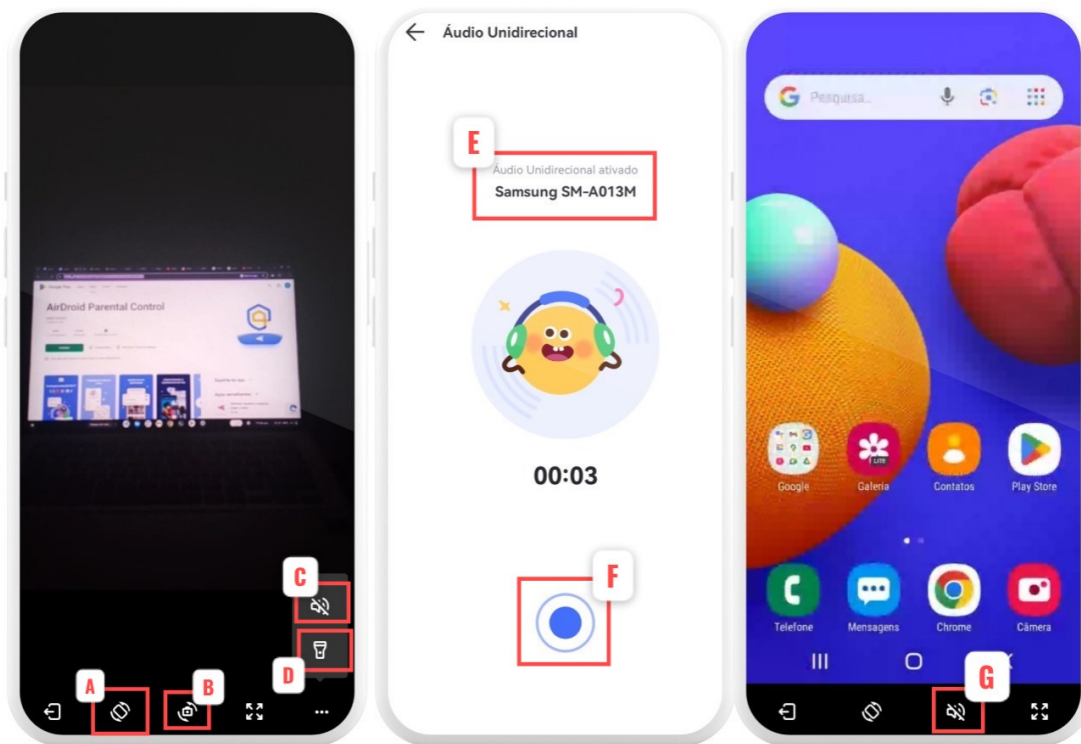


Fig. 3: Essa imagem é a representação das funcionalidade de acesso a câmera remota, áudio unidirecional e espelhamento de tela, respectivamente.

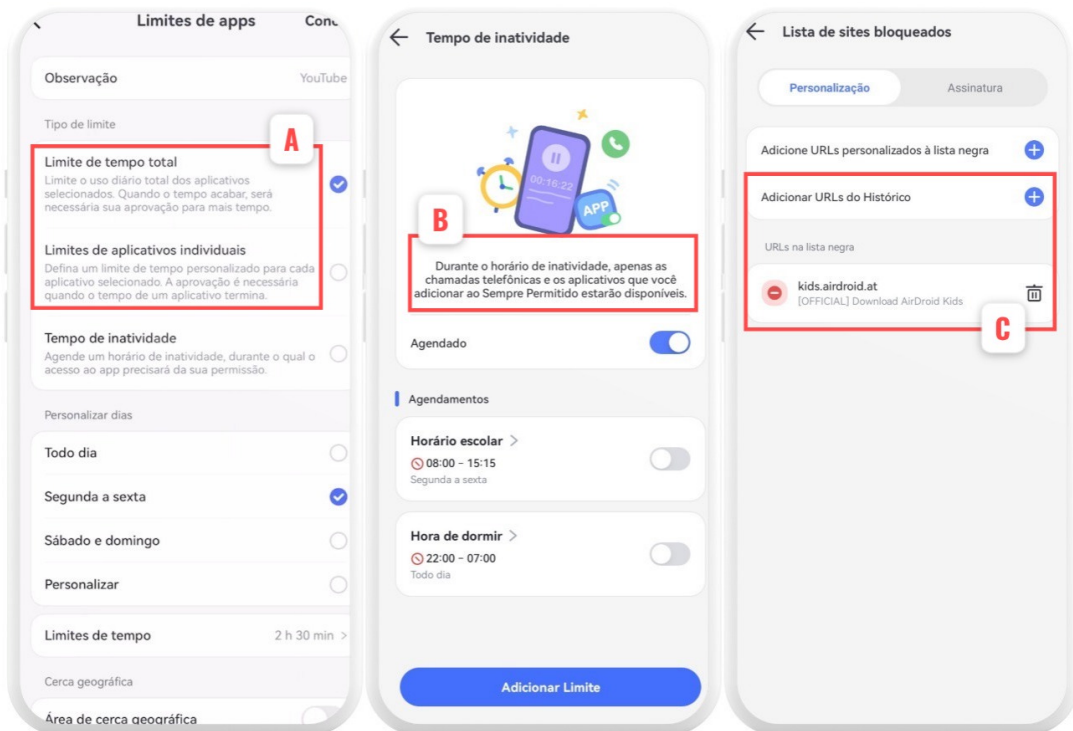


Fig. 4: Essa imagem é a representação das telas de configuração de limite de tempo, tempo de inatividade e listas de sites bloqueados, respectivamente.

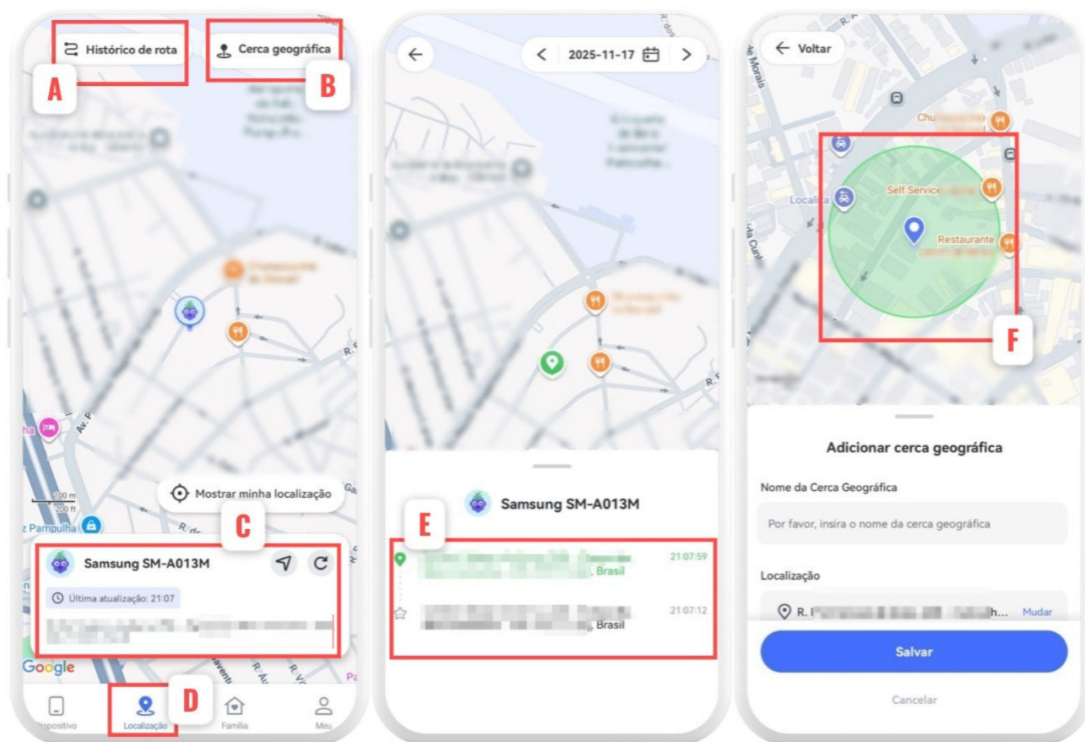


Fig. 5: Essa imagem exemplifica as funcionalidades de acesso a localização em tempo real, histórico de rotas e cercas geográficas, respectivamente.

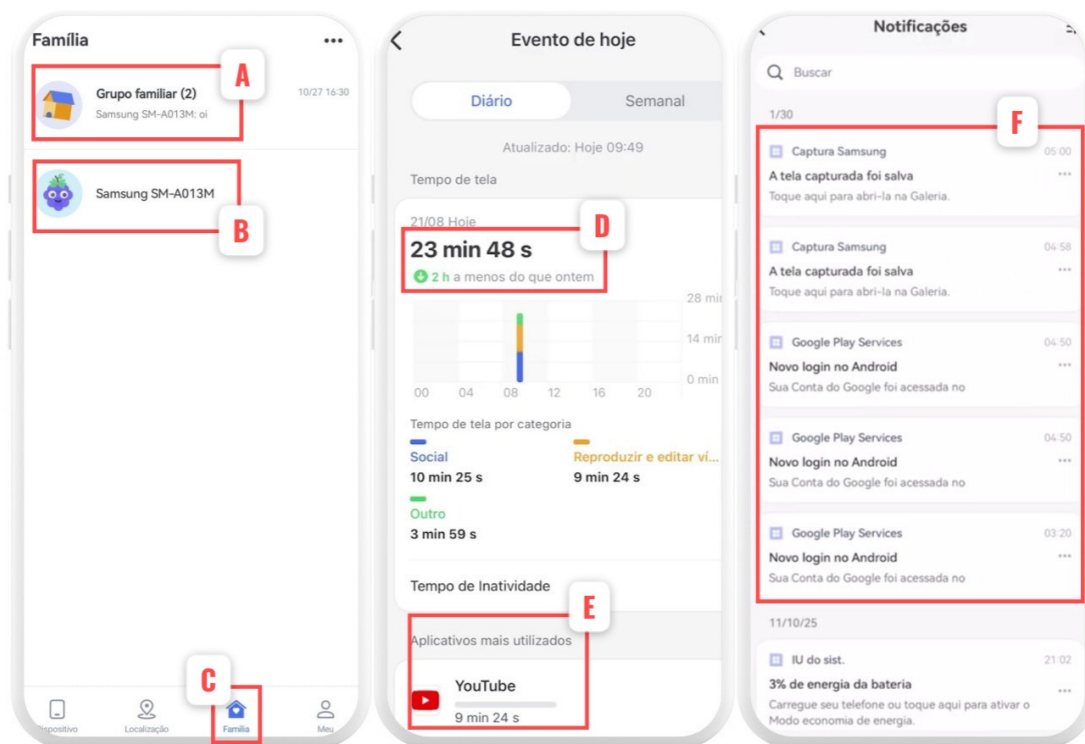


Fig. 6: Essa imagem representa as funcionalidades de chat, relatório de uso e acesso as notificações do aparelho supervisionado, respectivamente.

B. Google Family Link



Fig. 7: Essa figura representa partes da documentação disponível sobre o app na Play Store, no site da ferramenta e no FAQ.



Fig. 8: Essa imagem representa a página inicial do aplicativo com todas as funcionalidades e configurações relacionadas a limites de tempo e configurações e permissões do dispositivo.

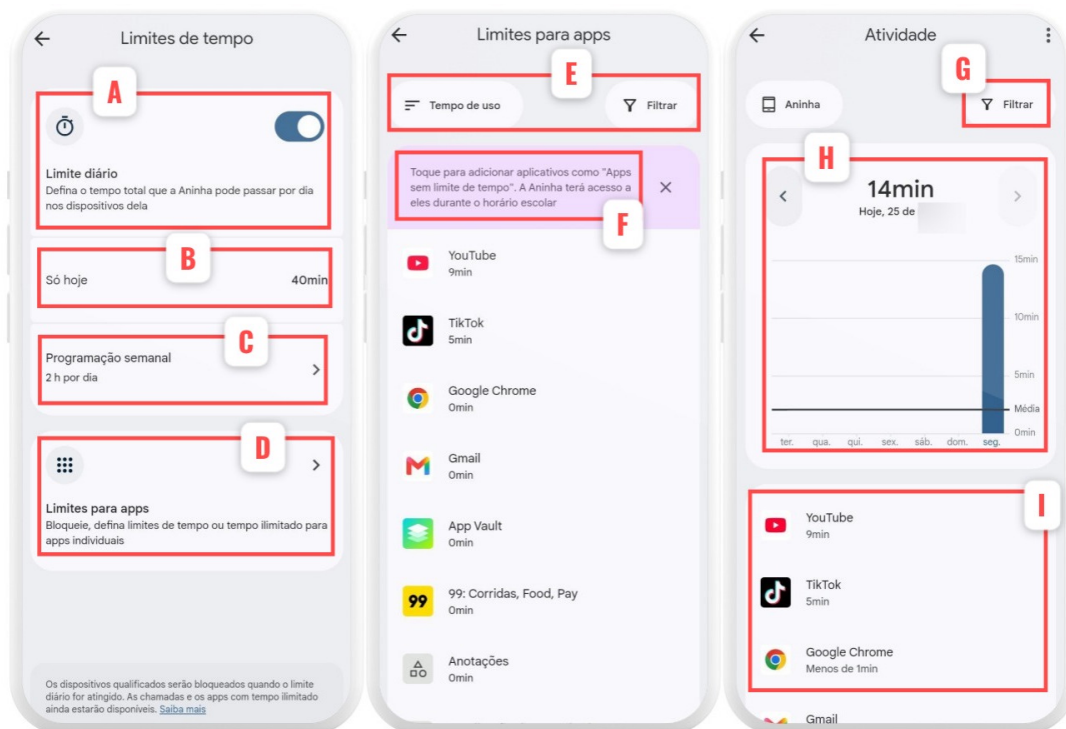


Fig. 9: Essa imagem representa as funcionalidades de limite de tempo, diário e para aplicativos, e o relatório de atividades no dispositivo supervisionado.

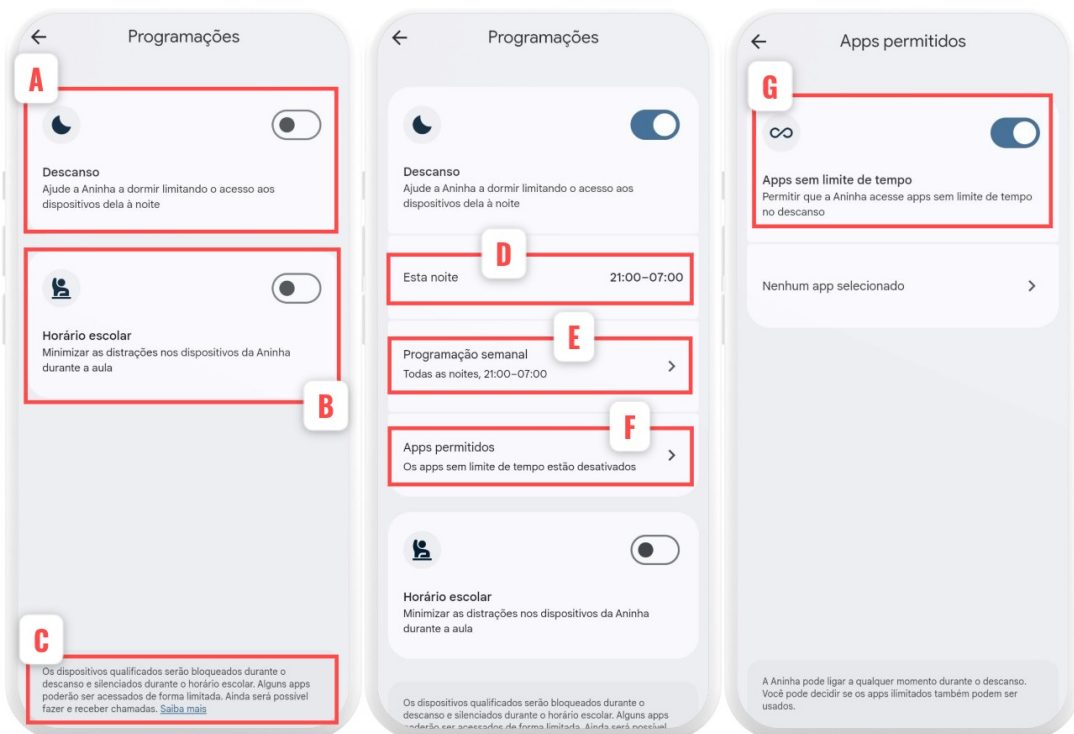


Fig. 10: Essa imagem explicita a funcionalidade de 'Programações', que define períodos de foco, filtrando o que pode ser acessado nesses períodos.

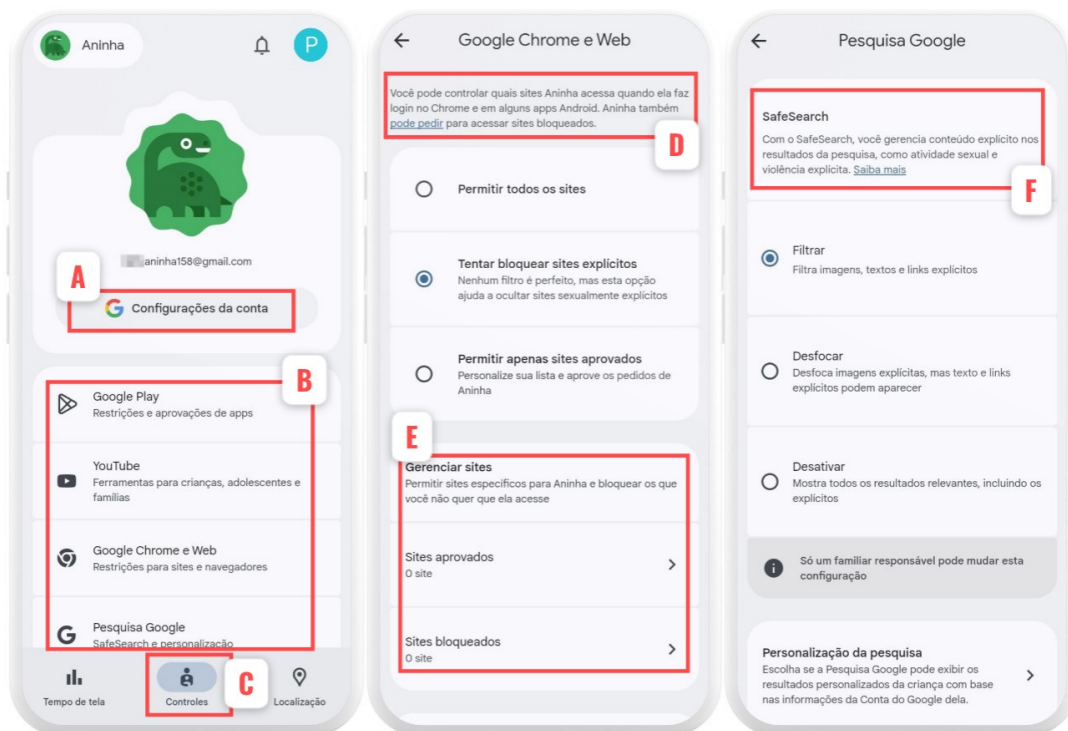


Fig. 11: Essa imagem representa o menu de 'Controles' do app, que é responsável por configurações nas ferramentas Google, como o *YouTube*, a *Play Store* e o *Chrome*.

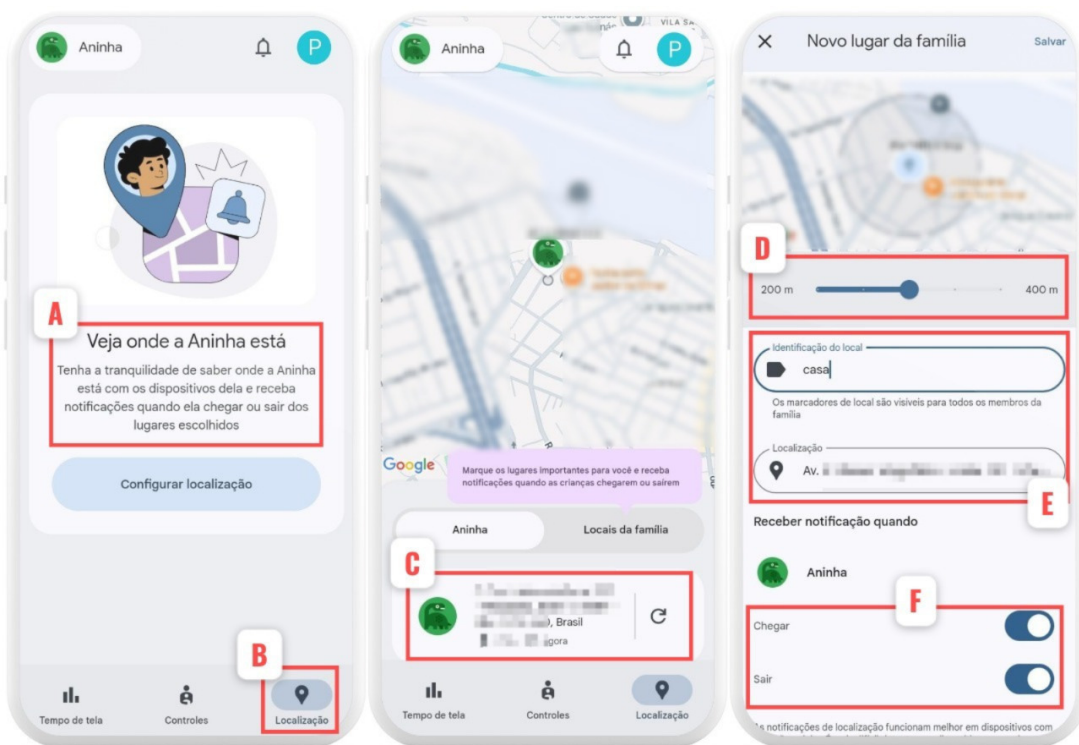


Fig. 12: Essa imagem representa as funcionalidades de localização, respectivamente, localização em tempo real e locais da família.