UNIVERSIDADE FEDERAL DE PERNAMBUCO
CIn – CENTRO DE INFORMÁTICA
PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Natália Ribeiro Barreto

Desenvolvimento de jogos digitais para crianças e adolescentes: um guia de práticas éticas para desenvolvedores

Recife
2025

Natália Ribeiro Barreto

Desenvolvimento de jogos digitais para crianças e adolescentes: um guia de práticas éticas para desenvolvedores

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

.

Área de concentração:
Inteligência Computacional.

Orientador(a): Prof. Dr. Geber L. Ramalho

Recife
2025

.Catalogação de Publicação na Fonte. UFPE - Biblioteca Central

Barreto, Natália Ribeiro.
Desenvolvimento de jogos digitais para crianças e adolescentes: um guia de práticas éticas para desenvolvedores / Natalia Ribeiro Barreto. - Recife, 2025.
157f.: il.

Dissertação (Mestrado) - Universidade Federal de Pernambuco, Centro de Informática, Programa de Pós-graduação em Ciência da Computação, 2025.
Orientação: Geber Lisboa Ramalho.
Inclui referências e apêndices.

1. Crianças e adolescentes; 2. Ética; 3. Jogos digitais; 4. Legislação; 5. Design dark patterns; 6. Boas práticas. I. Ramalho, Geber Lisboa. II. Título.

UFPE-Biblioteca Central

Natália Ribeiro Barreto

“Desenvolvimento de jogos digitais para crianças e adolescentes: um guia de práticas éticas para desenvolvedores”

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Inteligência Computacional

Aprovado em: 29/04/2025.

BANCA EXAMINADORA

_____

Profa. Dra. Carina Frota Alves
Centro de Informática / UFPE

_____

Prof. Dr. André Menezes Marques das Neves
Departamento de Design / UFPE

_____

Prof. Dr. Geber Lisboa Ramalho
Centro de Informática / UFPE
(**orientador**)

AGRADECIMENTOS

A Deus…

Agradeço aos meus pais, Kátia e Genival; e, sobretudo à minha mãe pela motivação e inspiração dos passos a serem seguidos, mesmo diante de todos os desafios.

Agradeço ao meu orientador, Prof. Geber Ramalho, por todo o apoio e compreensão, ao longo dessa caminhada, sem os quais não seria possível a realização deste trabalho.

Agradeço a todos os profissionais que dedicaram um pouco do seu tempo para participar da pesquisa.

Agradeço a todos os docentes do programa de Pós-Graduação do Centro de Informática da UFPE, pelo conhecimento compartilhado nesta caminhada.

Enfim, agradeço a todos e todas que sempre me ajudaram com uma palavra amiga, um estímulo, uma confiança de que eu chegaria até aqui.

RESUMO

Crianças e adolescentes são usuários ativos e altamente engajados no consumo de jogos digitais. Nos últimos anos, à medida que o volume de dados compartilhados e a exposição *online* desses usuários aumentam, intensificam-se os debates globais sobre violações dos direitos das crianças no ambiente virtual e a necessidade de regulamentar práticas éticas no design de jogos voltados a esse público. Observa-se uma lacuna entre os princípios éticos, as exigências legais e algumas decisões tomadas pelo mercado de jogos. Este trabalho propõe um guia de boas práticas éticas para servir como suporte de orientação aos desenvolvedores independentes de jogos. Para isso, compilamos a legislação pertinente e as recomendações da literatura sobre jogos — com ênfase em *design dark patterns* — elaborando uma lista de hipóteses que foi submetida a um grupo de desenvolvedores por meio de um *survey* para validação. Como resultado, elegemos 48 boas práticas, organizadas em 9 categorias e apontamos quais foram consideradas mais relevantes pelos desenvolvedores.

Palavras-chave: *crianças e adolescentes; ética; jogos digitais; legislação; design dark patterns; boas práticas*

ABSTRACT

Children and adolescents are active and highly engaged users of digital games. In recent years, as the volume of shared data and online exposure of these users increases, global debates have intensified regarding violations of children's rights in the virtual environment and the need to regulate ethical practices in game design targeting this audience. In practice, there is a gap between ethical principles, legal requirements, and some decisions made by the game industry. This study proposes a guide of ethical best practices to serve as a reference for independent game developers. To this end, we compiled relevant legislation and recommendations from game literature - with a focus on *design dark patterns* - developing a list of hypotheses that was submitted to a group of developers through a survey for validation. As result, we identified 48 best practices, organized into 9 categories, and highlighted those deemed most relevant by developers.

Keywords: *children and teens; ethics; digital games; legislation; design dark patterns; best practices*

LISTA DE GRÁFICOS

Gráfico 1 - Atividades: Permissão do responsável para o uso da Internet. 19
Gráfico 2 - Mediação técnica do responsável para uso da Internet. 20
Gráfico 3 - Áreas de atuação profissional dos participantes da pesquisa. 85
Gráfico 4 - Categorias de jogos desenvolvidas pelos participantes da pesquisa. 86
Gráfico 5 - Público-alvo dos jogos desenvolvidos pelos participantes da pesquisa. 87

LISTA DE TABELAS

Tabela 1 - Atributos dos dark pattern. 38

Tabela 2 - Taxonomia dark pattern proposta por Zagal et. al. 39

Tabela 3 - Taxonomia dark pattern proposta por Gray et. al. 40

Tabela 4 - Taxonomia dark pattern proposta por Fitton e Read. 42

Tabela 5 - Strings de pesquisa/palavras-chave. 48

Tabela 6 - Práticas candidatas e suas fontes de coleta. 49

Tabela 7 - Práticas candidatas da Categoria 1- Gerenciamento de Dados. 54

Tabela 8- Recomendações para adaptação de recursos por faixa etária. 56

Tabela 9 - Práticas candidatas da Categoria 2 - Controle parental. 58

Tabela 10 - Práticas candidatas da Categoria 3 - Classificação de usuários. 63

Tabela 11 - Práticas candidatas da Categoria 4 - Publicidade: geral. 66

Tabela 12 - Práticas candidatas da Categoria 5 - Publicidade: anúncios. 68

Tabela 13 - Práticas candidatas da Categoria 6 - Compras in-game. 72

Tabela 14 - Práticas candidatas da Categoria 7 - Game design: geral. 74

Tabela 15 - Práticas candidatas da Categoria 8 - Game design: recompensas. 77

Tabela 16 - Práticas candidatas da Categoria 9 - Game design: social features. 79

Tabela 17 - Resultado do survey da Categoria 1- Gerenciamento de dados. 89

Tabela 18 - Resultado do survey da Categoria 2 - Controle parental. 90

Tabela 19 - Resultados do survey da Categoria 3 - Classificação de usuários. 91

Tabela 20 - Resultados do survey da Categoria 4 - Publicidade: geral. 93

Tabela 21 - Resultados do survey da Categoria 5 - Publicidade: anúncios. 94

Tabela 22 - Resultados do survey da Categoria 6 - Compras in-game. 96

Tabela 23 - Resultados do survey da Categoria 7 - Game design: geral. 97

Tabela 24 - Resultados do survey da Categoria 8 - Game design: recompensas. 99

Tabela 25 - Resultados do survey da Categoria 9 - Game design: social features. 100

LISTA DE FIGURAS

Figura 1 - Categorização de selos kidSafe. 35

Figura 2 - Fluxograma geral de etapas metodológicas 46

Figura 3 - Fluxograma da metodologia da Etapa 1. 47

Figura 4 - Tópicos de enfoque e categorias criadas 52

Figura 5 - Exemplo de boa prática na tela de login do Roblox 58

Figura 6 - Exemplo ilustrativo de dark pattern “Privacy Zuckering” 59

Figura 7 - Etapa 1 do processo de consentimento dos pais da Epic Games 64

Figura 8 - Etapa 2 do processo de consentimento dos pais da Epic Games 65

Figura 9 - Etapa 3 do processo de consentimento dos pais da Epic Games 66

Figura 10 - Etapa 4 do processo de consentimento dos pais da Epic Games 67

Figura 11 - Etapa 5 do processo de consentimento dos pais da Epic Games 68

Figura 12 - Etapa 6 do processo de consentimento dos pais da Epic Games 69

Figura 13 - Exemplos de conformidade de parental gates 70

Figura 14 - Exemplo de bom uso do recurso Report no chat desktop do Roblox 71

Figura 15 - Exemplo de bom uso do recurso Report no chat mobile do Roblox 71

Figura 16 - Exemplos de conformidade para tela neutra. 74

Figura 17 - Esquema de remarketing para resgate de jogadores 77

Figura 18 - Esquema de remarketing para anúncio de produtos 77

Figura 19 - Exemplo de anúncio com uso de conteúdo nativo do jogo 80

Figura 20 - Exemplo de anúncio invasivo 81

Figura 21 - Exemplo de anúncios múltiplos na mesma tela 81

Figura 22 - Exemplo de dark pattern no jogo Kick the Buddy 82

Figura 23 - Conteúdos impróprios de anúncios para crianças 83

Figura 24 - Exemplo de Obstruction do iOS6 para limitar o rastreio de ads 85

Figura 25 - Exemplo ilustrativo de padrão Obstruction no contexto de compras 86

Figura 26 - Exemplo de prática sneaking em compra casada de itens 87

Figura 27 - Exemplo de padrão Pay to skip em FarmVille 2 88

Figura 28 - Exemplo de Pay to progress em My Little Pony 88

Figura 29 - Interface de passe de batalha no Fornite Season 10 89
Figura 30 - Exemplo ilustrativo de dark pattern de falsa hierarquia 90
Figura 31 - Exemplo de manipulação do jogador por notificações do Facebook 92
Figura 32 - Exemplo de manipulação do jogador em FarmVille 92
Figura 33 - Exemplo de temporal dark pattern em Animal Crossing 93
Figura 34 - Exemplo de padrão Grinding em Pokémon Go 94
Figura 35 - Exemplo de interface com uso de nudge indevido 95
Figura 36 - Exemplo ilustrativo de dark pattern Trick question 96
Figura 37 - Tela de loot boxes compradas com dinheiro em Overwatch 1 98
Figura 38 - Tela de recompensas diárias de login do Brawl Stars 99
Figura 39 - Exemplo de dark pattern Social Capital Based, em Farmville 2 102
Figura 40 - Exemplos de manipulação psicológica em Animal Crossing 103
Figura 41 - Exemplo ilustrativo de dark pattern Friend Spam 105
Figura 42 - Exemplo de pergunta do formulário aplicado ao survey 108
Figura 43 - Escala de classificação de relevância da prática 113

SUMÁRIO

1. Introdução..... 14
1.1 Contexto e motivação..... 14
1.2 Objetivos..... 16
1.3 Método..... 16

2. Conceitos fundamentais..... 17
2.1 Ética em software..... 17
2.2 Ética e direitos da criança no ambiente virtual..... 17
2.3 Ética em desenvolvimento de jogos..... 19

3. Problema de pesquisa..... 22
3.1 Experiência de crianças e pais/responsáveis..... 22
3.2 Experiência das instituições reguladoras..... 26
3.3 Experiência dos desenvolvedores de jogos..... 28

4. Estado da arte das forças regulatórias..... 31
4.1 Legislação..... 31
4.1.1 Children's Online Privacy Protection Act (COPPA)..... 31
4.1.2 General Data Protection Regulation (GDPR)..... 32
4.1.3 Artigo 14 da Lei Geral de Proteção de Dados (LGPD)..... 33
4.1.4 Projeto de lei nº 2628/2022..... 34
4.2 Normas e políticas de mercado..... 35
4.2.1 Players distribuidores..... 35
4.2.2 Entidades normativas..... 37
4.2.3 Programas de certificação..... 38
4.2.4 Ferramentas e plataformas compliance..... 39
4.3 Educação e capacitação..... 40
4.4 Dark patterns em jogos digitais..... 41
4.4.1 Conceito..... 41
4.4.2 Taxonomia..... 42
4.4.3 Implicações de uso..... 47

5. Etapa 1: Catalogação de candidatos via estudos e documentos..... 50
5.1 Método..... 51
5.1.1 Objetivo..... 51
5.1.2 Processo..... 51
5.1.3 Levantamento do rol de práticas..... 52
5.1.4 Agrupamentos das práticas similares..... 54
5.1.5 Categorização das práticas..... 55

5.2 Resultado e discussão das práticas candidatas..... 57
5.2.1 Categoria 1 - Gerenciamento de dados..... 58
5.2.2 Categoria 2 - Controle Parental..... 63
5.2.3 Categoria 3 - Classificação de usuários..... 76
5.2.4 Categoria 4 - Publicidade: geral..... 79
5.2.5 Categoria 5 - Publicidade: anúncios..... 82
5.2.6 Categoria 6 - Compras in-game..... 88
5.2.7 Categoria 7 - Game design: geral..... 94
5.2.8 Categoria 8 - Game design: recompensas..... 100
5.2.9 Categoria 9 - Game design: social features..... 103

6. Etapa 2: Validação via survey..... 109
6.1 Método..... 109
6.1.1 Objetivo..... 110
6.1.2 Elaboração do formulário..... 110
6.1.3 Participantes..... 111
6.2 Resultados: Validação..... 115
6.2.1 Categoria 1 - Gerenciamento de dados..... 116
6.2.2 Categoria 2 - Controle parental..... 118
6.2.3 Categoria 3 - Classificação de usuários..... 119
6.2.4 Categoria 4 - Publicidade: geral..... 120
6.2.5 Categoria 5 - Publicidade: anúncios..... 121
6.2.6 Categoria 6 - Compras in-game..... 123
6.2.7 Categoria 7 - Game design: geral..... 124
6.2.8 Categoria 8 - Game design: recompensas..... 126
6.2.9 Categoria 9 - Game design: social features..... 127
6.3 Consolidação dos resultados por categoria e tipo de relevância..... 129

7. Limitações e aprimoramentos de pesquisa..... 130

8. Considerações finais..... 132

REFERÊNCIAS..... 135

APÊNDICE A..... 141

APÊNDICE B..... 149

1. Introdução

1.1 Contexto e motivação

Em 2022, a Epic Games - empresa desenvolvedora do jogo *Fortnite* - enfrentou graves acusações sobre coletar dados pessoais de menores de 13 anos, sem o devido consentimento dos pais ou responsáveis, violando o que estabelece o *Children's Online Privacy Protection Act* (COPPA). Além disso, a empresa também foi apontada por usar estratégias desonestas para induzir compras não intencionais dentro do seu jogo. Como resultado da sanção e acordos entre as partes, uma multa total equivalente a $520 milhões de dólares foi aplicada, por parte da *FTC - Federal Trade Comission* (CNN, 2022).

Esse caso - além de outros semelhantes enfrentados por empresas como Youtube, Tik Tok entre outros - aquecem debates ao redor do mundo em volta de um assunto que, por muito tempo, foi tratado com negligência ou pouca relevância por milhares de empresas desenvolvedoras: a violação dos direitos da criança no ambiente virtual e a importância de regulamentar práticas éticas no *design* de jogos que envolvam crianças e adolescentes como usuárias.

É inegável que, atualmente, crianças e adolescentes são consumidores virtuais altamente engajados. Um percentual significativo de menores de 18 anos compõe - muitas vezes, sem qualquer distinção em relação aos jogadores adultos - uma parcela imensa da base de usuários de títulos de sucesso, no mercado de jogos digitais, como *Roblox*, *Freefire*, *Minecraft*, *Pokemon Go* entre outros. Os pais, por sua vez, pouco conseguem administrar e controlar, com facilidade, segurança e critérios adequados, as atividades *online* dos filhos.

As estratégias de retenção, bem como monetização, utilizadas pelos jogos mais recentes pressupõem uma experiência cada vez mais personalizada, apresentando *features* que, frequentemente, exigem captura dos mais diversos tipos de dados, de natureza pessoal ou não, relativos ao perfil e comportamento dos usuários (SEIF EL-NASR; KLEINMAN, 2020).

Em contramão, concomitante a esse cenário, as legislações internacionais e nacionais enrijeceram suas restrições quanto à proteção da privacidade de dados digitais de crianças e adolescentes, com o objetivo de coibir e sancionar práticas abusivas que possam comprometer sua integridade física, emocional e cognitiva.

Liccardi (2014) argumenta que o acesso aos dados pessoais não está, necessariamente, relacionado à presença de política de privacidade, sendo a maioria delas de difícil entendimento e ignoradas pelos usuários. As políticas de privacidade das lojas de aplicativos podem ser enganosas para compreensão dos pais e responsáveis; e, demonstra que há uma disparidade entre o conteúdo real, com base nas descrições dos desenvolvedores, e a classificação indicativa selecionada dos aplicativos.

Esse cenário reforça a existência de um *gap* entre os princípios éticos genéricos, as exigências legais e a prática do mercado desenvolvedor.

Como forma de proteger crianças e adolescentes contra práticas abusivas, os agentes reguladores criam instrumentos legais que contemplam um amplo espectro de partes interessadas, mas o desenvolvedor que está na ponta dessa cadeia - a quem se imputa tais exigências - ainda carece de instrumentos técnicos que suportem suas decisões de design e operação.

Ao mencionarmos "desenvolvedores" ao longo deste trabalho, referimo-nos de forma abrangente a todos os profissionais envolvidos na cadeia de produção de jogos digitais. Isso inclui não apenas programadores, mas também produtores, designers, artistas, roteiristas, game designers, testers, especialistas em usabilidade, entre outros. Cada um desses profissionais, a seu modo, contribui para as decisões de design, funcionamento e operação de um jogo, influenciando diretamente na experiência do usuário final. Portanto, a responsabilidade ética no desenvolvimento de jogos deve ser entendida como um compromisso coletivo, compartilhado entre os diversos agentes que integram esse ecossistema criativo e técnico.

Nesse sentido, as práticas recomendadas aqui não se dirigem exclusivamente a um único papel ou função, mas abrangem todos os envolvidos no processo de desenvolvimento. Acreditamos que atribuir a responsabilidade ética a apenas uma função profissional não seria possível de forma assertiva, pois simplificaria de forma inadequada a complexa dinâmica de governança que caracteriza a indústria de jogos digitais, marcada por processos colaborativos; decisões interdependentes; e, estruturas, muitas vezes, descentralizadas.Por isso, a promoção de uma cultura ética deve ser compreendida como um esforço coletivo, transversal a todas as etapas e funções do ciclo de produção.

Acreditamos que o trabalho é relevante e original por apresentar, de forma inédita, um guia de boas práticas éticas voltado especificamente para o desenvolvimento de jogos digitais destinados a crianças e adolescentes. A originalidade reside na abordagem multidisciplinar adotada, que integra fundamentos legais, normativos e acadêmicos — com destaque para o conceito de *dark patterns* — e os traduz em orientações técnicas acessíveis aos profissionais da área.

Ao propor uma ponte entre teoria e prática, o trabalho tenta oferecer um instrumento aplicável ao cotidiano dos desenvolvedores para mitigar essas ameaças no contexto do design e da operação de jogos.

1.2 Objetivos

Neste trabalho, nosso objetivo principal é propor um guia de boas práticas éticas que possa servir como suporte de orientação para os desenvolvedores independentes de jogos. Como objetivo complementar, procuramos validar as práticas candidatas compiladas no guia, com o propósito de investigar a adesão desses desenvolvedores às respectivas práticas.

1.3 Método

Tendo estes objetivos em mente, a metodologia foi estruturada em duas principais etapas: a catalogação de potenciais práticas éticas; e, em seguida, a realização de um *survey*, junto aos profissionais do mercado de jogos.

Na primeira etapa, o objetivo foi estabelecer uma lista de hipóteses de boas práticas, através da revisão de fontes legais, normativas e acadêmicas. Esta última com foco, particularmente, em *design dark patterns*. Como resultado consolidado desta etapa, criamos um documento guia de práticas éticas candidatas.

Já na segunda etapa, nosso objetivo foi validar a relevância das práticas propostas no documento criado na primeira etapa. Para tal, aplicamos um formulário, em caráter de *survey*; e com base nas respostas, pontuamos conclusões e hipóteses acerca da experiência dos desenvolvedores.

2. Conceitos fundamentais

A pesquisa desta dissertação concentra-se no campo de estudo acerca da Ética da Informação, que discute os impactos morais da tecnologia digital, com ênfase na relação de crianças, adolescentes e pais, no contexto do consumo dos jogos digitais.

Sendo assim, neste capítulo, apresentaremos os conceitos fundamentais pertinentes a este recorte para atualização e melhor compreensão sobre os termos que serão citados ao longo de todo trabalho e que, também, embasam os demais trabalhos científicos da área.

2.1 Ética em *software*

Lessig (2006) argumenta que a **ética em *software*** está intrinsecamente ligada ao poder regulador do código-fonte, pois suas estruturas técnicas (como algoritmos, sistemas de criptografia ou mecanismos de vigilância) podem restringir ou ampliar a autonomia dos usuários, muitas vezes sem seu conhecimento. Para esse autor, é essencial que desenvolvedores e empresas reconheçam essa capacidade normativa do código e adotem princípios éticos no design, garantindo que sistemas digitais promovam **transparência, liberdade de expressão e justiça**, em vez de reforçar controle arbitrário ou desigualdades.

Floridi (2013) fundamenta o conceito de **ética da informação** como o ramo da Filosofia da Informação que investiga, em sentido amplo, o impacto ético da tecnologia digital na vida humana e na sociedade. Destaca-se como seus princípios fundamentais: (1) a beneficência, abrangendo dignidade e bem-estar; (2) a não-maleficência, abrangendo privacidade e segurança; (3) a autonomia, enfatizando a liberdade; (4) a justiça, que inclui a equidade e a solidariedade; (5) a transparência, que envolve a responsabilidade, a confiança e a explicabilidade (FLORIDI et. al.,2018; JOBIN et.al.,2019).

2.2 Ética e direitos da criança no ambiente virtual

O ambiente virtual tornou-se uma nova e significativa dimensão do desenvolvimento infantil, transformando a forma como elas aprendem, se comunicam e constroem identidades. A internet passou a desempenhar um papel central no processo de socialização das crianças, funcionando como um espaço de

aprendizagem informal, expressão e construção de laços sociais (HOLLOWAY et.al., 2013).

Conforme Lessig (2006), reconhecemos a existência 4 principais **mecanismos reguladores** do ambiente virtual: (1) a lei, formulada pelo Estado, que impõe regras formais de comportamento aos grupos sociais; (2) as normas sociais que, como regras informais, determinam quais comportamentos são socialmente aceitos ou não; (3) o mercado, que regula por meio de oferta e demanda os preços de produtos, serviços e sua competitividade; (4) a arquitetura (ou, podemos dizer, o código ou design) que define as possibilidades e limitações técnicas, influenciando diretamente a interação dos usuários no ambiente virtual (LESSIG, 2006).

A lei, como norma formal de regulação, reconhece que "a criança, em virtude de sua falta de maturidade física e mental, necessita de proteção e cuidados especiais, incluindo a devida proteção legal, tanto antes quanto após seu nascimento" (UNICEF, 2025). Em conformidade à Convenção dos Direitos da Criança da ONU, o Estatuto da Criança e do Adolescente (ECA) - principal marco legal no Brasil para a proteção dos direitos de crianças e adolescentes - além de resguardar seus direitos, preocupa-se em prevenir situações de risco, como violência, abuso e exploração (TEFFÉ, 2021).

No centro desta discussão, o **princípio do melhor interesse da criança,** consagrado no Artigo 3º da Convenção sobre os Direitos da Criança (CDC/1989), desponta como eixo central do direito internacional da infância, reforçando que políticas públicas, medidas judiciais devem sempre avaliar o impacto sobre a criança, garantindo sua proteção e dignidade. O princípio também se estende aos agentes privados de forma que, ao serem tomadas decisões que afetem as crianças, o interesse delas deve sempre ter prioridade em relação a quaisquer outras preocupações, inclusive interesses comerciais (Instituto ALANA, 2020). No Brasil, este princípio está incorporado ao Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069/1990) em seu artigo 4º.

A proteção da dignidade e da integridade física e emocional de crianças e adolescentes constitui um dos pilares fundamentais da ordem social. No contexto digital, assegurar seu **direito à privacidade** torna-se crucial para prevenir violências e explorações decorrentes da divulgação inadequada de suas informações.

Como mencionado anteriormente, Floridi (2013) destaca que este é um direito fundamental para a ética da informação, visando à proteção da identidade e à

autonomia dos indivíduos em um mundo cada vez mais interconectado, onde **dados pessoais** são coletados e processados em uma escala cada vez maior. Caso contrário, os indivíduos ficariam vulneráveis a manipulações, discriminações e perda de liberdade, o que compromete sua capacidade de agir como agentes morais livres.

São considerados como **dados pessoais** quaisquer *"informações individualmente identificáveis sobre um indivíduo coletadas online"* (COPPA, 2025). Entre alguns exemplos, estão inclusos: a) o primeiro e último nome; b) um endereço residencial ou outro endereço físico; c) informações de contato on-line, como e-mail e redes sociais; um número de telefone; d) imagens, vídeos, arquivos de áudio; e) um *cookie* ou qualquer outro tipo de identificador persistente que pode ser usado para reconhecer um usuário ao longo do tempo e em diferentes sites ou serviços on-line.

O **consentimento parental** é um princípio central na proteção de crianças no ambiente digital, reconhecendo o papel essencial dos pais e responsáveis na mediação do acesso e uso seguro de tecnologias. Envolver os pais na regulação do uso digital das crianças é crucial para promover ambientes online mais seguros e apropriados às suas necessidades e direitos (LIVINGSTONE; THIRD, 2017). Essa mediação, no entanto, enfrenta inúmeros desafios, como, por exemplo, a falta de transparência, que abordaremos mais adiante no tópico 3.1.

2.3 Ética em desenvolvimento de jogos

Os modelos de negócios em jogos digitais vêm-se adaptando ao longo do tempo, modificando, por consequência, seu relacionamento com sua base de usuários. Moreira et. al.(2014) destacam que o modelo *premium* foi, durante muito tempo, o modelo de negócio mais usual adotado pelos desenvolvedores de jogos, consistindo no requisito de compra antes do uso da aplicação.

O crescimento da concorrência, no entanto, forçou os desenvolvedores a recorrer a novas estratégias, como o modelo dos jogos *freemium*. O que, na prática, resulta de uma estratégia de monetização híbrida entre o *free* e o *premium,* onde o desenvolvedor fornece gratuitamente a aplicação e monetiza os usuários por recursos "premium" ou bens virtuais, posteriormente (MOREIRA *et.al*, 2014).

Esse modelo, por sua vez, pressupõe uma relação de longo prazo com os jogadores e os desenvolvedores devem estar prontos para atendê-la.

> Dados são criados desde o momento em que se inicia uma sessão de jogo virtual até o momento em que ela é desligada, e esses dados estão disponíveis para desenvolvedores e produtores analisarem seus jogadores. [...] os desenvolvedores usam esses dados para formar modelos estatísticos para ter uma melhor compreensão de seus jogadores e jogos. (ODIERNA, 2018).

O conceito de ***data-driven games***, isto é, jogos orientados por dados, refere-se à integração de grandes volumes de dados e inteligência artificial no processo de desenvolvimento e execução de jogos digitais. Essa abordagem permite a personalização da experiência do jogador, a adaptação dinâmica de cenários e a geração procedural de conteúdo, por meio de algoritmos que aprendem e se ajustam com base no comportamento dos usuários (TOGELIUS et. al., 2016; SMITH, 2014)

Existem inúmeros tipos de dados que podem ser coletados nos jogos digitais; bem como as finalidades e os interesses que envolvem seu uso são amplos (ALBUQUERQUE, 2016). O uso de dados, como recurso-chave, já vem sendo, há tempos, extensivamente, explorado na indústria e no desenvolvimento de estudos como criação de levels (CHIU et.al., 2008); aperfeiçoamento do *game design* (LANZI, 2013); classificação de jogadores com base em comportamento (ODIERNA et. al., 2018) e treinamento de modelos de inteligência.

Seif; Kleinman (2020) ressaltam que:

> (...) à medida que a indústria de jogos começa a sistematizar os processos de uso de dados em diversos aspectos do desenvolvimento, design e pesquisa de jogos, elas também enfrentarão questões e preocupações semelhantes em relação à privacidade, viés, injustiça e marginalização de grupos específicos de jogadores, o que pode gerar problemas de confiança ou desconfiança dentro da comunidade.

É de fundamental relevância compreendermos que o tratamento ético da privacidade dos dados deve ser integrado desde a fase de concepção de sistemas e tecnologias, e não como uma medida tardia. Essa perspectiva é fundamentada no conceito ***Privacy by Design***, formulado por Ann Cavoukian (Ph.D., ex-Comissária de Informação e Privacidade de Ontário - Canadá), em 1995, e formalizado em 2009:

> The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to

> materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after. (CAVOUKIAN, 2009).

Entre seus princípios, Cavoukian também defende o *privacy by default*, isto é, garantir a máxima proteção de dados pessoais em sistemas e práticas empresariais automaticamente, sem exigir qualquer ação do usuário. Isso significa que as finalidades de coleta devem ser comunicadas claramente e limitadas ao essencial.

Inspirados pelo *Privacy by Design* e alinhado à Convenção sobre os Direitos da Criança da ONU, Livingstone e Third (2023) introduziram o conceito de ***Children´s Rights by Design***, que propõe a integração proativa e prioritária dos direitos das crianças no desenvolvimento de produtos, serviços e ambientes digitais, garantindo sua proteção, privacidade e desenvolvimento saudável desde a fase de concepção. Em seu trabalho, apresentam-se 10 princípios, dentre eles destacamos:

a) Proteção de dados e privacidade: garantir privacidade por padrão, especialmente contra coleta excessiva de dados ou rastreamento.
b) Transparência e linguagem acessível: comunicação clara sobre termos de uso, políticas e riscos, adaptada à idade e compreensão da criança.
c) Segurança e proteção contra danos: prevenir exposição a conteúdos nocivos, aliciamento, cyberbullying e outros abusos *online*.
d) Minimização de riscos psicológicos: evitar mecânicas que induzam vício, ansiedade, manipulação ou comparação social excessiva.
e) Responsabilidade corporativa: empresas devem auditar os impactos de seus produtos e corrigir violações de direitos infantis.
f) Conformidade com marcos legais: alinhamento às leis como GDPR-K (Europa), COPPA (EUA) e às legislações locais.

Relativo ao princípio da minimização de riscos psicológicos, temos o conceito de ***dark patterns*** (ou padrões obscuros). Aplicado ao design de jogos, Zagal et. al (2013) define *dark pattern* como *"*(...) a pattern used intentionally by a game creator to cause negative experiences for players that are against their best interests and happen without their consent". Aprofundaremos este assunto no tópico 4.5 deste trabalho.

3. Problema de pesquisa

Quando falamos de proteção aos direitos da criança, muitos agentes e interesses estão envolvidos. Neste capítulo, abordaremos o problema de pesquisa sob a perspectiva de três diferentes partes interessadas: **os jovens jogadores e seus pais/responsáveis**, como titulares dos direitos a serem protegidos; **o Estado**, como protetor desses direitos e agente regulador; e por último, **os desenvolvedores de jogos**, como agentes econômicos e a de quem se exige o respeito à legislação e a adoção de condutas éticas.

3.1 Experiência de crianças e pais/responsáveis

As tecnologias de informação e comunicação (TICs), em sentido amplo, estão transformando a vida das crianças, criando novas oportunidades — mas também riscos — para seu bem-estar e seus direitos. Famílias, escolas e comunidades estão incorporando as tecnologias digitais como parte da infraestrutura natural da sociedade na era digital. Entre as oportunidades, destacam-se aprendizagem, lazer, saúde, comunicação e participação social. Por outro lado, os riscos à segurança, privacidade, saúde mental e desenvolvimento infantil são igualmente abrangentes (LIEVENS, 2018).

O aumento dos casos de violação de dados pessoais resulta da proteção insuficiente incorporada ao crescimento acelerado de tecnologias e serviços cujos modelos de negócios são baseados em coleta e análise de dados personalizados, que abrangem desde redes sociais a *wearables*. Nesse cenário, a privacidade infantil desponta como um recorte que traz questões ainda mais urgentes no círculo público e político (LIVINGSTONE, 2018).

A responsabilidade por garantir que crianças e adolescentes se comportem de forma segura e responsável no ambiente digital tem recaído, majoritariamente, sobre os pais. No entanto, muitos deles relatam sentir-se inseguros diante da complexidade crescente das tecnologias digitais (LIVINGSTONE et. al., 2017), além de enfrentarem dificuldades para acompanhar a rápida adoção de novos aplicativos e dispositivos cada vez mais individualizados e privados (LIEVENS, 2017).

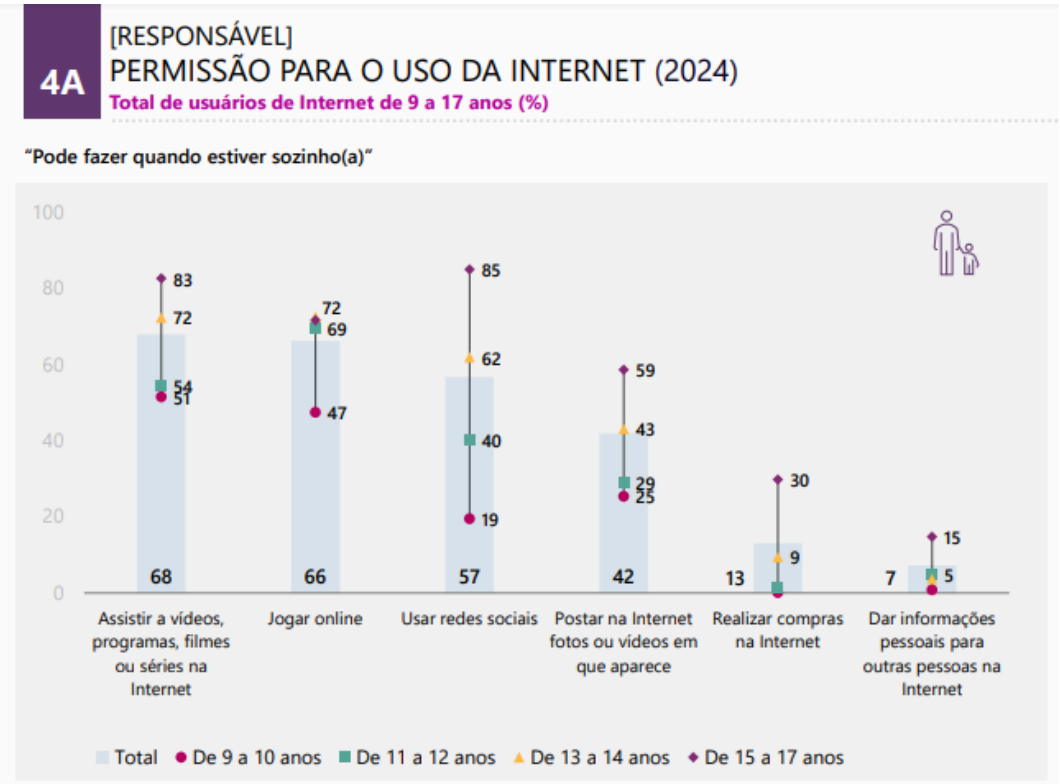
Três aspectos principais podem ser apontados para isso: primeiro, as crianças costumam ser pioneiras na adoção de novas tecnologias, dispositivos e conteúdos; segundo, com o entusiasmo natural que apresentam, as crianças têm menos senso crítico e compreensão dos riscos presentes e futuros para seu

bem-estar por meio do uso de ambientes digitais; e terceiro, considera-se que a existência de necessidades e direitos específicos do desenvolvimento infantil ainda são poucos reconhecidos e previstos pela concepção do ambiente digital e organizações comerciais (LIVINGSTONE et.al, 2018).

Segundo estimativas de 2024, 74% das crianças e jovens entre 3 a 18 anos, em 21 países, reportaram jogar videogames (The Insights Family Report, 2025). No Brasil, estima-se que - das crianças, entre 9 a 17 anos que têm acesso à internet - cerca de 78% a utilizam para acessar jogos *online* (CETIC, 2024).

A hiperconectividade e a independência das gerações mais recentes são características marcantes na rotina dessas atividades. No Gráfico 1, lista-se uma série de atividades que esses usuários possuem consentimento para realizarem sozinhos, sem supervisão do responsável. No geral, podemos dizer que 66% deles têm permissão para jogar online; especificamente, na faixa entre 15 a 17 anos, essa estimativa sobe para 72%.

Gráfico 1 - Atividades: Permissão do responsável para o uso da Internet.



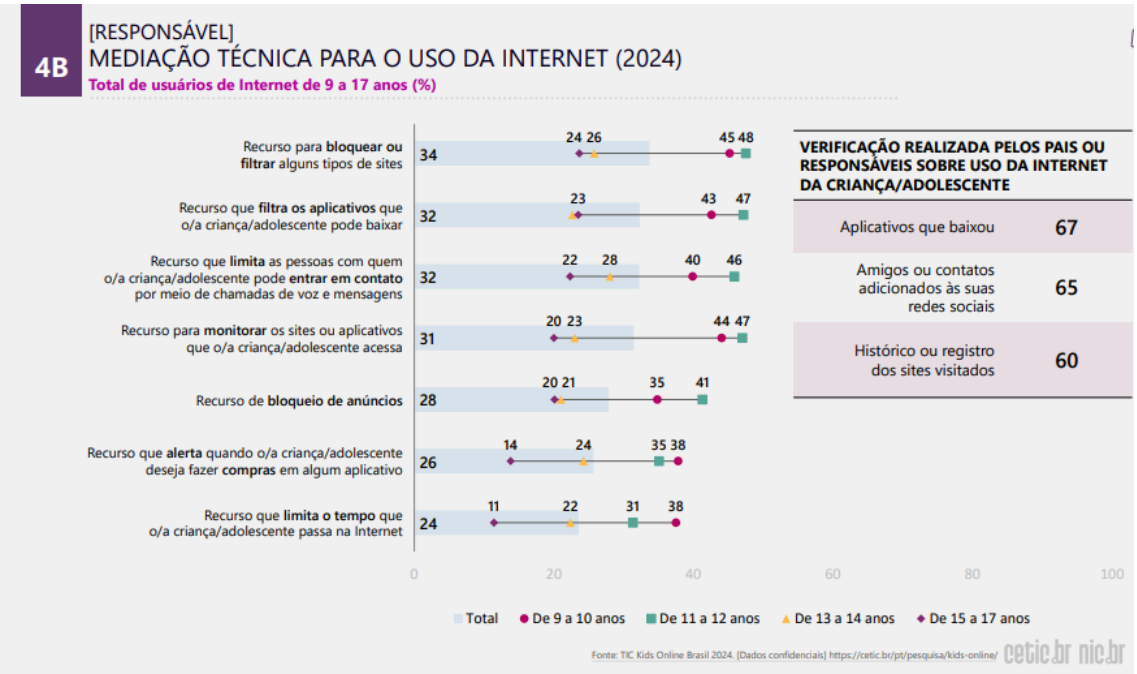
Fonte:CETIC, 2024

Uma consequência inevitável dessa independência em todas as atividades listadas no Gráfico 1 é a superexposição *online* desses jovens, bem como de seus

dados pessoais. Focaremos, neste trabalho, na exposição relativa ao contexto dos jogos online, acessados por meio de apps ou sites.

A supervisão por parte dos pais e responsáveis, nesse contexto, é uma prerrogativa indispensável para segurança desses jovens. Como podemos ver no Gráfico 2 a seguir, 60% a quase 70% dos pais e/ou responsáveis declaram fazer uma mediação técnica dos aplicativos baixados e contatos adicionados pelos filhos. Essa supervisão ainda pode ser considerada genérica e superficial, já que apenas 20% a 30% dos responsáveis afirmam utilizar ferramentas específicas, como filtros, monitoramento e bloqueios, para proteger os dados pessoais dos jovens nos aplicativos e sites que acessam. No entanto, entre crianças menores, esse percentual tende a ser maior. Mesmo assim, mal abrange 50% dos responsáveis.

Gráfico 2 - Mediação técnica do responsável para uso da Internet.



Fonte: CETIC,2024

Segundo um estudo publicado, em 2018, pela Universidade de Berkeley (EUA), dos quase 6.000 apps estudados que tinham crianças como público-alvo, 19% deles coletavam informações pessoais via SDKs, cujos termos de serviço proíbem totalmente o uso em aplicativos direcionados a crianças. Por fim, demonstra-se que os esforços do Google para limitar o rastreamento por meio do uso de um ID de publicidade tem pouco sucesso: dos 3.454 aplicativos que compartilham o ID com os anunciantes, 66% transmitem também outros

identificadores persistentes (REYES *et.al*, 2018). Acredita-se que, considerando jogos que alcançam públicos mistos de crianças e adultos, este percentual seja muito superior.

Nascimento e Fernandes (2021) destacam que a maioria dos responsáveis tende a aplicar medidas apenas restritivas, limitando tempo e conteúdo, mas sem promover discussões mais profundas sobre os usos da tecnologia.O acesso às tecnologias e o comportamento dos pais também variam de acordo com fatores como escolaridade, renda e grau de alfabetização digital dos próprios responsáveis.

Inúmeros estudos também alertam para outros riscos. Lemos e Silva (2018) criticam a forma como as descrições e interfaces lúdicas de apps infantis mascaram práticas de coleta de dados e publicidade, que os pais geralmente não percebem. Menezes e Albuquerque (2020) ressaltam que há um certo grau de ingenuidade por parte dos pais ao acreditar que aplicativos voltados ao público infantil são seguros por definição, principalmente, com base nas descrições nas lojas de aplicativos.

As políticas de privacidade, apresentadas pelos jogos, podem ser confusas para compreensão dos pais e responsáveis. O desacordo entre os termos sob os quais os dados são fornecidos e a finalidade incerta de seu uso resulta em problema ético no cenário das relações digitais. Além disso, muitas vezes, há uma disparidade entre o conteúdo real do e a classificação de conteúdo selecionada, com base nas descrições fornecidas pelos desenvolvedores (LICCARDI, 2014).

Em decorrência dos desafios enfrentados pelos pais e da superexposição virtual desses menores, existem os inúmeros riscos associados, entre eles: acesso a conteúdos nocivos que estimulam violência e automutilação, vazamento de imagens íntimas, cyberbullying, aliciamento sexual e contato com pessoas desconhecidas e perigosas (TEFFÉ, 2021). Agregados a isso, ainda há lacunas significativas na operacionalização de mecanismos eficazes que permitam a essas crianças ou seus representantes legais apresentarem reclamações de forma acessível e compreensível, especialmente no contexto digital (VAN DER HOF, 2020).

No Brasil, apesar da criação da Autoridade Nacional de Proteção de Dados (ANPD), como órgão responsável por fiscalizar e garantir o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD), grande parte da população ainda desconhece que pode registrar denúncias diretamente nesse canal. A falta de campanhas educativas amplas e acessíveis, contribui para que muitos pais,

responsáveis e jovens não saibam como agir diante de práticas abusivas envolvendo o tratamento de dados pessoais (WIMMER, 2021).

3.2 Experiência das instituições reguladoras

As legislações voltadas à proteção de dados infantis, como a COPPA e a GDPR-K, apresentam lacunas significativas e interpretações abertas que comprometem sua efetividade na prática. A COPPA, por exemplo, tem sido criticada por sua ênfase excessiva no consentimento parental, sem garantir mecanismos robustos de verificação, o que, segundo Solove (2012), acaba transferindo a responsabilidade para os pais, ignorando a complexidade dos ecossistemas digitais e das práticas comerciais envolvidas.

Já no contexto europeu, a GDPR-K introduz salvaguardas importantes, mas sua redação ambígua quanto à idade mínima para consentimento e à definição de "melhor interesse da criança" permite interpretações divergentes entre os Estados-membros, dificultando a harmonização da proteção. Como aponta Eva Lievens (2018), *"*a falta de orientação clara na GDPR-K gera incerteza jurídica e fragiliza sua aplicação uniforme na proteção dos dados de menores".

No contexto brasileiro, também observa-se que a lei exige o consentimento específico de um dos pais ou responsável legal para o tratamento de dados de menores de idade, mas não define claramente os critérios técnicos para validação desse consentimento, o que abre margem para interpretações divergentes e fragiliza a proteção desse grupo vulnerável. A LGPD adotou uma perspectiva focada em princípios gerais para tratar dados de crianças, sem estabelecer instrumentos normativos mais precisos, o que gera incerteza sobre como os agentes de tratamento devem proceder (BIONI, 2021).

Outro aspecto observado é o de que, frequentemente, há falta de transparência das descrições dos jogos e aplicativos sobre políticas de privacidade e recursos técnicos das empresas desenvolvedoras sobre suas funcionalidades técnicas, políticas de privacidade ou os mecanismos utilizados para coleta e tratamento de dados. A assimetria de informação é uma ferramenta poderosa nas mãos das plataformas digitais, que ocultam intencionalmente os detalhes operacionais para preservar vantagens comerciais (ARIEL EZRACHI, 2016).

A COPPA, por exemplo, determina que qualquer operador cujo site ou serviço seja reconhecidamente direcionado a crianças - intencionalmente ou não - e que

colete dados deve cumprir as normas estabelecidas. No entanto, diversos serviços e aplicativos acessíveis a crianças permanecem numa zona cinzenta, sem classificação clara como conteúdo infantil (SANDOVAL, 2024).

Esse tipo de ambiguidade técnica abre brechas que dificultam a fiscalização e a responsabilização das plataformas. Como observa Reidenberg et al. (2013), “a falta de mecanismos confiáveis para identificar usuários infantis e a ausência de requisitos técnicos claros na COPPA resultam em conformidades aparentes, mas não efetivas”. Assim, muitas empresas se beneficiam de interpretações ambíguas para evitar adaptações técnicas que garantiriam uma proteção mais robusta.

Sem classificação explícita, as plataformas podem coletar dados de crianças alegando desconhecer seu uso por esse público, evitando assim a obrigação de obter consentimento parental verificado (SANDOVAL, 2024).

Adicionado a isso, fiscalizar violações à proteção de dados infantis impõe altos custos ao Estado, exigindo estruturas complexas e constante vigilância, quando a conduta de proteção deveria ser incorporada desde o desenvolvimento das tecnologias, com uma postura ética e proativa por parte das empresas. Como ressalta Cavoukian (2009), a privacidade precisa estar embutida no sistema, não ser adicionada depois; destacando assim, a necessidade de prevenir riscos desde a origem, em vez de apenas reagir a danos já causados.

As leis de proteção de dados, especialmente para crianças, têm dificuldade em acompanhar o ritmo acelerado das inovações tecnológicas e das estratégias de coleta de dados do mercado digital. Como afirmam Livingstone e Third (2017), *“*as tecnologias digitais se desenvolvem mais rapidamente do que os marcos regulatórios podem responder, criando zonas cinzentas de risco para as crianças *online*”. Isso reforça a permanente necessidade de uma regulação mais dinâmica e atualizada.

Nesse cenário, compreendemos que o papel das instituições governamentais e dos instrumentos legais seja essencial na consolidação de princípios e diretrizes gerais que orientam o enfrentamento do problema e promovem a abertura ao diálogo. Consideramos que tais iniciativas, no entanto, ainda carecem de um nível de aprofundamento e detalhamento técnico para oferecer soluções mais efetivas capazes de sanar ou, ao menos minimizar, o problema em questão.

3.3 Experiência dos desenvolvedores de jogos

A falta de uniformidade e centralização nas legislações de proteção de dados pessoais, especialmente no que se refere a crianças, impõe desafios significativos aos desenvolvedores de softwares e jogos. A coexistência de diferentes marcos regulatórios no cenário internacional e nacional cria um cenário regulatório fragmentado, dificultando a criação de soluções padronizadas para a proteção infantil.

Por meio da aplicação de um *survey*, Ekambaranathan et. al (2021) investigaram os principais obstáculos enfrentados por desenvolvedores de aplicativos infantis para implementar práticas eficazes de proteção de dados.

Embora os desenvolvedores demonstrassem preocupações ética com o bem-estar infantil, relataram três barreiras centrais: (1) **dificuldade de acesso à bibliotecas de terceiros e a falta de transparência** sobre seus mecanismos de coleta de dados (por exemplo, SDK´s e API´s a serem integrados); (2) **pressão econômica para monetizar os apps**, geralmente via publicidade que envolve rastreadores de dados, dificultando alternativas éticas sustentáveis; e (3) **ausência de diretrizes técnicas claras e acessíveis** sobre design apropriado para crianças. Sobre o último aspecto, os autores destacam que:

> More than half indicated that they struggled to find suitable and specific design guidelines. Guidelines provided by the app marketplaces provide limited discussions on how to design for children's developmental needs. [...] Developers also indicated that following guidelines has not always been possible, as they constantly changed, and provided insufficient support for smaller companies or individual developers.(EKAMBARANATHAN et. al., 2021)

A proliferação de normas legais heterogêneas torna o cumprimento um "labirinto" regulatório. Isso exige que desenvolvedores adaptem constantemente seus produtos a critérios variados de consentimento, idade mínima e requisitos de transparência (VAN DER HOF; LIEVENS, 2018).

Além disso, a ausência de coordenação regulatória global aumenta os custos de conformidade e pode inibir a inovação responsável (STODDEN, 2014). Essa complexidade regulatória revela a necessidade urgente de esforços para harmonização de normas e diretrizes éticas mais claras e aplicáveis em escala global.

Outro obstáculo, enfrentado pelos desenvolvedores, é diretrizes operacionais específicas que orientem sua aplicação prática no desenvolvimento de software. Os marcos regulatórios estabelecem exigências amplas, como o dever de obter consentimento verificável ou adotar o *design* apropriado para crianças, mas, muitas vezes, deixam de fornecer instruções claras sobre sua implementação. A ausência de orientações técnicas detalhadas sobre privacidade infantil impede que os desenvolvedores consigam traduzir princípios jurídicos em funcionalidades técnicas robustas e coerentes (GURSOY et. al., 2021).

Os jogos, frequentemente - conforme já mencionado em tópicos anteriores, - dependem de coleta e análise de dados comportamentais para personalizar experiências, realizar monetização por meio de anúncios e prever tendências de consumo. As leis de proteção infantil limitam ou proíbem esse tipo de prática. Nair et. al. (2022) observaram que “o conflito entre proteção de dados e monetização orientada por análise de comportamento está no cerne dos dilemas enfrentados pelos desenvolvedores”.

O modelo de negócio de muitos jogos não são pensados, originalmente, para lidar com tantas exigências legais, decorrendo, não raramente, em um frequente “embate fiscalizatório” entre instituições e desenvolvedores. Esses últimos, muitas vezes, como forma de driblar e escapar da fiscalização e das medidas punitivas, têm descaracterizado seus jogos como conteúdo atrativo para crianças e atribuindo, exclusivamente, aos pais a responsabilidade desse uso (VALENTINO-DEVRIES et.al., 2018).

Tratando-se de jogos *mobile*, as políticas de privacidade de lojas de aplicativos têm-se tornado cada vez mais rigorosas. As lojas de aplicativos passaram a exigir que os todos os aplicativos - incluindo SDKs, APIs e anúncios - que comportem usuários menores de 13 anos - estejam em conformidade com a COPPA e a GDPR, (como por exemplo, no caso da Google Play e Apple Store). De uma perspectiva prática, a observância dessa condição resultou em uma série de desafios, mesmo para sites e aplicativos que têm adultos como público-alvo, mas que, porventura, ainda capturam interesse de crianças (LICCARDI et.al., 2014).

Adaptar-se às exigências da legislação representa custos e burocracia aos desenvolvedores. Assim, o rótulo de “direcionado a crianças” acaba criando um incentivo perverso: as empresas preferem alegar que seu conteúdo não é infantil para escapar da regulamentação (SANDOVAL, 2024).

Em resumo, os desenvolvedores se vêem inundados de informações e exigências, como pré-requisito, para que seu jogo possa ser considerado adequado ao seu público-alvo e cheguem ao mercado, recorrendo, muitas vezes, a estratégias ilegais ou questionáveis como forma de viabilizar seus projetos.

4. Estado da arte das forças regulatórias

Neste capítulo, apresentamos uma análise sobre o estado da arte relacionado ao problema investigado nesta pesquisa, destacando as principais abordagens teóricas e técnicas propostas para mitigação do problema e suas respectivas limitações. O objetivo é mapear os avanços já consolidados, identificando tanto as contribuições relevantes quanto as lacunas persistentes.

Desta forma, buscamos contextualizar a necessidade de novas soluções e fundamentar a contribuição deste trabalho. Estruturamos o tópico com base nos mecanismos reguladores (leis, normas, mercado e arquitetura “by design”), propostos por Lessig (LESSIG, 2006) e fundamentados no tópico 2.2.

4.1 Legislação

Abordaremos os principais instrumentos legais de alcance internacional que se consolidaram como referência na proteção de crianças e adolescentes em ambientes digitais, assim como os marcos legais pertinentes ao contexto jurídico brasileiro.

4.1.1 *Children’s Online Privacy Protection Act* (COPPA)

Sancionada nos EUA e regulamentada pela *Federal Trade Commission* (FTC), a *Children’s Online Privacy Protection Act* (COPPA) é considerada uma das legislações pioneiras na proteção da privacidade infantil online.

A legislação, que entrou em vigor em 2000 - sofrendo frequente revisões nos anos seguintes - estipula que websites, aplicativos e serviços online que coletem, direta ou indiretamente, informações de crianças menores de 13 anos devem obter, *a priori*, consentimento deliberado dos pais e/ou responsáveis (LICCARDI, 2014).

A COPPA é composta por duas partes principais: o texto legal original (15 U.S.C. §§ 6501–6506), que estabelece os princípios e definições gerais, e a COPPA Rule (16 CFR Part 312), elaborada pela FTC, que regulamenta detalhadamente sua aplicação. Entre os fundamentos de sua aplicação podemos destacar:

a) a obrigatoriedade de obtenção do **consentimento parental verificável** antes que qualquer dado pessoal seja coletado de uma criança. Esse consentimento deve ser obtido de forma clara e documentada, com

mecanismos que assegurem que o responsável legal foi devidamente informado e autorizou a prática (Art. 312.5);

b) a obrigação de transparência dos operadores, exigindo a **disponibilização de uma política de privacidade clara e acessível**, que informe, entre outros pontos, quais dados serão coletados, como serão utilizados, se serão compartilhados com terceiros e quais os direitos dos pais sobre essas informações (Art. 312.4);
c) a garantia aos pais o **direito de acessar, revisar e solicitar a exclusão dos dados pessoais** de seus filhos, bem como recusar futuras coletas. (Art. 312.6);
d) a garantia de segurança e integridade dos dados, determinando que os operadores implementem medidas razoáveis para **proteger as informações coletadas de acessos não autorizados ou usos indevidos**, inclusive por terceiros (Art. 312.10).

Embora a COPPA represente um marco indiscutível na abordagem da proteção de dados infantis, Sandoval (2024) destaca algumas problemáticas que comprometem sua efetividade, tais como: 1) plataformas acessadas por públicos mistos, frequentemente, evitam obrigações legais como o consentimento parental verificado, a menos que tenham “conhecimento real” do uso infantil; 2) a lei foca em mecanismos de verificação de idade, mas muitos são facilmente burlados por crianças; 3) muitos pais não compreendem totalmente os termos de uso, considerando-os longos, cansativos e difíceis de entender.

4.1.2 *General Data Protection Regulation* (GDPR)

Semelhante à legislação americana, na União Europeia (UE), a *General Data Protection Regulation* (GDPR) tornou-se aplicável em 2018, também exigindo consentimento parental e transparência no que diz respeito à coleta e uso de dados de menores, com a diferencial de que define a idade necessária para consentimento para menores 16 anos, mas permite que os estados membros, individualmente, possam reduzir a idade de consentimento para 13 anos (LIVINGSTONE et.al, 2018).

A GDPR é composta por duas grandes partes, a primeira contém 173 considerações, que explicam a motivação do regulamento e seus objetivos, e 99 artigos que discorrem sobre os direitos, deveres e princípios aplicáveis ao

tratamento de dados no espaço europeu. Os dispositivos da lei, focados especialmente nas crianças - comumente conhecido por GDPR-K - encontram-se no Artigo 8º (*Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação*).

Além deste, os Artigos 5º e 6º reforçam os princípios da limitação de finalidade, minimização de dados e licitude do tratamento, também aplicáveis ao contexto infantil.

Nenhuma justificativa específica, entretanto, foi apresentada pelo legislador europeu quanto à escolha da faixa etária entre 13 e 16 anos para o consentimento infantil. Além disso, persiste uma incerteza jurídica relevante: não está claro se a aplicação do artigo 8º do GDPR deve seguir a legislação do país de residência da criança ou do país em que o serviço está estabelecido (MIKAITE; LIEVENS, 2019).

Vale aqui frisar alguns diferenciais entre a legislação americana e a europeia. Enquanto a COPPA é orientada por obrigações específicas e contextos comerciais, a GDPR-K insere a criança como sujeito de direitos fundamentais, isso faz com que esta seja considerada, por alguns autores, um modelo mais centrado na criança, ainda que sua implementação prática dependa da harmonização entre os Estados-Membros e do enfrentamento de lacunas técnicas e conceituais (LIVINGSTONE et. al., 2019; LIEVENS et.al., 2018).

4.1.3 Artigo 14 da Lei Geral de Proteção de Dados (LGPD)

No Brasil, a Lei Geral de Proteção de Dados (LGPD), atualmente, é o principal instrumento legal sobre a privacidade e o tratamento de dados pessoais, tendo o Artigo 14º dedicado ao tratamento de dados de crianças e adolescentes, em conformidade com os direitos da crianças estabelecidos pela Constituição Federal, pelo Estatuto da Criança e do Adolescente (ECA) e pelas convenções internacionais.

No que se refere ao tratamento de dados pessoais de crianças e adolescentes, o consentimento (por parte de um dos pais ou responsável) é a única base legal para a qual a LGPD estabeleceu regras específicas de forma expressa, conforme o §1º do Art. 14. Considerando que o consentimento representa um instrumento central para a autodeterminação informativa e o controle dos dados (FERNANDES; MEDON, 2021). Menciona-se, inclusive, uma “hipertrofia do

consentimento” junto ao restante do corpo normativo de proteção de dados pessoais (BIONI, 2021):

> Em seu art. 5º, XII, a LGPD, define consentimento como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Todavia, esses três passos necessários para transformar a simples manifestação em um consentimento válido são, na atualidade, dificilmente verificados. (FERNANDES; MEDON, 2021).

Fernandes e Medon (2021) destacam lacunas interpretativas relevantes decorrentes do Art.14, que ainda exigem aprofundamento jurídico: 1) delimitação do regime normativo aplicável ao consentimento 2) discussão sobre quais outras bases legais seriam possíveis ou adequadas para legitimar o tratamento de dados desse público, já que o artigo restringe-se ao consentimento; 3) análise sobre o papel do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), como mecanismo de salvaguarda e prevenção de riscos à privacidade de crianças e adolescentes.

4.1.4 Projeto de lei nº 2628/2022

O Projeto de lei nº 2628/2022 - Proteção de crianças e adolescentes em ambientes digitais - em tramitação no Congresso Nacional, propõe a criação de um marco legal específico para a proteção de crianças e adolescentes em ambientes digitais. O projeto visa complementar a LGPD ao estabelecer diretrizes claras para plataformas digitais, aplicativos, jogos e demais serviços online que tenham como público-alvo (ou atraiam) pessoas menores de 18 anos.

O projeto determina que os desenvolvedores de produtos digitais devem assegurar que "as funcionalidades e os recursos tecnológicos ofertados estejam em conformidade com o desenvolvimento físico, emocional e cognitivo do público infantojuvenil" (Art. 6º, §1º).

Inspirado nas leis internacionais, como a COPPA e a GDPR-K, no projeto também consta a exigência de consentimento parental verificável, restrições à publicidade baseada em comportamento e o uso de design apropriado à idade como mecanismo central de proteção. O texto ainda obriga plataformas a disponibilizarem informações claras e acessíveis sobre o tratamento de dados pessoais e o funcionamento de algoritmos (Art. 7º).

O PL estabelece que os agentes digitais devem "adotar medidas técnicas e administrativas para mitigar riscos de danos aos direitos de crianças e adolescentes" (Art. 4º, inciso IV), o que exige investimentos em *compliance*, segurança e design ético. Além disso, o projeto determina que os responsáveis pelos serviços deverão elaborar relatórios de impacto de proteção de dados pessoais infantojuvenis (Art. 10º).

Apesar de representar um avanço relevante no cenário brasileiro, tais exigências presentes neste projeto, bem como nos demais instrumentos legais mencionados anteriormente, impõem desafios técnicos e operacionais significativos, sobretudo para empresas de pequeno porte ou desenvolvedores independentes.

4.2 Normas e políticas de mercado

As normas, como mencionado no tópico 2.2, representam regras que, mesmo sem caráter legal, orientam comportamentos na esfera social. Agentes de mercado e entidades delegadas do poder público, frequentemente, são os responsáveis por formular diretrizes e regras técnicas para estabelecer padrões de conduta.

4.2.1 *Players* distribuidores

Impulsionados pelas exigências legais, os principais *players* do mercado de jogos vêm assumindo um papel cada vez mais ativo na criação de diretrizes específicas voltadas à elegibilidade, design e avaliação de jogos destinados ao público infantil ou que possam atrair esse público.

Tanto o Google quanto a Apple disponibilizam frameworks que vão além das exigências legais, como a COPPA (*Children's Online Privacy Protection Act*), oferecendo recomendações sobre design de interface, coleta de dados, monetização responsável e conteúdos apropriados à faixa etária. Por exemplo, o programa *Building for Kids* da Google Play define critérios específicos para que um app seja considerado seguro e educativo para crianças. Já a Apple possui políticas similares em suas diretrizes da App Store, especialmente relacionadas a aplicativos na categoria infantil.

Entre os principais focos do programas da Google Play estão: 1) garantir que os desenvolvedores não coletem dados pessoais de crianças sem consentimento verificável dos pais; 2) assegurar que o conteúdo do app ou jogo deve ser adequado à faixa etária indicada, sem linguagem imprópria, violência, ou publicidade

enganosa; 3) garantir que apenas redes de anúncios certificadas para o público infantil sejam utilizadas; 4) promover uma navegação simples e clara, sem o uso de *dark patterns*, especialmente em se tratando de compras dentro dos aplicativos (Google Play Families, 2025).

Esses programas ensinam práticas valiosas para os desenvolvedores, tais como: adaptar conteúdos ao estágio de desenvolvimento cognitivo das crianças; limitar interações sociais que envolvam riscos; e informar de maneira clara sobre publicidade e compras dentro do app.

Essas orientações, contudo, ainda se encontram dispersas em diferentes domínios. A ausência de um referencial unificado leva à duplicação de esforços por parte de desenvolvedores que atuam em diferentes plataformas e à confusão sobre como atender consistentemente às expectativas de cada loja digital. O cenário *mobile* depende de uma combinação entre políticas da plataforma, regulamentação estatal e responsabilidade do desenvolvedor – mas a ausência de padronização torna a aplicação dessas práticas mais difícil (TAKAHASHI, 2021).

Além das plataformas móveis, o mercado de jogos para PC e console também vem incorporando diretrizes e políticas de responsabilidade voltadas à proteção infantil. Plataformas como Steam, Epic Games Store e Microsoft passaram a adotar medidas que buscam garantir experiências seguras e apropriadas para crianças e adolescentes. Contudo, essas iniciativas variam amplamente em escopo e rigor, dependendo da empresa e do país de operação.

Por exemplo, a Microsoft, por meio do *Xbox Family Settings* e da loja de aplicativos do Windows, permite que os pais gerencie o tempo de tela, as configurações de privacidade, as interações sociais, o acesso a conteúdo adulto e habilite o monitoramento com configurações familiares exclusivas (Xbox.com, 2025).

A Epic Games, por sua vez, tem investido em funções de controle parental e políticas de privacidade, especialmente após as sanções recebidas por violações relacionadas à coleta de dados de menores, mencionados na introdução deste trabalho. “A ferramenta de controle parental permite o gerenciamento das interações sociais on-line da criança nas experiências e jogos da Epic, definindo permissões para solicitações de amizade, bate-papo por voz e texto e filtragem de linguagem adulta. Os pais são incentivados a analisar também as configurações sociais em nível de plataforma.” (Epic Games Safety and Security Center, 2025).

A dispersão das informações, entretanto, em diferentes domínios e linguagens técnicas dificulta o acesso de desenvolvedores independentes a práticas padronizadas de design ético e proteção de dados. A multiplicidade de *frameworks* entre plataformas digitais dificulta uma proteção eficaz e consistente de crianças em ambientes digitais complexos. (Livingstone et al.,2022).

Portanto, embora iniciativas importantes estejam em curso nos principais canais de distribuição, a dispersão de informações e a carência de manuais práticos dificultam o engajamento efetivo do setor de desenvolvimento com as obrigações éticas e legais voltadas à infância.

4.2.2 Entidades normativas

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão público responsável por fiscalizar, orientar e zelar pela aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Criada pela Lei nº 13.853/2019, a ANPD tem como missão assegurar a proteção de dados pessoais e promover uma cultura de privacidade no país.

Sua atuação inclui editar regulamentos, fiscalizar condutas, aplicar sanções e conscientizar a sociedade sobre boas práticas no tratamento de dados. Além disso, a ANPD é encarregada de avaliar impactos à proteção de dados em tecnologias emergentes, mediar conflitos entre titulares e controladores de dados, e cooperar com outras autoridades nacionais e internacionais (Bezerra, 2019).

No contexto da proteção de dados de crianças e adolescentes, a ANPD tem papel central na regulamentação e fiscalização do Artigo 14 da LGPD, que estabelece que o tratamento de dados de menores deve sempre respeitar o “princípio do melhor interesse”.

Em decorrência de intenso debate e cobranças advindos de diversos setores da sociedade civil quanto à correta interpretação das bases legais que legitimam o tratamento de dados de crianças, a ANPD publicou o Enunciado CD/ANPD nº 1, maio de 2023, pretendendo uniformizar a interpretação da LGPD quanto às hipóteses legais que autorizam o tratamento de dados de crianças e adolescentes. (ANPD, 2024).

Similar às atribuições da ANPD, temos a da *Federal Trade Comission* (FTC), principal órgão responsável pela aplicação e fiscalização da COPPA, nos EUA. Suas atribuições incluem fiscalizar empresas que coletam, armazenam ou compartilham

dados de crianças, avaliar se há consentimento parental verificável, e aplicar sanções administrativas e financeiras em casos de descumprimento. Além disso, a FTC é responsável por emitir diretrizes técnicas, validar métodos de consentimento, e supervisionar programas de autorregulação (*safe harbor*), como o kidSAFE e PRIVO (FTC, 2022).

Na Europa, cada país tem relativa autonomia para aplicação da GDPR, tendo a entidade centralizadora a *European Data Protection Board* (EDPB). Suas atribuições incluem emitir diretrizes interpretativas, facilitar a cooperação entre autoridades nacionais de proteção de dados e resolver disputas transfronteiriças (EDPB, 2024).

O *UK Information Commissioner's Office* (ICO) é uma autoridade europeia independente, responsável por proteger e garantir os direitos relacionados à informação no interesse público, além de promover a privacidade de dados dos indivíduos.Com o objetivo de lidar com as preocupações sobre a privacidade das crianças no ambiente digital, o ICO lançou o *Age Appropriate Design Code* (AADC).

Esse código busca garantir que os serviços online protejam os dados pessoais de crianças e estejam em conformidade com o Regulamento Geral de Proteção de Dados (GDPR).A partir de setembro de 2021, os serviços que não estiverem em conformidade poderão ser alvo de notificações formais e multas de até 4% do faturamento global da empresa, caso violem as diretrizes de proteção de dados (EKAMBARANATHAN, 2021).

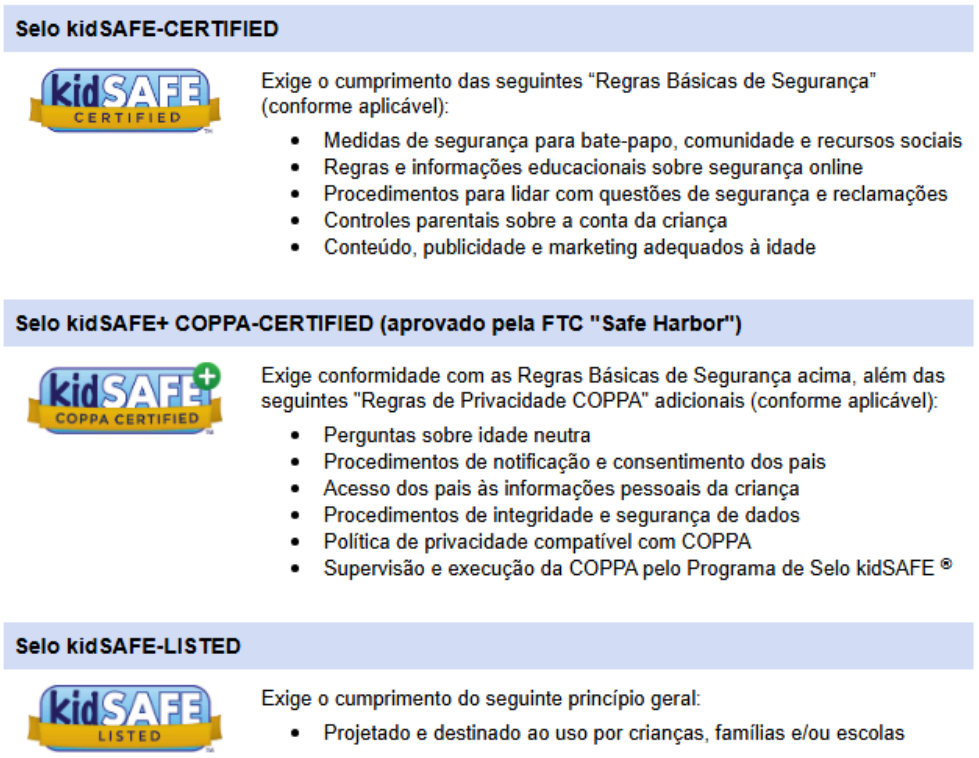
4.2.3 Programas de certificação

Exibir selos de certificação de padrões de segurança em um site ou aplicativo, voltado ao público infantil, sinaliza que o produto segue padrões rigorosos de segurança e privacidade, aumentando sua credibilidade junto à sociedade, demonstrando conformidade com legislações, além de diferenciar o produto no mercado.

O "Programa de Selo kidSAFE" - criado por Shai Samet, um consultor experiente e premiado em privacidade infantil - é um serviço independente de certificação de segurança e selo de aprovação criado, exclusivamente, para sites e tecnologias voltadas ao público infantil. Ele abrange plataformas como sites de jogos online, serviços educacionais, mundos virtuais, redes sociais, aplicativos móveis, dispositivos como tablets, brinquedos conectados e outros serviços digitais e

interativos similares (kidSAFE, 2024). Cada categoria de selo exige conformidade a uma série de regras específicas, conforme mostrado na Figura 1.

Figura 1 - Categorização de selos kidSafe.



Fonte: kidSAFE, 2024

Outro programa relevante a ser citado é o PRIVO (Privacy Vaults Online). Ele oferece programas de certificação e conformidade que ajudam seus membros a atender à conformidade de privacidade da COPPA e do GDPR, no que se refere a crianças e aos regulamentos de Privacidade Digital de Estudantes dos EUA (PRIVO, 2024). Assim como o kidSAFE, o PRIVO também possui categorias específicas de certificação.

4.2.4 Ferramentas e plataformas *compliance*

Atualmente, diversas ferramentas e plataformas têm sido desenvolvidas com o objetivo de auxiliar empresas no cumprimento das exigências legais de proteção de dados de crianças, oferecendo soluções que prometem um selo de conformidade com marcos como a COPPA e a GDPR-K.

Entre essas soluções, destaca-se a plataforma *Kids Web Services* (KWS), da empresa *SuperAwesome*, que fornece uma infraestrutura projetada para facilitar a

implementação do consentimento parental verificável, gerenciamento de contas infantis e controle de publicidade segura. Essas ferramentas têm sido amplamente adotadas por desenvolvedores de jogos e aplicativos infantis como uma forma prática de alinhar seus produtos às exigências legais, reduzindo riscos regulatórios e promovendo confiança junto ao público e às autoridades.

Apesar de representarem avanços importantes, essas soluções ainda são limitadas em seu escopo. Grande parte das funcionalidades oferecidas concentra-se quase exclusivamente na coleta e gestão do consentimento parental, sem necessariamente abordar outros aspectos críticos da privacidade infantil, como o design adequado à idade, restrição à monetização ou fiscalização de *dark patterns*. Como observa Livingstone et al. (2021), a conformidade formal com as exigências legais não garante, por si só, uma experiência digital verdadeiramente segura e ética para as crianças.

4.3 Educação e capacitação

A capacitação de profissionais que atuam no desenvolvimento de produtos digitais, especialmente voltados ao público infantil, é essencial para garantir a proteção de dados e o respeito à privacidade desde as etapas iniciais do design.

É fundamental que essas iniciativas educativas possam ir além do âmbito das interpretação normativa, envolvendo também uma abordagem prática e interdisciplinar que torne os princípios de proteção de dados aplicáveis ao cotidiano dos profissionais (Mantelero, 2014). Percebemos, no entanto, que essas formações costumam ser conduzidas majoritariamente por profissionais do Direito, que tendem a abordar o tema sob uma perspectiva, muitas vezes, ainda abstrata para os desenvolvedores, resistentes ao “juridiquês” padrão.

Programas internacionais como o *KidAware*, desenvolvido pela Super Awesome, um treinamento focado na capacitação de profissionais sobre conformidade, regulamentações e padrões da indústria no universo digital infantil, como COPPA e GDPR-K. No entanto, esses treinamentos ainda são pouco acessíveis - possuindo um processo relativamente burocrático para submissão - além de não abrangerem legislações como a LGPD, por exemplo, não estando disponíveis em português, o que limita sua aplicação ao Brasil.

4.4 *Dark patterns* em jogos digitais

Neste tópico, trataremos sobre o conceito de dark patterns como uma manifestação da força regulatória *arquitetura*, conforme proposto por Lessig (tópico 2.2). Nesse sentido, ao falarmos em *dark patterns*, estamos nos referindo à maneira como o design intencional de interfaces e funcionalidades pode influenciar, manipular ou restringir escolhas dos usuários, neste caso de forma antiética.

Esta discussão dialoga, diretamente, com o conceito de *privacy by design*, formulada por Ann Cavoukian e tratado no tópico 2.3. De forma similar, acreditamos que a ética no design de jogos digitais deve ser pensada desde a concepção do projeto, buscando não apenas conformidade legal, mas também a promoção ativa do bem-estar dos usuários (*ethics by design*).

4.4.1 Conceito

O conceito de *dark patterns* (ou *deceptive patterns)* surgiu em 2010, desenvolvido por Harry Brignull, para descrever interfaces e elementos de design digital criados intencionalmente para manipular o comportamento dos usuários de forma enganosa ou coercitiva, muitas vezes levando-os a tomar decisões contrárias aos seus interesses.

Ao contrário de boas práticas de design, que prezam pela clareza, acessibilidade e transparência, os *dark patterns* operam de maneira dissimulada, explorando vulnerabilidades cognitivas e psicológicas. Brignull (2010) define-os como *“tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something”.*

Arunesh et. al. (2021) sintetizam os atributos característicos de um *dark pattern*, agrupados sob critério do seu impacto na escolha do usuário (ver Tabela 1).

Tabela 1 - Atributos dos *dark pattern*.

Choice Architecture	Attribute	Description
Modifying the decision space	Asymmetric	Unequal burdens on choices available to the user
	Restrictive	Eliminate certain choices that should be available to users
	Disparate Treatment	Disadvantage and treat one group of users differently from another
	Covert	Hiding the influence mechanism from users
Manipulation the information flow	Deceptive	Induce false beliefs in users either through affirmative mis-statements, misleading statements, or omissions
	Information Hiding	Obscure or delay the presentation of necessary information to users

Fonte: Arunesh et. al., 2021.

Dark patterns que são assimétricos, encobertos, restritivos ou que envolvem tratamento desigual buscam influenciar as decisões dos usuários modificando o conjunto de opções disponíveis. Já os *dark patterns* baseados em induções enganosas ou ocultação de informações atuam manipulando as informações que são apresentadas ao usuário. Em última instância, ambos os tipos revelam como esses padrões escuros interferem na arquitetura de escolha, alterando a forma como os usuários percebem e tomam decisões dentro de uma interface (Arunesh et. al., 2021).

4.4.2 Taxonomia

Zagal et. al (2013) aprofundam o estudo sobre *dark patterns*, originalmente formulado por Brignull, no contexto da experiência dos usuários de jogos digitais, formalizando o conceito de *dark game design pattern*, mencionado no tópico 2.3, e propondo uma taxonomia específica de padrões manipulativos, em três principais categorias:

a) **Temporal:** são padrões que exploram o tempo do jogador como recurso. *“Jogadores são incentivados a gastar tempo excessivo em tarefas repetitivas ou a retornar com frequência ao jogo sob pena de perder o progresso."* (Zagal et. al., 2013)
b) **Monetário:** o propósito desses padrões consiste em monetizar, ao máximo, a experiência do jogador. O design incentiva compras contínuas, muitas vezes

por meio de microtransações mal sinalizadas, loot boxes ou acesso bloqueado por *paywalls*;

c) ***Social-Capital Based*****:** são padrões que exploram o capital social do jogador, ou seja, suas conexões, status ou pressão de grupo. O jogo incentiva a realização de ações que beneficiam o desenvolvedor, como convidar amigos, postar nas redes sociais ou gastar para “não prejudicar” o time.

Pertinente a cada categoria, Zagal et.al. (2013) categoriza e detalha tipos específicos de padrões obscuros, conforme a Tabela 2.

Tabela 2 - Taxonomia *dark pattern* proposta por Zagal et. al.

Category	Type	Description
1.Temporal	1.1 Grinding	Performing repetitive and tedious tasks in order to make progress in a game. Focusing on time spend in game instead player performance.
	1.2 Playing by Appointment	Require that players play at specific times (and or dates) as defined by the game.
2.Monetary	2.1 Pay to Skip	Pay to progress or skip hard level
	2.2 Pre-Delivered Content	When certain game content or functionality is provided in the purchase of a game, but is unavailable until the player pays an additional fee.
	2.3 Monetized Rivalries/Pay to Win	Exploring player competitiveness; encouraging them to spend money to achieve in-game status such as a high placement on a leaderboard. When players are encouraged to spend money purchasing enhancements in games that presumably have a level playing field.
3.Social-Capital Based	3.1 Social Pyramid Schemes	Similar to multilevel marketing, many games encourage players to invite their friends to participate. The combination of rewards and need for progression result in what we call social pyramid scheme.
	3.2 Impersonation/Friend Spam	When the game impersonates other players by communicating actions they never performed, thus misleading the player about the activities of their friends in the game.
4. Others	4.1 Encoraging Anti-social Behaviour	When games require that players have a behaviour considered unethical outside of a game’s context.
	4.2 Psycological Tricks	Applying insights and results from psychology and behavioral economics to games; explore sticky or irrational behaviors.

Fonte: Elaboração da autora

Partindo da tipologia original de Brignull (2010), Gray et al (2018) em seu estudo elenca um rol de padrões obscuros com base em exemplos compartilhados por profissionais de UX. A partir da sua análise, formatou uma taxonomia de *dark patterns* em cinco categorias principais. Construímos uma tabela resumo para facilitar a identificação dos padrões (Tabela 3).

Tabela 3 - Taxonomia *dark pattern* proposta por Gray et. al.

Category	Category Description	Type	Type Description
1. Nagging	Redirection of expected functionality that persists beyond one or more interactions.	***	***
2. Obstruction	Making a process more difficult than it needs to be, with the intent of dissuading certain action(s).	2.1 Roach Motel	Describes a situation that is easy to get into, but difficult to get out of. This usually occurs when a user signs up for a service easily, but closing or cancelling is difficult or impossible.
		2.2 Comparision prevention	Seeks to dumped the effect of market competition by making direct price comparisons between products and services.
		2.3 Intermediate Currency	Spend real money to purchase a virtual currency which is then spent on a good or service. The goal of this pattern is to disconnect users from the real dollar value spent in order to cause the user to interact differently with the virtual currency.
3. Sneaking	Attempting to hide, disguise, or delay the divulging of information that is relevant to the user.	3.1 Forced Continuity	Continue to charge the user after the service they have purchased expires.
		3.2 Hidden Costs	Provide users with a late disclosure of certain costs.
		3.3 Sneak into Basket	Add itens not chosen by the user to their online shopping cart, often claiming to be a suggestion based on other purchased items.
		3.4 Bait and Switch	Make it apparent that a certain action will cause a certain result, only to have it cause a different, likely undesired result.
4. Interface interference	Manipulation of the user interface that privileges	4.1 Hidden Information	Options or actions relevant to the user but not made immediately or

	certain actions over others.		readily accessible.
		4.2 Preselection	A situation where an option is selected by default prior to user interaction.
		4.3 Aesthetic Manipulation/Misdirection	A manipulation of the user interface that deals more directly with form than function. This includes design choices that focus the user's attention on one thing to distract them from or convince them of something else.
		4.4 Toying with emotions	Includes any use of language, style, color or other similar elements to evoke an emotion in order to persuade the user into a particular action.
		4.5 False Hierachy	Give one or more options visual or interactive precedence over others, particularly where items should be in parallel rather than hierarchical. This convinces the user to make a selection that they feel is either the only option or the best option.
		4.6 Disguised Ad	Include ads disguised as interactive games, or ads disguised as a download button or other interesting interaction.
		4.7 Trick Question	Includes a question that appears to be one thing but is actually another, or uses confusing wording, double negatives, or otherwise leading language to manipulate user interactions.
5. Forced Action	Requiring the user to perform a certain action to access (or continue to access) certain Functionality.	5.1 Social Pyramid	Requires users to recrute others users to use the service.
		5.2 Privacy Zuckering	Tricks users into sharing more information about themselves than they intend to or would agree to.
		5.3 Gamefication	Certain aspects of service can only be "earned" through repeated actions or frenquently service use.

Fonte: Elaboração da autora

Revisitando as categorias propostas por Zagal et. al (2013) e aquelas propostas por Gray et al. (2018), Fitton e Read (2019) desenvolveram uma classificação ainda mais abrangente de categorização para os possíveis *dark patterns* presentes em aplicativos *freemium* voltados para crianças, conforme a Tabela 4.

Tabela 4 - Taxonomia *dark pattern* proposta por Fitton e Read.

Category	Type	Description
1.Temporal	1.1 Grinding	Performing repetitive and tedious tasks in order to make progress in a game. Focusing on time spend in game instead player performance.
	1.2 Play by Appointment	Require that players play at specific times (and or dates) as defined by the game.
	1.3 Interstitial non-app content	Ads appears between levels which are difficult to dismiss due to inconsistent dismiss button locations
2. Monetary	2.1 Pay for Permanent Enhancements	The user is encouraged to purchase additional in-game items which were not essential but potentially enhanced the playing experience
	2.2 Pay for Expendable Updates	
	2.3 Pay to Skip/Progress	Pay to progress or skip hard level
	2.4 Pay to Win	Players are encouraged to spend money purchasing enhancements in games that presumably have a level playing field.
	2.5 Subscriptions	
	2.6 Intermediate Currencies	Spend real money to purchase a virtual currency which is then spent on a good or service. The goal of this pattern is to disconnect users from the real dollar value spent in order to cause the user to interact differently with the virtual currency.
3. Social	3.1 Impersonation / Friend Spam	When the game impersonates other players by communicating actions they never performed, thus misleading the player about the activities of their friends in the game.
	3.2 Prompts to Share	Design features that ask, encourage, or reward players for sharing content or inviting friends. They often do this without clearly explaining the consequences or giving an easy way to say no without missing out
	3.3 Social Pyramid Schemes	Requires users to recruit others users to use the service.
4. Disguised Ads	4.1 Advergames	Refers to the use of well-known branded characters or mascots within a game environment in a way that blurs the line between entertainment and advertisement
	4.2 Characters Placement	

5. Sneaky Ads	5.1 Difficult/Deceptive to Dismiss	The design makes it very easy for you to get into a certain situation, but then makes it hard for you to get out of it (e.g. a subscription).
	5.2 Camouflaged Game Items	Refer to in-game elements that function as advertisements but are presented as regular game content, such as rewards, power-ups, or collectible items
	5.3 Notification-based Ads	Promotional messages delivered through system notifications or in-app alerts, often appearing similar to standard game notifications.
6.Innapropriate	6.1 Unsuitable Adverts	Inappropriate ads (format and content) for an age group.
	6.2 Encouraging Anti-social behavior	When games require that players have a behaviour considered unethical outside of a game's context.
	6.3 Psycological Manipulation	Applying insights and results from psychology and behavioral economics to games; explore sticky or irrational behaviors.
	6.4 Persuasive Design	Aesthetic manipulation or misdirection
	6.5 Developmentally Insensitive	When the designer includes elements in their apps which may have a negative effect on users due to their psychosocial development.

Fonte: Elaboração da autora

A principal distinção da taxonomia proposta por Fitton e Read (2018), em relação às classificações elaboradas por Zagal et al. (2013) e Gray et al. (2018), está na distinção de categoria denominada "Inappropriate". Essa categoria abrange padrões obscuros que exploram elementos de design inadequados para a faixa etária dos usuários, explorando as vulnerabilidades cognitivas, emocionais ou sociais.

4.4.3 Implicações de uso

O uso de *dark patterns* é especialmente preocupante em ambientes voltados ao público infantil, como jogos e aplicativos, onde a capacidade de discernimento e julgamento está em desenvolvimento.

Quando pesquisadores argumentam que um *dark pattern* contraria os "melhores interesses" do usuário, o "prejudica" ou cria uma "experiência negativa" de uso, eles estão, na verdade, concentrando-se em aspectos relacionados ao bem-estar individual (Arunesh et. al., 2021). Por analogia, concluímos que a adoção de *dark patterns* em produtos digitais, dirigidos ao público mais jovem, encontra-se em contradição ao "princípio do melhor interesse da criança".

Em jogos digitais, esses padrões podem assumir diversas formas: desde manipulações para aumentar o tempo de uso, como notificações constantes e recompensas intermitentes, até estratégias que induzem compras *in-app* por meio de botões chamativos ou ambíguos.

El-Nasr & Kleinman (2020) descrevem como o uso de dados podem se converter em práticas predatórias em diferentes contextos da operação de jogos:

a) **Relativo à retenção:** utilizando métricas como tempo de sessão e frequência de retorno, os desenvolvedores ajustam algoritmos e mecânicas de jogo para manter os usuários engajados o máximo possível. Embora esses dados ajudem a entender padrões de comportamento, eles também podem ser usados para criar estratégias de retenção excessivas, que exploram vulnerabilidades cognitivas e incentivam hábitos compulsivos, especialmente em públicos mais jovens;
b) **Relativo à monetização:** o uso de dados comportamentais permite aos desenvolvedores otimizar estratégias para induzir gastos, muitas vezes sem considerar o bem-estar financeiro ou emocional dos jogadores. Estudos apontam que essas práticas podem gerar ciclos predatórios, penalizando quem não consome e favorecendo perfis mais lucrativos. Além disso, recursos são usados para manipular escolhas e estimular compras por meio de gatilhos emocionais, o que levanta sérias questões sobre transparência e ética no design de jogos;
c) **Relativo à modelagem/personalização:** os desafios de adaptar modelos às diferenças individuais dos jogadores ampliam o debate de aplicar conceitos éticos na implementação de, por exemplo, sistemas de recomendação, balanceamento e previsão de evasão (*churn*). Embora a personalização tenha o potencial de melhorar a experiência do usuário, ela também pode reforçar vieses algorítmicos, limitar a diversidade de conteúdos acessados e afetar negativamente grupos sub-representados, como jogadores casuais, novatos ou pertencentes a minorias. Os modelos preditivos utilizados para ajustar desafios, narrativas e recompensas são, muitas vezes, opacos e não levam em conta a diversidade de estilos de jogo, o que pode comprometer a justiça e a inclusão no design de jogos digitais.

A prática de recompensar os jogadores de forma aleatória - comumente através de *loot boxes* – por exemplo, demanda preocupações éticas, uma vez que o jogador não tem ciência da probabilidade de obtenção dos prêmios. Trazendo elementos dos jogos de azar, nessa condição, torna-se praticamente impossível avaliar se o investimento financeiro vale a pena, comprometendo sua capacidade de decisão consciente e informada (Neely, 2019).

Neely (2019) também analisa distinções relativas ao design de itens disponíveis nos jogos. Itens cosméticos de valor fixo são considerados menos problemáticos, pois não impõem desvantagens ao jogador. Por exemplo, um jogador pode jogar *League of Legends* tão bem com a aparência padrão de um personagem quanto com uma aparência sofisticada; a compra com dinheiro real é apenas um extra divertido para os jogadores. Já a disponibilidade de itens funcionais, por meio de compra, “levanta preocupações quanto à transformação do jogo em um modelo *pay to win*, no qual o progresso do jogador deixa de depender de habilidade ou esforço, e passa a ser determinado pela quantia de dinheiro investida” (Neely, 2019).

A presença de *dark patterns* no design de jogos infantis levanta sérias questões éticas e legais, principalmente quando aliados a práticas de coleta de dados. Crianças, mais suscetíveis à persuasão visual e emocional, tornam-se alvos fáceis de mecanismos que forçam interações, diluem o consentimento informado e encorajam gastos sem plena consciência.

Um jogo que adota um design ético deve, entre outros aspectos, incentivar os jogadores a avaliarem seus próprios valores morais, o contexto das questões abordadas, bem como a considerarem as possíveis consequências de diferentes ações (Zagal, 2011). Nesse sentido, podemos concluir que um jogo com design ético é aquele que privilegia a autonomia decisória dos seus jogadores.

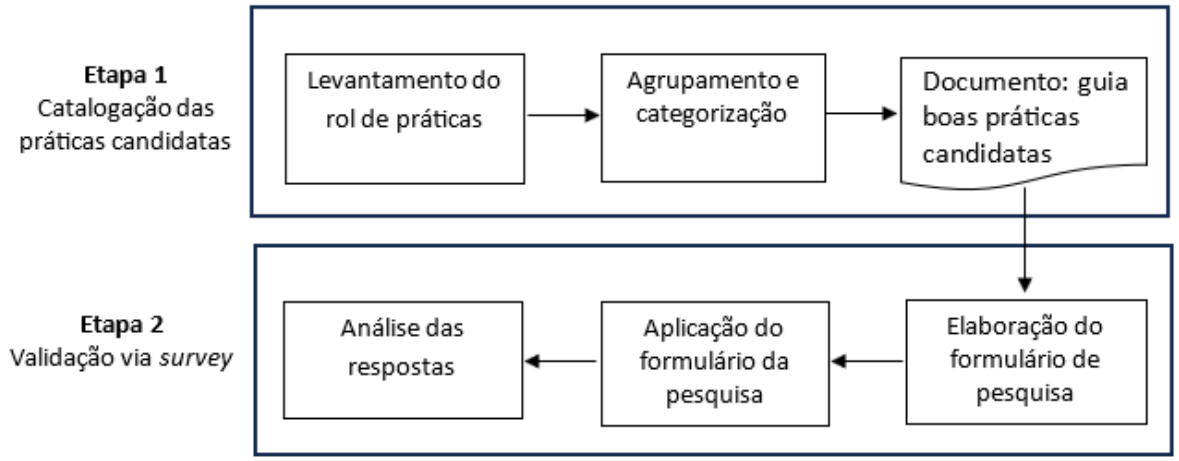
5. Etapa 1: Catalogação de candidatos via estudos e documentos

Antes de abordamos detalhadamente a primeira etapa, apresentaremos a seguir uma visão geral de todas as etapas metodológicas (Figura 2) através das quais esta pesquisa foi desenvolvida; sendo elas duas principais:

1) a catalogação de potenciais boas práticas, com base na revisão da literatura e da legislação;

2) a realização de um *survey*, junto aos profissionais do mercado de jogos, para validação da relevância e aceitação como boas práticas a se adotar.

Figura 2 - Fluxograma geral de etapas metodológicas



Fonte: Elaboração da autora

Na etapa 1, temos as seguintes subetapas: levantamento do rol de práticas; agrupamentos e categorização que resultaram no documento guia de boas práticas candidatas. A partir desse documento, na etapa 2, elaboramos o formulário de pesquisa (survey) para a coleta dos dados quantitativos. Após a aplicação do formulário, realizamos a análise dos resultados para inferir e analisar as práticas candidatas levantadas.

5.1 Método

O método de Revisão da literatura é um processo essencial para avaliar o que já foi produzido sobre o tema em questão, permitindo situar a pesquisa proposta no contexto do conhecimento existente e identificar a sua possível contribuição para a compreensão do objeto de estudo (Severino, 2016).

Não seria coerente, portanto, propor práticas descoladas das forças regulatórias do ambiente digital; desconsiderando, assim, todo o processo em que o problema já está inserido.

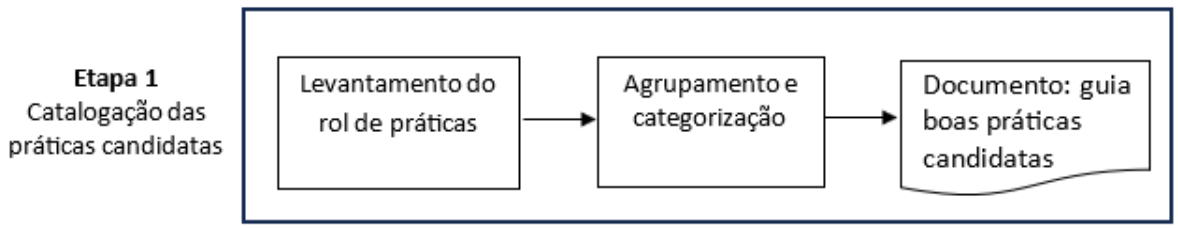
5.1.1 Objetivo

O objetivo desta etapa foi revisar referências legais e não-legais sobre privacidade e ética no desenvolvimento de jogos digitais, identificando e categorizando as boas práticas mencionadas. Buscou-se compilar um repertório fundamentado em diretrizes reconhecidas, como regulamentações e recomendações de especialistas.

5.1.2 Processo

Retomando o que já dissemos no início deste capítulo, no processo da etapa 1, tivemos as seguintes subetapas (Figura 3): levantamento do rol de práticas; agrupamentos e categorização que resultaram no documento de guia de boas práticas candidatas (APÊNDICE A). No levantamento do rol de práticas, tínhamos um total de 62 práticas que, após agrupamento, resultaram em 48 práticas, alocadas em 9 categorias.

Figura 3 - Fluxograma da metodologia da Etapa 1.



Fonte: Elaboração da autora

5.1.3 Levantamento do rol de práticas

Ao iniciar a revisão da literatura, levantamos palavras-chave que nos pareciam pertinentes ao tema do trabalho e, por meio da plataforma Google Acadêmico, realizamos diferentes buscas combinadas entre elas. As *strings* de pesquisa que trouxeram um volume de resultados interessante e bem delimitado estão apresentadas na tabela abaixo.

Todos os resultados das buscas foram revisados por nível de relevância/interesse para a pesquisa; e os artigos julgados de interesse foram lidos, destacando-se de que forma abordavam e/ou respondiam às perguntas de pesquisa.

Tabela 5 - Strings de pesquisa/palavras-chave.

Strings de pesquisa/palavras-chave	Resultado total*	Resultados de interesse*
("children" OR "kids") AND ("ethics" OR "ethical" OR "data privacy") AND ("online games" OR "mobile games") AND "game design" AND ("data-driven" OR "data mining")	1595	35
("kids" OR "children") AND ("regulation" OR "rights") AND "games" AND ("ethical" OR "ethics") AND "personal information" AND "data privacy"	2861	134
("children" OR "kids") AND ("ethics" OR "ethical" OR "data privacy" OR "dark patterns") AND ("online games" OR "mobile games") AND "game design" AND ("data-driven" OR "data mining")	1605	30

Fonte: Elaboração da autora
* Resultado válido para consulta realizada em março de 2023

Uma vez revisadas as referências, seguimos para o levantamento do rol de práticas. Por exemplo, a COPPA determina em seu Artigo 312.5:

> An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

O desenvolvedor enquadra-se, neste caso, no papel de operador, conceituado como: *“operator means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service* (COPPA,§ 312.2).

Dessa forma, tal exigência converteu-se na prática BP2.2 da Categoria 2 - Controle parental: *“Obter consentimento parental verificável antes de qualquer coleta, uso e/ou divulgação de informações pessoais de crianças, alocando de todos os esforços e recursos disponíveis”.*

O critério utilizado para o levantamento das práticas foi a completude; isto é, mesmo que uma prática seja citada em apenas uma das fontes pesquisadas, ela foi incluída no rol de práticas recomendadas.

Como estratégia didática, optamos por organizar as práticas em formato de tabela. Na linha listamos as práticas e, nas colunas, assinalamos as fontes nas quais a prática foi coletada, conforme exemplificado na Tabela 6.

Em alguns casos, uma prática pode estar descrita de forma explícita em uma determinada fonte; porém, em outras pode aparecer de forma implícita dentro dos princípios. Por isso, optamos por assinalar ambas as fontes:

Tabela 6 - Práticas candidatas e suas fontes de coleta.

	FONTE COLETADA						
PRÁTICA	**COPPA**	**GDPR-K**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
Prática candidata 1	**X**	**X**	**X**	**X**	**X**		
Prática candidata 2	**X**		**X**	**X**	**X**	**X**	

Fonte: Elaboração da autora

Elegemos e agrupamos as fontes, segundo a abordagem apresentada no capítulo 4 deste trabalho intitulado “ Estado da arte das forças regulatórias”:

- Legislação: COPPA, GDPR-K, LGPD, PL 2628/22
- Normas e políticas de mercado: *Google Play*, *App Store*
- *Design Dark Patterns*: referente à literatura acadêmica sobre o assunto

Optamos por escolher o *Google Play* e a *App Store, como fontes normativas de política de mercado*, por serem as duas principais plataformas de distribuição de jogos *mobile*. Por essa natureza, preocupam-se em divulgar, para os desenvolvedores, práticas e orientações para criação de experiências seguras e adequadas ao público infantil e juvenil. Também constatamos que todas as práticas

levantadas a partir das fontes legais estão contidas nas políticas do *Google Play* e *App Store,* uma vez que exigem compliance com as exigências da legislação.

É importante observar e estar ciente de que as práticas éticas levantadas apresentam diferentes níveis de granularidade: algumas, mais amplas e conceituais; outras, mais específicas e operacionais. Essa heterogeneidade decorre da própria natureza das fontes consultadas, que variam entre legislações, diretrizes técnicas de mercado e literatura acadêmica.

Até o momento, não identificamos na literatura uma metodologia consolidada para uniformizar ou hierarquizar essas práticas de forma sistemática. Diante disso, optamos por manter a diversidade de granularidade como forma de preservar a completude do guia.

5.1.4 Agrupamentos das práticas similares

Conforme já mencionado, a etapa intitulada “Levantamento do rol de práticas” resultou na identificação de 62 práticas distintas relacionadas a aspectos éticos, regulatórios e de design voltados à proteção de crianças em ambientes digitais.

Ao realizar uma análise mais aprofundada da natureza dessas práticas, contudo, foi possível observar que diversas delas apresentavam sobreposições conceituais ou operacionais, fazendo referência a ações semelhantes, por exemplo:

> **Prática A:** *Fornecer acesso a uma política de privacidade no site ou serviço online sobre quais informações coleta da criança, como usa essas informações e suas práticas de divulgação de tais informações.* (COPPA, § 312.4(b))

> **Prática B:** *Incluir um link proeminente e claramente rotulado para uma política de suas práticas de informações com relação a crianças na página inicial e em cada área do site ou serviço on-line em que informações pessoais de crianças são coletadas. O link deve estar próximo aos pedidos de informação de cada uma dessas áreas.* (COPPA, § 312.4(d))

Ambas as práticas, neste caso, convergem para a exigência do acesso claro, destacado e facilmente localizável de uma política de privacidade, garantindo assim transparência no tratamento dos dados pessoais.

Constatações dessa natureza nos permitiram agrupar as práticas promovendo uma maior síntese do conjunto de itens a serem propostos. Após o processo de agrupamento, o rol inicial de 62 itens foi consolidado em 48 práticas finais, mantendo a abrangência dos conteúdos originais. Esse refinamento contribuiu para uma análise mais clara, estruturada e aplicada às diretrizes do trabalho.

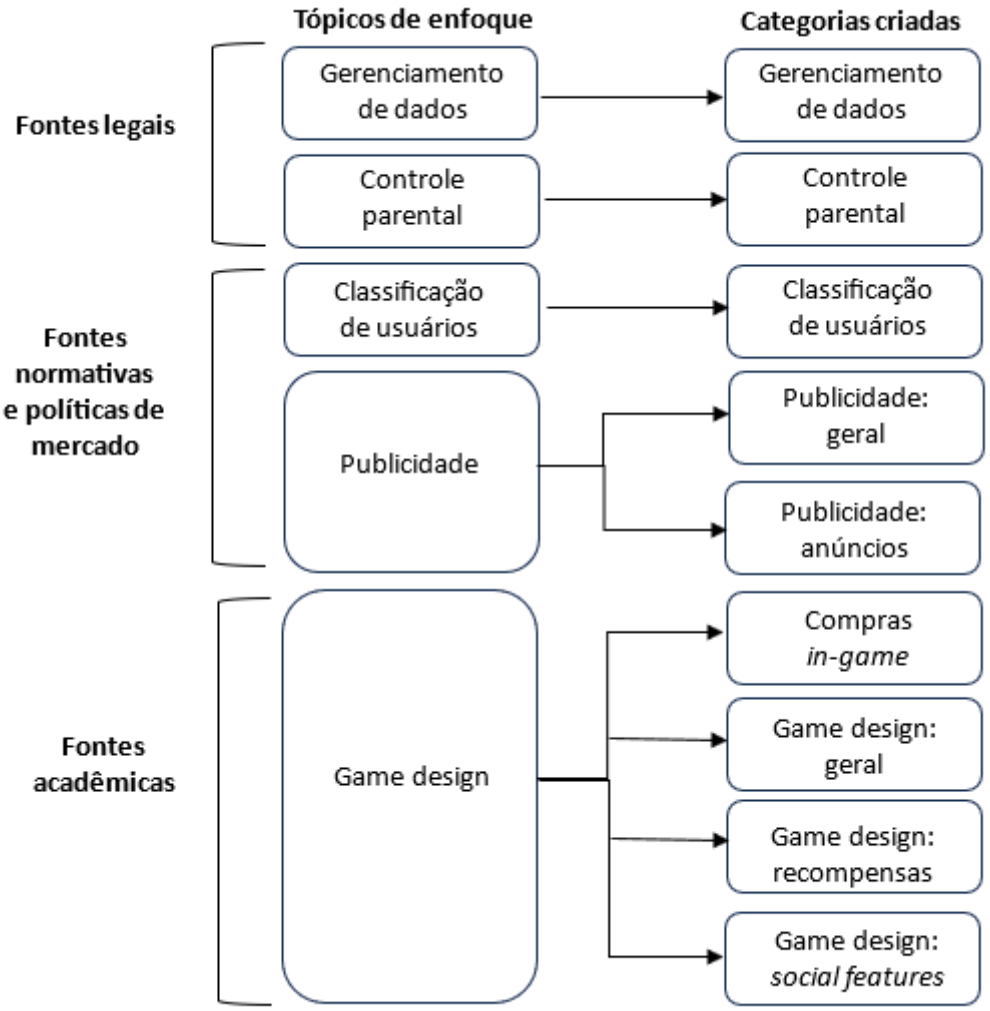
5.1.5 Categorização das práticas

Observamos que a depender do tipo de fonte consultada, os tópicos abordados pelas práticas levantadas convergiam de acordo com o enfoque dado:

a) Fontes legais, como COPPA, GDPR, LGPD tratam, majoritariamente, de práticas relativas à coleta, armazenamento, compartilhamento e exclusão de dados pessoais; bem como a práticas relativas a recursos que garantam aos pais a ciência e o controle sobre os dados fornecidos pelos filhos.
b) Fontes normativas de políticas de mercado - além de fazer referência às práticas das fontes legais - agregam práticas relativas à classificação de usuários, inclusive, como forma de adequação às exigências das fontes legais; e ao uso de publicidade, como forma de resguardar os usuários do consumo inadequado de conteúdos.
c) Já as fontes acadêmicas - além de apontar as práticas das fontes legais, das normas e políticas de mercado - contribuem com discussões acerca de práticas relativas à arquitetura mecânica do jogo em si, principalmente, para fins de retenção e monetização.

Observando essa configuração, fizemos o seguinte raciocínio (como ilustrado na figura 4): a partir das fontes, designamos os tópicos de enfoque em que cada uma delas mais contribuíram e, por fim, convertemos esses tópicos em categorias.

Figura 4 - Tópicos de enfoque e categorias criadas



Fonte: Elaboração da autora

Como mostramos na Figura 4 acima, convertemos os tópicos Gerenciamento de dados, Controle parental e Classificação de usuários em categorias. Optamos por subdividir as categorias Publicidade e Game Design devido ao grande número de práticas e a diversidade de assuntos abordados.

Na categoria Publicidade, uma parcela das práticas tinha a ênfase na formatação e exibição de anúncios dentro do jogo; por isso, mantivemos a divisão em geral e de anúncios. As categorias tidas como gerais não apresentam nenhum assunto em específico, tratando do tópico em questão de forma abrangente.

Na categoria *Game design*, as práticas são decorrentes, em sua maioria, dos padrões considerados *dark patterns* pela literatura, apresentados no capítulo 4 " Estado da arte das forças regulatórias".

Na categoria *Game design*, o número de práticas era extenso e os assuntos diversificados. Em grande parte, havia foco em práticas relativas à compra in-game, a estratégias de recompensa de usuários e a estratégias de uso do “capital social” do jogador.

Como já vimos no tópico 4.5.2, El-Nasr & Kleinman (2020) abordam práticas predatórias no contexto relativos à monetização e retenção, especialmente, fazendo uso de recompensas ou da rede de contatos dos jogadores. Optamos, então, por converter as práticas relativas à compras *in-game* em uma categoria independente, uma vez que elas dizem respeito não apenas às mecânicas do jogo, mas ao seu modelo de negócio.

As demais práticas, que dizem respeito às mecânicas do jogo em si, foram convertidas nas categorias *Game design: recompensas*, *Game design: social features* e *Game design*: geral. Esta última apresenta práticas diversificadas, que não têm por enfoque, nem ao capital social do jogador, nem ao uso de recompensas para retenção.

Tendo em vista que o objetivo final deste trabalho é a proposição de um guia de práticas éticas voltado ao desenvolvedor, é fundamental não perdê-lo de vista como usuário final ao longo de todo o processo. Acreditamos, portanto, que a configuração adotada para as categorias também desempenha um papel didático, ao empregar conceitos acessíveis e alinhados à realidade do desenvolvedor, tanto no contexto de design quanto no modelo de negócio de seus jogos.

5.2 Resultado e discussão das práticas candidatas

Neste tópico, apresentaremos e discutiremos as 48 práticas consolidadas e reunidas nas 9 categorias, após agrupamento e categorização, descritos nos tópicos anteriores (5.1.4 e 5.1.5).

A discussão será centrada no aprofundamento teórico e técnico das práticas apresentadas, com o objetivo de identificar estratégias e orientações exemplificativas, para sua aplicação em conjunto com as *features* comumente empregadas por desenvolvedores em seus jogos. Essas estratégias e diretrizes foram extraídas das mesmas fontes revisadas para levantamento do rol geral de práticas.

5.2.1 Categoria 1 - Gerenciamento de dados

A Categoria 1 – Gerenciamento de Dados foi estruturada com base na definição de que este processo envolve a coleta, o processamento, o armazenamento e o uso de dados pessoais de forma transparente, assegurando o respeito aos direitos de privacidade dos indivíduos e a implementação de medidas de segurança para prevenir violações ou minimizar danos potenciais (COPPA). Nessa perspectiva, reunimos sete práticas relacionadas a esse processo, listadas na Tabela 7 abaixo:

Tabela 7 - Práticas candidatas da Categoria 1- Gerenciamento de Dados.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 1.1	Não coletar dados excessivos ou desnecessários para a funcionalidade da sua aplicação.	**X**	**X**	**X**				
BP 1.2	Manter os dados apenas no período de tempo razoável e justificável para o propósito para o qual foi coletado.		**X**	**X**			**X**	
BP 1.3	Não enviar para terceiros informações de identificação pessoal, localização ou informações do dispositivo	**X**	**X**	**X**			**X**	
BP 1.4	Permitir ao responsável a possibilidade de apagamento total do dados fornecidos, em qualquer momento	**X**	**X**	**X**			**X**	
BP 1.5	Não usar cookies de rastreamento ou quaisquer outros recursos similares de rastreamento passivo.	**X**	**X**	**X**	**X**	**X**	**X**	
BP 1.6	Se você permitir que os usuários se registrem com um username, lembre-os de que eles devem evitar usar nomes reais ou identificadores de mídia social existentes.				**X**	**X**		

BP 1.7	Evite utilizar recursos ou estratégias subliminares para que o jogador compartilhe mais informações do que realmente pretende.		**X**					Gray et. al, 2018.

Fonte: Elaboração da autora

Embora a maioria dessas práticas esteja claramente respaldada por normas legais, elas também são reforçadas por diretrizes de mercado, como as políticas da Google Play e da App Store, que demonstram adesão integral a essas exigências.

As práticas, desta categoria, abordam princípios-chave de proteção de dados pessoais de crianças, com ênfase na minimização da coleta, limitação temporal, transparência no uso de informações sensíveis e na garantia dos direitos dos pais ou responsáveis.

A prática BP 1.1 sobre não coletar dados excessivos ou desnecessários encontra conformidade com o princípio da minimização, previsto no Art. 5(1)(c) do GDPR e no Art. 6º, inciso III e V da LGPD, que determinam que o tratamento deve se limitar ao mínimo necessário para atingir sua finalidade. Por exemplo, aplicativos infantis que exigem acesso ao microfone ou câmera mesmo sem necessidade funcional. Muitos apps, voltados ao público infantil, solicitam permissões invasivas para coletar dados de voz, localização ou sensor, mesmo que essas funções não sejam parte central da experiência.

O GDPR estabelece a minimização de dados como princípio central, em seu Art.5º(1)(c): *“Os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.”*; a LGPD contempla os mesmos princípios em seu Art. 6º, Inciso III: *“Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.” e* Art. 6º, Inciso V: *“Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades.”*

Não compartilhar informações de identificação pessoal, localização ou dados do dispositivo com terceiros sem consentimento parental (BP 1.3) está diretamente alinhada à COPPA (16 CFR § 312.4 e § 312.5), que exige consentimento verificável dos pais antes de qualquer coleta, uso ou divulgação de dados de crianças menores de 13 anos. Por exemplo, o *TikTok* foi multado por transferir dados de localização e

de dispositivos de crianças para servidores externos. O app repassava informações sem consentimento explícito dos responsáveis (Gazeta do Povo, 2023).

A possibilidade de apagamento total dos dados a qualquer momento (BP 1.4) encontra respaldo no direito ao apagamento, previsto no Art. 17 do GDPR, Art. 18 da LGPD; e. nos requisitos de revogação de consentimento da COPPA (§ 312.6).

A *Information Commissioner's Office* (ICO, Reino Unido) oferece orientações importantes sobre a criação e a adaptação de recursos que apoiem o gerenciamento adequado dos dados fornecidos por crianças, pais e responsáveis, respeitando as diferentes faixas etárias dos usuários. A Tabela 8 apresenta um resumo dessas recomendações, por faixa etária:

Tabela 8 - Recomendações para adaptação de recursos por faixa etária.

Faixa etária	**Recomendações**
2-5 anos (pré-alfabetização e alfabetização inicial)	Forneça ícones, avisos de áudio ou similares que até as crianças mais novas reconhecerão como significando "Não estou feliz" ou "Preciso de ajuda". Se esses botões forem pressionados ou outros avisos forem respondidos, forneça material de vídeo ou áudio solicitando à criança que procure ajuda de um dos pais ou de um adulto de confiança.
6-9 anos	Forneça ícones, avisos de áudio ou similares que as crianças reconheçam como significando "Não estou feliz" ou "Preciso de ajuda". Se esses botões forem pressionados ou outros avisos forem respondidos, forneça material de vídeo ou áudio solicitando à criança que procure ajuda de um dos pais ou de um adulto de confiança e, em seguida, direcione a criança para sua ferramenta online.
10-12 anos	Forneça ícones, avisos de áudio ou similares que as crianças reconheçam como significando "Não estou feliz" ou "Preciso de ajuda". Se esses botões forem pressionados ou outros avisos forem respondidos, direcione a criança para sua ferramenta on-line e peça a ela que procure ajuda de um dos pais ou de um adulto de confiança, se precisar.
13 anos ou mais	Forneça ícones, avisos de áudio ou similares que as crianças reconheçam como "Quero relatar uma preocupação", "Quero acessar minhas informações" ou "Preciso de ajuda".

	Se esses botões forem pressionados ou outros avisos forem respondidos, direcione a criança para suas ferramentas on-line e peça que ela procure ajuda dos pais ou de outro recurso confiável, se precisar.

Fonte: *Information Commissioner's Office* (ICO, Reino Unido)

A ICO ainda recomenda a implementação de ferramentas específicas que operacionalizem os direitos previstos na legislação de proteção de dados, tanto das crianças quanto dos seus pais ou responsáveis. Essas ferramentas devem ser claras e acessíveis, por exemplo:

- Uma função de *"Baixar todos os meus dados"*, para viabilizar o direito de acesso e à portabilidade;
- Uma opção para *"Apagar todos os meus dados"* ou *"selecionar dados para exclusão"*, em apoio ao direito ao apagamento;
- Um mecanismo de *"Interromper o uso dos meus dados"*, que atenda ao direito à limitação ou oposição ao tratamento;
- Uma funcionalidade de *"Corrigir meus dados"*, que garanta o direito à retificação.

Além disso, devem ser implementados mecanismos contínuos de acompanhamento e comunicação, permitindo que crianças e seus responsáveis monitorem o status de solicitações ou reclamações. É essencial informar os prazos de resposta às solicitações; e, os procedimentos internos também devem prever respostas rápidas e proativas em casos que indiquem risco iminente ou violações de proteção de dados.

A proibição do uso de rastreamento passivo (BP 1.5) em aplicações digitais destinadas a crianças é uma diretriz central nas legislações voltadas à proteção da privacidade infantil. Além dos *cookies* invisíveis, outras técnicas como *fingerprinting* de dispositivo e coleta automática de localização também são consideradas invasivas por todas as legislações pertinentes.

Frequentemente, os jogadores criam seus perfis de usuário, mediante um *username* público. A prática BP 1.6 recomenda que, na página de criação de conta, haja um aviso expresso para que o jogador não utilize nomes reais. A página *Sign in*

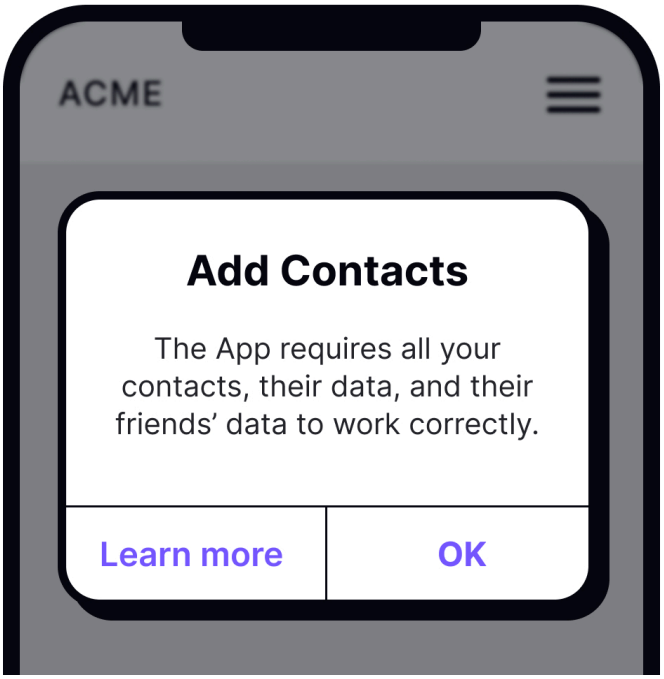
do Roblox (Figura 5) é um bom exemplo de como essa recomendação pode ser aplicada.

Figura 5 - Exemplo de boa prática na tela de login do Roblox

Fonte: Roblox.com

A recomendação de evitar estratégias subliminares ou persuasivas que induzam a criança a compartilhar mais informações do que pretendia (BP 1.7) é chamada na literatura como um padrão "*Privacy Zuckering*" (Gray et. al, 2018), em referência a uma prática utilizada por Zuckerberg, criador do Facebook. Por exemplo, sugerir ao usuário que - para funcionar corretamente - o jogo precisa ter acesso a informações excessivas e sem qualquer aplicabilidade direta com o contexto de uso (Figura 6).

Figura 6 - Exemplo ilustrativo de dark pattern “Privacy Zuckering”



Fonte: Uxcel

A prática (BP 1.7) está alinhada à proibição de *nudges* com fins manipulativos, tratado no documento complementar *Age Appropriate Design Code* (ICO, 2020), reforçando a importância de um design centrado no melhor interesse da criança e compatível com sua capacidade de compreensão. Abordaremos mais sobre o assunto no tópico 5.2.7.

5.2.2 Categoria 2 - Controle Parental

A Categoria 2 – Controle Parental foi organizada com base na definição de que esse conceito refere-se às práticas e mecanismos que permitem aos pais ou responsáveis controlar e monitorar as atividades *online* de seus filhos menores (COPPA). A partir dessa perspectiva, reunimos seis práticas relacionadas a esses mecanismos e recursos, apresentadas na Tabela 9 a seguir.

Tabela 9 - Práticas candidatas da Categoria 2 - Controle parental.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 2.1	Deixar explícito e acessível um link para acesso da política de privacidade do jogo na página inicial e em cada página em que informações pessoais das crianças são coletadas.	**X**	**X**	**X**	**X**	**X**	**X**	
BP 2.2	Obter consentimento parental verificável antes de qualquer coleta, uso e/ou divulgação de informações pessoais de crianças, alocando de todos os esforços e recursos disponíveis.	**X**	**X**	**X**	**X**	**X**	**X**	
BP 2.3	Fornecer um meio razoável para que os pais revisem as informações pessoais coletadas de uma criança e se recusem a permitir seu uso ou manutenção.	**X**	**X**	**X**	**X**	**X**	**X**	
BP 2.4	Incluir *parental gates* em momentos estratégicos para impedir que as crianças façam compras ou sigam links de um aplicativo para sites, redes sociais ou outros aplicativos sem o conhecimento de seus pais ou responsáveis.				**X**	**X**		
BP 2.5	Incluir um recurso para denunciar conteúdo inadequado no jogo.					**X**		
BP 2.6	Não incluir, fora da *parental gate*, oportunidades de compra ou outras distrações para as crianças.				**X**	**X**		

Fonte: Elaboração da autora

Na prática BP 2.1, temos a menção à política de privacidade, que consiste em um documento que descreve de forma clara, acessível e transparente como os dados pessoais dos usuários são coletados, utilizados, armazenados, protegidos e eventualmente compartilhados por um aplicativo, site ou serviço digital. Segundo a *Information Commissioner's Office* (ICO, 2020), a formulação de uma boa política de privacidade deve pressupor:

- **Clareza e linguagem simples:** redigida em linguagem compreensível para o público-alvo, especialmente crianças e seus pais;
- **Transparência:** informa claramente quais dados são coletados, por que são coletados, como serão usados, e com quem poderão ser compartilhados;
- **Finalidade específica:** explica o propósito de cada tipo de dado coletado, evitando generalizações vagas;
- **Medidas de segurança adotadas:** descreve como os dados são protegidos contra acesso indevido, vazamentos e uso não autorizado;
- **Consentimento parental:** especifica como é obtido o consentimento dos pais ou responsáveis, conforme exigido por leis;
- **Prazo de retenção dos dados:** indica por quanto tempo os dados serão armazenados e quando serão excluídos;
- **Direitos dos usuários:** explica como os usuários (ou seus responsáveis) podem acessar, corrigir, apagar ou contestar o uso dos dados;
- **Canal de contato:** fornece informações de contato para dúvidas ou solicitações relacionadas à privacidade.

As empresas desenvolvedoras devem revisar e atualizar periodicamente suas políticas de privacidade e termos legais para assegurar a conformidade com as legislações e regulamentações mais recentes. Esses materiais devem ser claros, objetivos e redigidos em linguagem acessível, compatível com o nível de compreensão de crianças e adolescentes.

Recomenda-se, ainda, a adoção de notificações de privacidade *just-in-time*, isto é, mensagens contextuais que informam, no momento da interação, quais dados estão sendo coletados e para que finalidade.

Como enfatizado anteriormente, a obtenção do consentimento parental verificável (BP 2.2) é um dos fundamentos centrais e obrigatórios para a proteção de dados de crianças e adolescentes, conforme estabelecido pelas principais

legislações de privacidade infantil. A COPPA (*Children's Online Privacy Protection Act*) é o instrumento legal que mais detalha os métodos aceitáveis para a obtenção desse tipo de consentimento. Entre os métodos expressamente reconhecidos, temos:

a) Disponibilizar um formulário de consentimento a ser assinado pelos pais ou responsáveis e devolvido ao operador por correio ou assinatura eletrônica;

b) Exigir que o responsável realize uma transação monetária, utilizando cartão de crédito, débito ou outro sistema de pagamento *online* que forneça notificação de cada transação ao titular da conta principal;

c) Permitir que o responsável entre em contato por telefone, ligando para um número gratuito operado por uma equipe treinada para validar o consentimento;

d) Realizar uma videoconferência direta com o responsável legal, conduzida por representantes da equipe de desenvolvimento;

e) Verificar a identidade do responsável por meio de um documento oficial, cruzando as informações com bases de dados apropriadas (sendo obrigatório que o documento seja excluído dos registros imediatamente após a verificação);

f) Quando não houver divulgação de dados pessoais da criança, o desenvolvedor pode solicitar o consentimento por e-mail, desde que adote etapas adicionais para garantir a identidade do responsável. Tais medidas incluem o envio de um e-mail de confirmação após o recebimento do consentimento, ou ainda, a solicitação de um endereço físico ou número de telefone, com validação posterior por meio de ligação.

Vale ressaltar aqui que as opções, atualmente, previstas na legislação para a obtenção do consentimento parental ainda nos parecem burocráticas e, em muitos casos, pouco ágeis, o que pode dificultar sua adoção prática por parte dos desenvolvedores. Nesse sentido, destaca-se a importância de incentivar o desenvolvimento de soluções inovadoras, que aliem agilidade, usabilidade e segurança, facilitando a implementação efetiva do consentimento.

Também existem exceções à necessidade da obtenção do consentimento parental, previstos pela COPPA, conforme descrito no 16 CFR § 312.5(c), tais como:

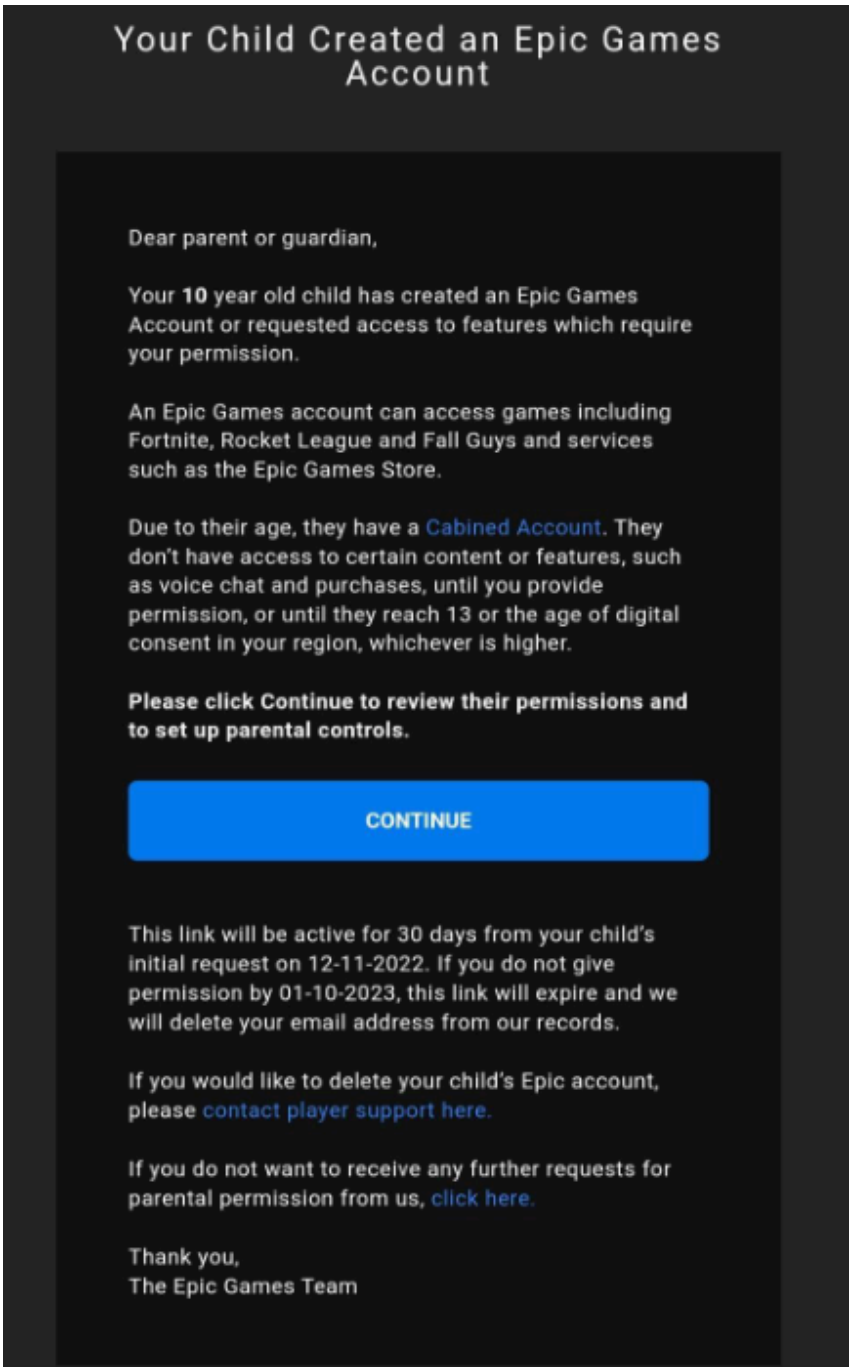
resposta a um contato direto da criança (contato único), suporte interno ao funcionamento do serviço e uso educacional autorizado por instituições escolares em nome dos pais. Em todos os casos, a coleta deve ser limitada, proporcional e não explorada para finalidades comerciais; ainda sendo obrigatório fornecer informações claras sobre o tratamento dos dados coletados.

É recomendado que, ao solicitar o consentimento, os desenvolvedores expliquem, de forma clara, como a coleta dos dados contribuirá para aprimorar a experiência da criança, promovendo, assim, uma tomada de decisão mais informada pelos pais e responsáveis (Super Awesome, 2018).

Relativo às práticas BP 2.1, BP 2.2 e BP 2.3, um bom exemplo prático e interessante de sua aplicabilidade é o *processo de consentimento dos pais,* elaborado pela *Epic Games* e detalhado em seu site (Epic Games, 2025):

a) Etapa 1 - Recebimento de comunicação eletrônica: após a identificação da criação da conta pelo usuário menor de idade, será enviado um e-mail de notificação ao endereço informado como de pai/responsável. No corpo da mensagem, deve-se acessar o link indicado para iniciar o processo de consentimento (Figura 7).

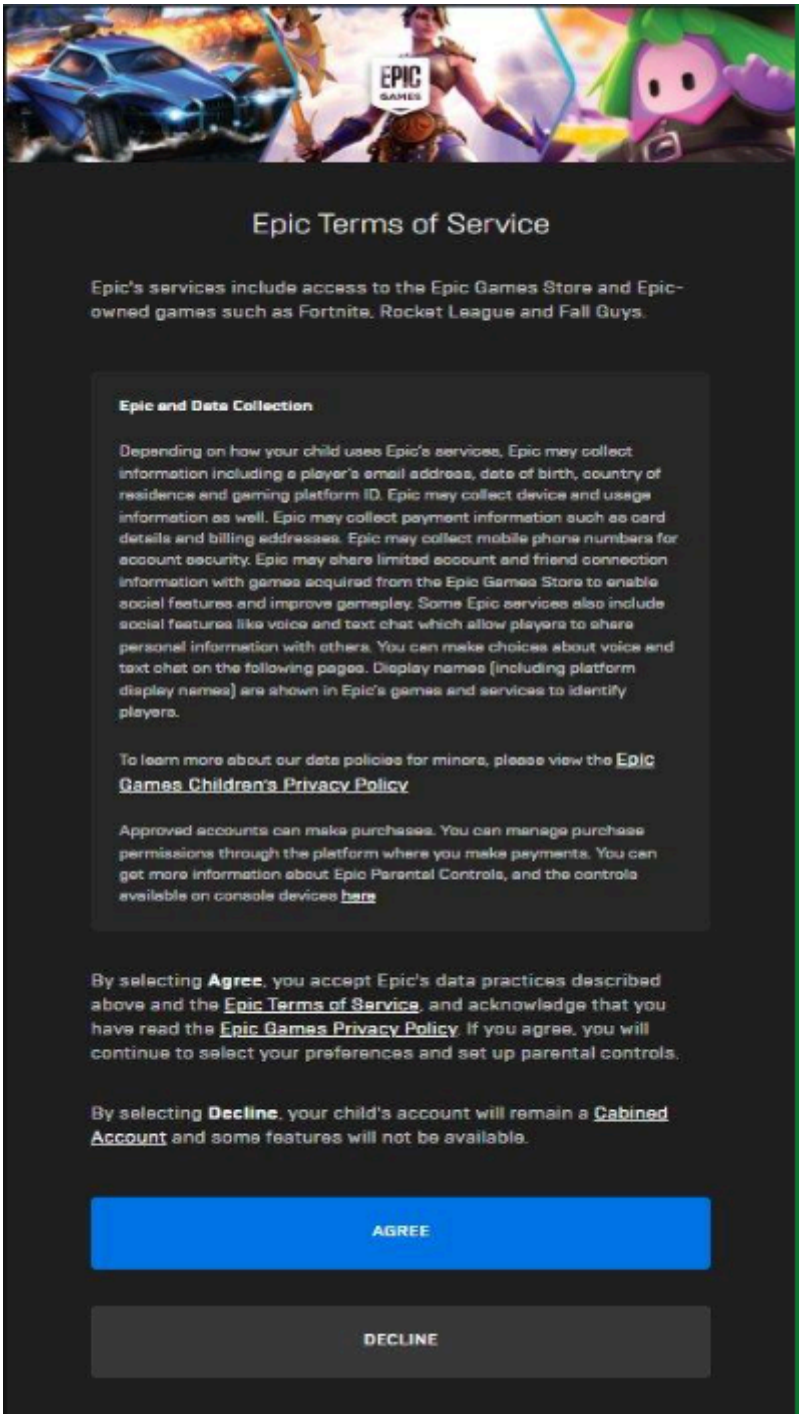
Figura 7 - Etapa 1 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

Etapa 2 - Aceite dos Termos de Serviço: o link redireciona para a página oficial da *Epic Games*, onde é requerida a concordância com os Termos de Serviço vigentes (Figura 8).

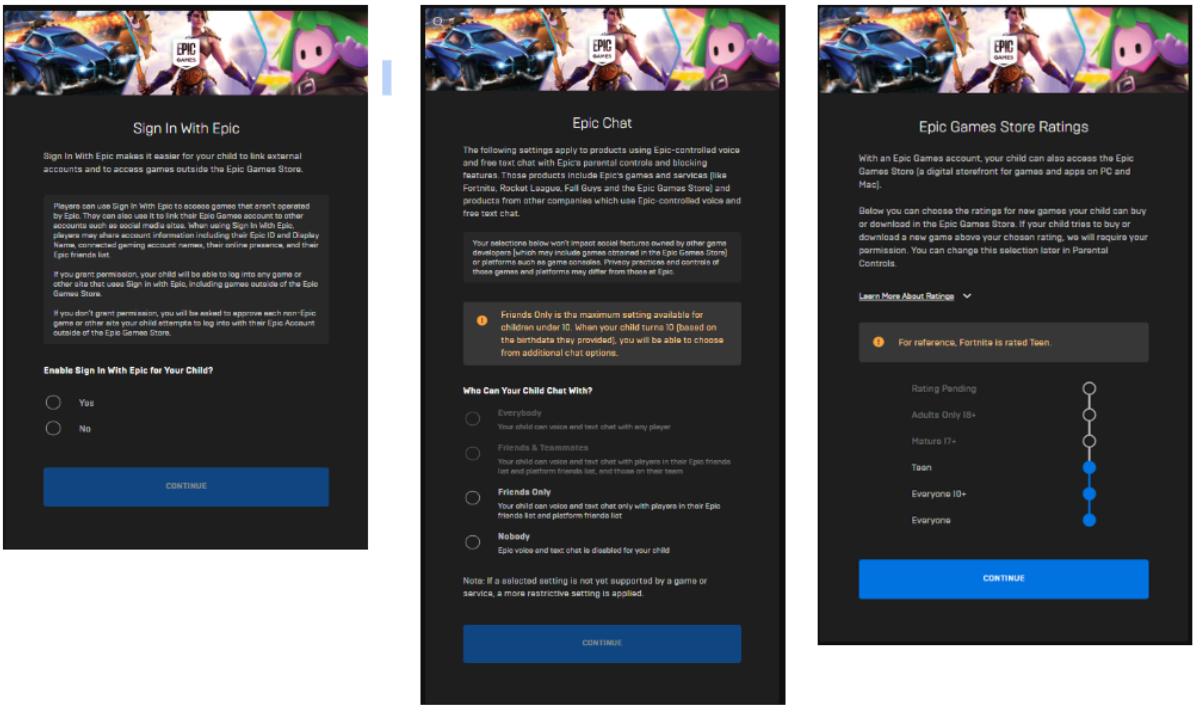
Figura 8 - Etapa 2 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

b) <u>Etapa 3 - Configuração de permissões da conta</u>**:** após a aceitação dos termos, devem ser estabelecidas as permissões relativas ao uso da conta, como acesso a chat, capacidade de realizar compras, *download* de conteúdo e classificação etária permitida (Figura 9).

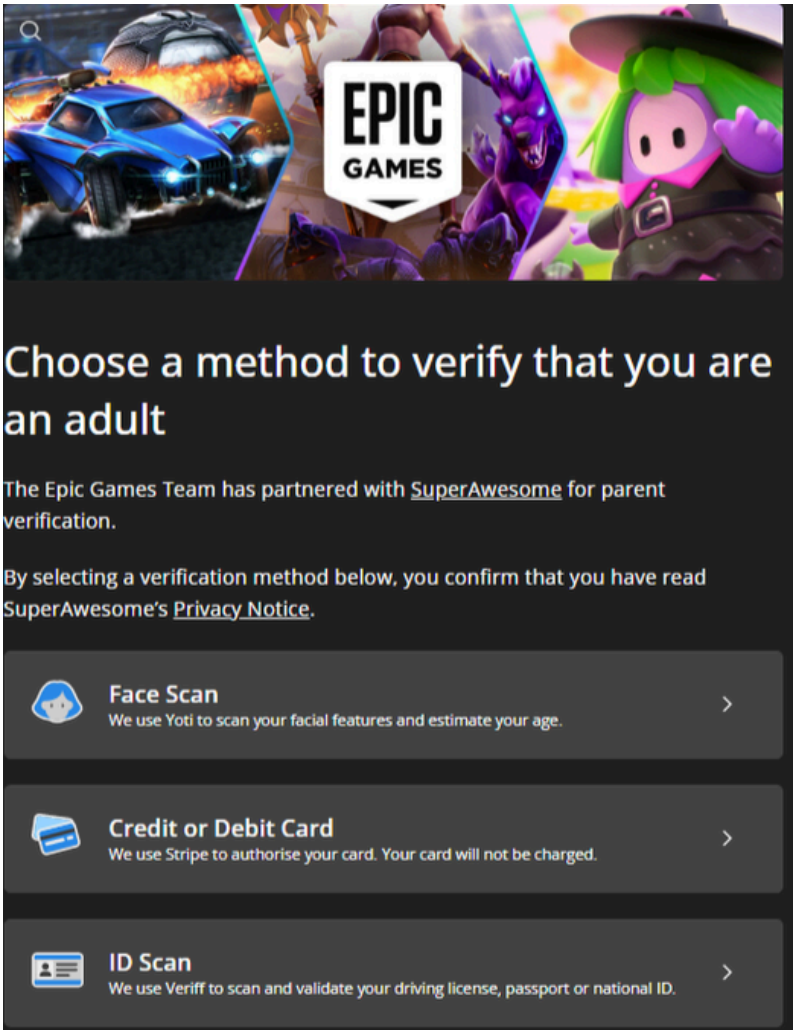
Figura 9 - Etapa 3 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

c) Etapa 4 - Verificação de maioridade: a comprovação de maioridade deve ser realizada por meio de um dos métodos disponíveis, conforme a localidade: escaneamento facial, cartão de crédito ou débito válido, digitalização de documento oficial (Figura 10).

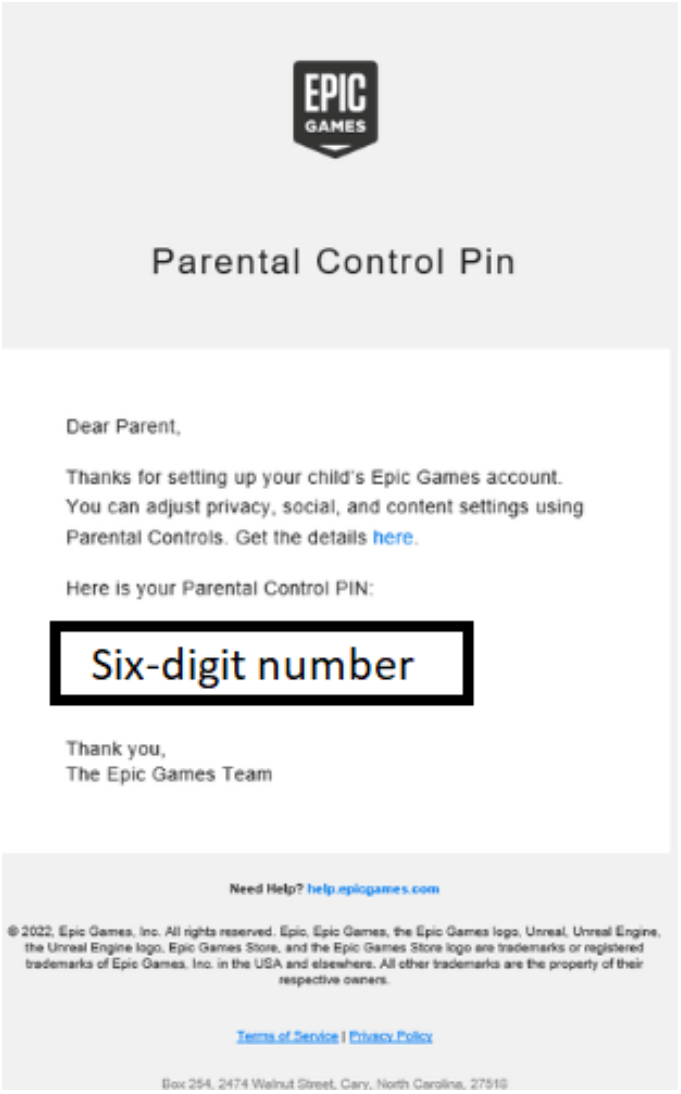
Figura 10 - Etapa 4 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

d) Etapa 5 - Geração de código PIN de controle parental: **a**pós validação, será gerado um código PIN vinculado à conta, o qual será exigido para futuras alterações de informações e de configurações de controle parental (Figura 11).

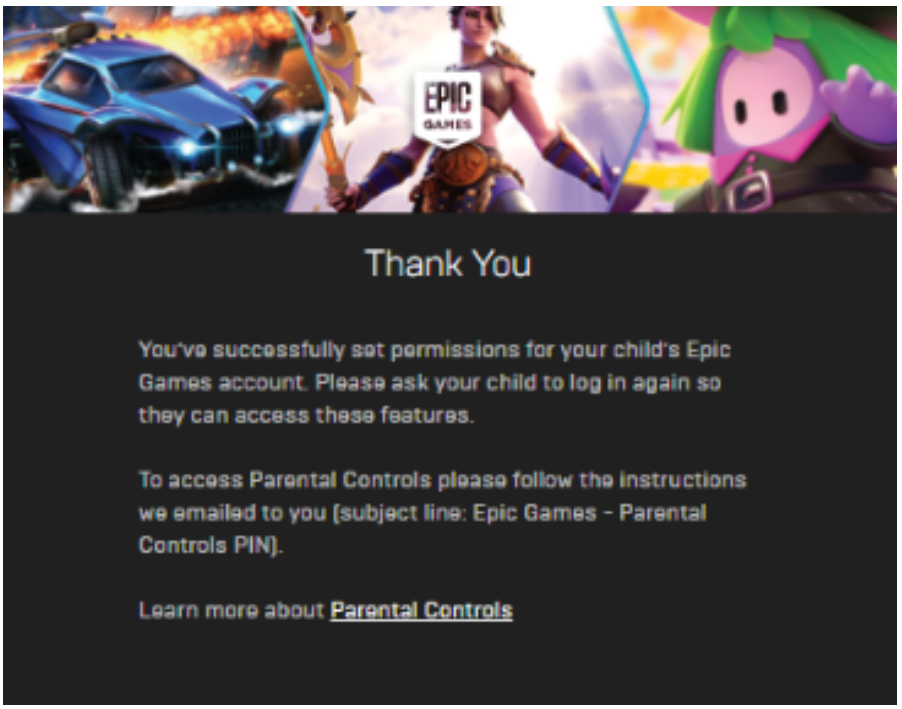
Figura 11 - Etapa 5 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

e) Etapa 6 - Confirmação de finalização do processo: **c**oncluídas as etapas anteriores, a plataforma exibirá a confirmação de que as permissões foram devidamente configuradas (Figura 12).

Figura 12 - Etapa 6 do processo de consentimento dos pais da Epic Games



Fonte: Epic Games, 2025.

Além das etapas anteriores mencionadas, a criação de um *parental gate* (BP 2.4 e BP 2.6) consiste na inserção de uma “tela-barreira” que exige a conclusão de uma tarefa voltada ao público adulto, como forma de restringir o acesso da criança a determinadas funcionalidades, em qualquer momento da experiência.

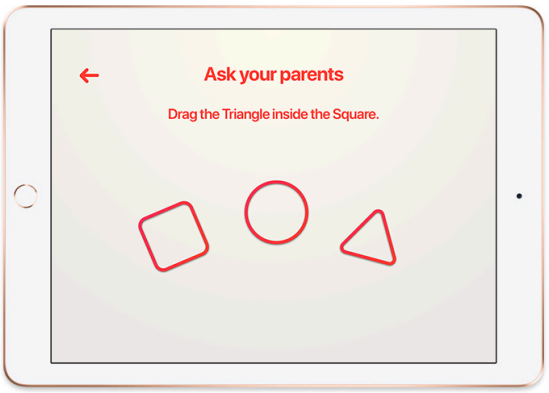
As diretrizes das lojas de aplicativos determinam que aplicativos enquadrados na categoria infantil implementem esse tipo de barreira para impedir que crianças realizem transações comerciais ou acessem links externos, como sites, redes sociais ou outros aplicativos, sem o conhecimento ou consentimento de seus pais ou responsáveis.

Uma prática recomendada é randomizar as perguntas e respostas a cada nova exibição do *parental gate*, a fim de evitar a memorização por parte das crianças. A seguir, na Figura 13, apresentamos alguns exemplos que podem servir de inspiração para o design dessa funcionalidade.

Figura 13 - Exemplos de conformidade de *parental gates*

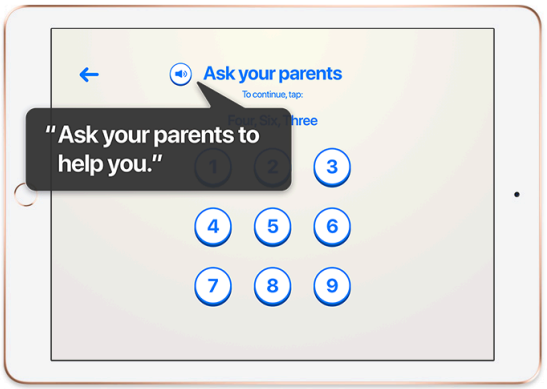
Lendo instruções simples

Alguns portões parentais incluem instruções simples que descrevem uma tarefa específica ou uma combinação de interações para um adulto concluir a fim de se envolver em comércio ou link fora do aplicativo.



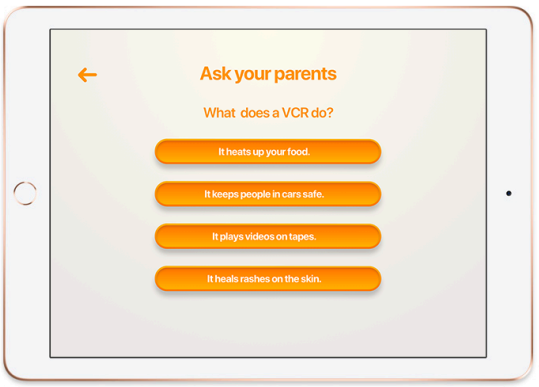
Falando instruções simples

Se seu aplicativo for destinado a crianças pré-alfabetizadas, considere o uso de um *prompt* de voz para ajudar as crianças a saberem que precisam envolver os pais.



Perguntas e respostas

Você também pode exigir que os usuários respondam corretamente às perguntas para continuar. A pergunta deve ser adequada à idade ou personalizável pelos pais, para que a criança não possa respondê-la facilmente.



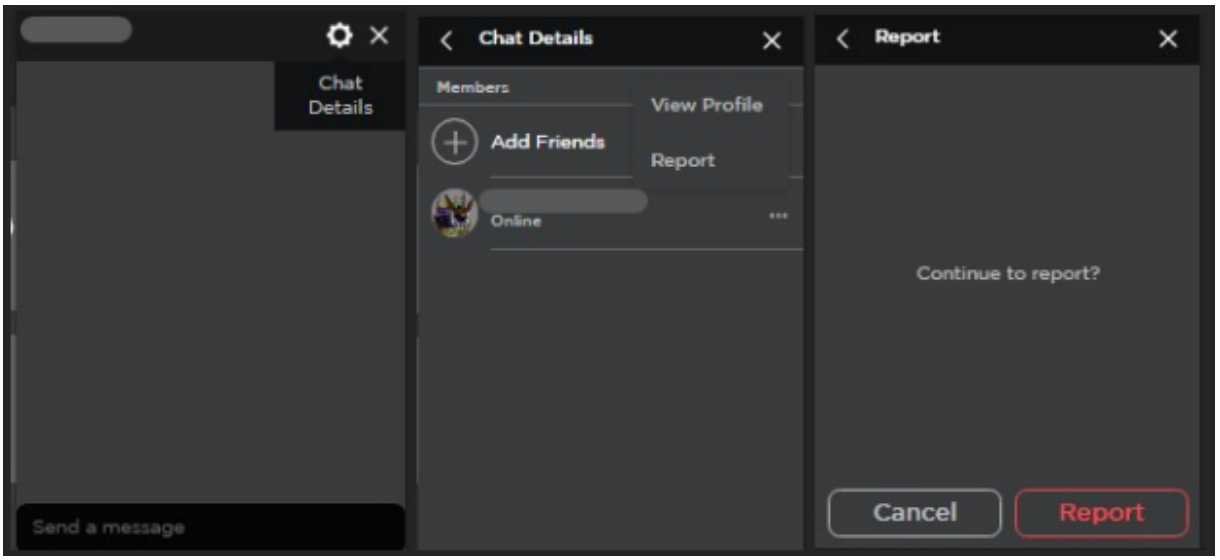
Fonte: *Apple Store Developer*, 2024

Importante destacar que o uso de *parental gates,* como barreira técnica, não substitui a exigência legal de consentimento parental verificável (BP 2.2) para a

coleta de dados pessoais de crianças, sendo instrumentos complementares com propósitos distintos.

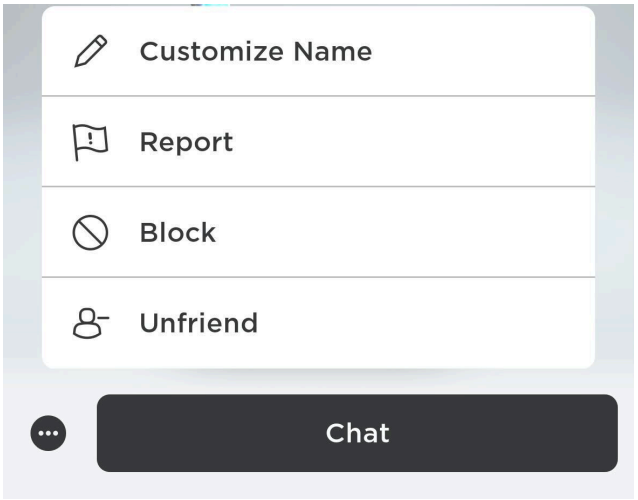
A inclusão de um recurso para denúncia de abusos (BP 2.5) é a melhor maneira de informar sobre infratores e conteúdo inadequado. A *Roblox*, por exemplo, disponibiliza que os jogadores usem o recurso “Report” para denunciar um bate-papo específico ou outro conteúdo que viole as regras da *Roblox* (Figura 14 e 15).

Figura 14 - Exemplo de bom uso do recurso Report no chat desktop do Roblox



Fonte: Roblox.com

Figura 15 - Exemplo de bom uso do recurso Report no chat mobile do *Roblox*



Fonte: Roblox.com

O recurso envia as informações diretamente aos moderadores do jogo e permitindo que vejam o que o outro usuário está fazendo de errado (*Roblox*, 2025).

5.2.3 Categoria 3 - Classificação de usuários

Estruturamos a Categoria 3 – Classificação de Usuários com base no conceito de que esse processo refere-se ao sistema utilizado por lojas de aplicativos para categorizar e avaliar apps de acordo com a adequação do conteúdo, a faixa etária indicada e o retorno dos usuários (*Google Play Store*). Com base nessa ideia, reunimos quatro práticas relacionadas a esses sistemas de classificação, apresentadas na Tabela 10 a seguir.

Tabela 10 - Práticas candidatas da Categoria 3 - Classificação de usuários.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 3.1	Definir, com clareza a faixa etária do seu público alvo, antes da publicação do jogo.				**X**	**X**		
BP 3.2	Declarar, no momento do registro em loja de apps, quais tipos de conteúdo podem ser encontrados no jogo de forma precisa e honesta para fins de classificação.				**X**	**X**		
BP 3.3	Antes de um jogador iniciar sua primeira sessão, verificar sua idade.				**X**	**X**		
BP 3.4	Analisar se há conteúdos, conceitos, temas delicados inadequados à idade segmentada.				**X**	**X**	**X**	

Fonte: Elaboração da autora

Definir com clareza a faixa etária do público-alvo, mesmo antes da publicação do jogo (BP 3.1) e declarar, no momento do registro em loja de apps, quais tipos de conteúdo podem ser encontrados no jogo de forma precisa e honesta (BP 3.2) são etapas fundamentais para garantir a conformidade legal, ética e comercial no que se refere à proteção de dados de crianças.

Essa definição de faixa etária orienta não apenas o design do conteúdo e da experiência do usuário, mas também as obrigações específicas impostas pelas

legislações dos países onde o jogo será comercializado e pelas políticas de distribuição em plataformas como a *Google Play* e a *App Store*.

Por exemplo, se o jogo se destina total ou parcialmente a crianças (menores de 13 anos nos EUA, menores de 12 anos no Brasil, e até 16 em alguns países da UE), o jogo será automaticamente submetido a regras mais restritivas de coleta de dados, consentimento parental e exposição à publicidade, impostas pelas legislações pertinentes.

Da mesma forma, se o jogo, mesmo incluindo adultos como público-alvo, apresentar imagens e termos que possam ser considerados voltados para crianças, possivelmente isso afete a avaliação em relação ao público-alvo declarado. Isso inclui todos os elementos da página e estratégias de marketing, como capturas de tela, vídeos, descrições do app, anúncios e estratégias de monetização.

Nesse sentido, classificar incorretamente o público pode levar ao tratamento indevido de dados de crianças, o que é considerado infração grave sob a COPPA, o GDPR e a LGPD, podendo resultar em multas elevadas ou remoção do app das lojas.

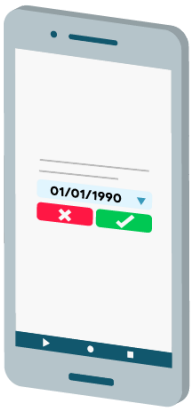
Segundo o programa *Designed for Families* do Google, algumas orientações para definição da faixa etária de forma apropriada envolvem:

- Avaliar o conteúdo, linguagem, mecânicas e estética do jogo;
- Considerar classificações etárias oficiais (IARC, ESRB, PEGI) como referência;
- Realizar testes de usabilidade com públicos diferentes e ajustar o conteúdo conforme necessário.

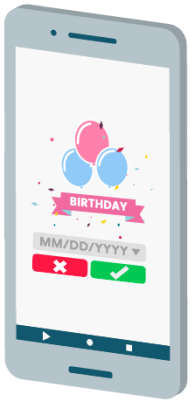
Caso haja público misto (crianças, adolescentes e adultos), torna-se de grande relevância a implementação de uma tela neutra com o objetivo de identificar corretamente o perfil etário (BP 3.3) e, a partir disso, aplicar os níveis adequados de proteção de dados, acesso a funcionalidades e exposição a conteúdos.

Esta tela neutra é uma etapa inicial do aplicativo, apresentada sem indução ou linguagem direcionada, que solicita de forma imparcial informações sobre a idade do usuário — como o mês e o ano de nascimento. Ilustramos na Figura 16 alguns exemplos de design de tela neutra que estão ou não em conformidade.

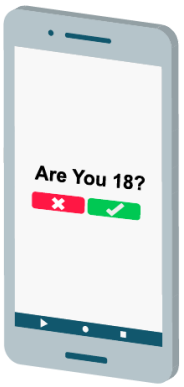
Figura 16 - Exemplos de conformidade para tela neutra.



Não está em conformidade
O desenvolvedor pré-selecionou a data de nascimento do usuário como adulto. O usuário não precisa indicar a idade e pode tocar no botão de marca de seleção para aceitar a informação pré-selecionada.



Em conformidade
O desenvolvedor exige que os usuários selecionem a data de nascimento usando o menu suspenso.



Não está em conformidade
O desenvolvedor perguntou ao usuário se ele tem mais de 18 anos. O usuário não precisa indicar a idade e pode selecionar o botão de marca de seleção para ignorar a tela neutra de informações de idade.

Fonte: *Google Play Developer*

Importante ressaltar que, a depender da faixa etária da criança e do adolescente, essa etapa pode ser facilmente burlada. Isso pode exigir etapas adicionais ou métodos mais rígidos, como validação de dados adicionais, através de informações de pagamento, e-mail ou telefone de maiores responsáveis.

5.2.4 Categoria 4 - Publicidade: geral

A Categoria 4 – Publicidade: geral foi estruturada com base no conceito de que publicidade, numa visão geral, representa qualquer prática ou atividade de *marketing* voltada à promoção de produtos ou serviços (COPPA). Sob essa perspectiva, reunimos três práticas relacionadas a esse tipo de abordagem, apresentadas na Tabela 11 a seguir.

Tabela 11 - Práticas candidatas da Categoria 4 - Publicidade: geral.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP. 4.1	Garantir que todos os SDKs de ads usados são adequados e certificados para crianças e estão em *compliance* com todas as leis aplicáveis.	**X**	**X**	**X**	**X**	**X**		
BP. 4.2	Não usar táticas de publicidade impróprias para crianças, como o remarketing ou a publicidade com base em interesses.				**X**	**X**		
BP. 4.3	Evite usar táticas agressivas de publicidade ou de compras no jogo.				**X**	**X**		

Fonte: Elaboração da autora

Acerca da prática BP 4.1, muitos jogos utilizam uma ampla variedade de SDKs (*Software Development Kits*) e APIs (*Application Programming Interfaces*), sendo que diversos desses componentes realizam a coleta e o compartilhamento de dados dos usuários. Por essa razão, é essencial que desenvolvedores realizem uma avaliação criteriosa das bibliotecas utilizadas, a fim de identificar quais tipos de

dados estão sendo coletados, com que finalidade, e para onde estão sendo transmitidos.

Para melhor adequação e segurança, as plataformas de distribuição de apps orientam integram de SDK de anúncios autocertificados para crianças. De qualquer forma, essa orientação permanece válida para jogos web. Os SDKs de anúncios autocertificados para famílias são bibliotecas de software desenvolvidas por terceiros - geralmente redes de publicidade - que foram declaradamente ajustadas para atender às exigências específicas de proteção infantil.

Aplicativos e jogos direcionados a públicos mistos (crianças, adolescentes e adultos) não podem usar SDKs e APIs que não sejam aprovados para uso em serviços direcionados a crianças, a menos que estejam protegidos por uma tela neutra quanto à idade (Google Play Developer, 2024).

Táticas de publicidade digital, como remarketing e publicidade baseada em interesses, a que se referem a prática BP 4.2, são amplamente criticadas quando aplicadas a crianças, devido ao seu caráter intrusivo e potencialmente exploratório.
O remarketing em jogos funciona como uma estratégia de publicidade digital que visa “reimpactar” usuários que já interagiram com o jogo ou aplicativo anteriormente, mas não realizaram determinada ação, como instalar, realizar uma compra ou voltar a jogar. As Figuras 17 e 18 ilustram, de forma simplificada, como esta estratégia pode ser utilizada para trazer jogadores de volta ao jogo ou até mesmo transformar o jogo em janela de publicidade de produtos de terceiros.

Figura 17 - Esquema de remarketing para resgate de jogadores

Fonte: Elaboração da autora

Figura 18 - Esquema de remarketing para anúncio de produtos

Fonte: Elaboração da autora

Barassi (2020) argumenta que tais práticas expõem as crianças a processos de vigilância comercial contínuos, comprometendo sua privacidade, autonomia e dignidade desde os primeiros anos de vida.

Práticas agressivas de publicidade (BP 4.3) podem ser caracterizadas como práticas, por exemplo, de pressão emocional para conversão (mensagens como "só mais hoje!", "você vai perder essa chance!" ou "todos os seus amigos já compraram"

etc); gatilhos baseados em recompensas sociais ou comparações; e anúncios persistentes e intrusivos (assunto que aprofundaremos no tópico 5.2.5 a seguir).

5.2.5 Categoria 5 - Publicidade: anúncios

Organizamos a Categoria 5 – Publicidade: anúncios com base no conceito de que anúncios são quaisquer peças promocionais exibidos dentro de aplicativos, incluindo banners gráficos, vídeos e outras formas de publicidade voltadas à promoção de produtos ou serviços (*Google Play Store*). Com essa perspectiva, reunimos sete práticas relacionadas a esse tipo de material promocional, apresentadas na Tabela 12 a seguir.

Tabela 12 - Práticas candidatas da Categoria 5 - Publicidade: anúncios.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 5.1	Diferenciar claramente anúncios do conteúdo do app, por exemplo, destacando a monetização e a publicidade no conteúdo do app usando cores e estilos diferentes.				**X**	**X**		Brignull, (2010); Gray et. al. (2018)
BP 5.2	Evitar anúncios invasivos que ocupem a tela inteira ou interfiram no uso normal do app e/ou não oferecem a opção de fechar, após 5 segundos, no máximo.				**X**	**X**		Gray et. al. (2018)
BP 5.3	Evitar mais de um anúncio em uma mesma página ou de forma subsequente.				**X**	**X**		
BP 5.4	Evitar exibir anúncios intersticiais e ofertas para compras no app logo após a abertura. Os usuários precisam experimentar a funcionalidade do seu app ou jogo primeiro.				**X**	**X**		

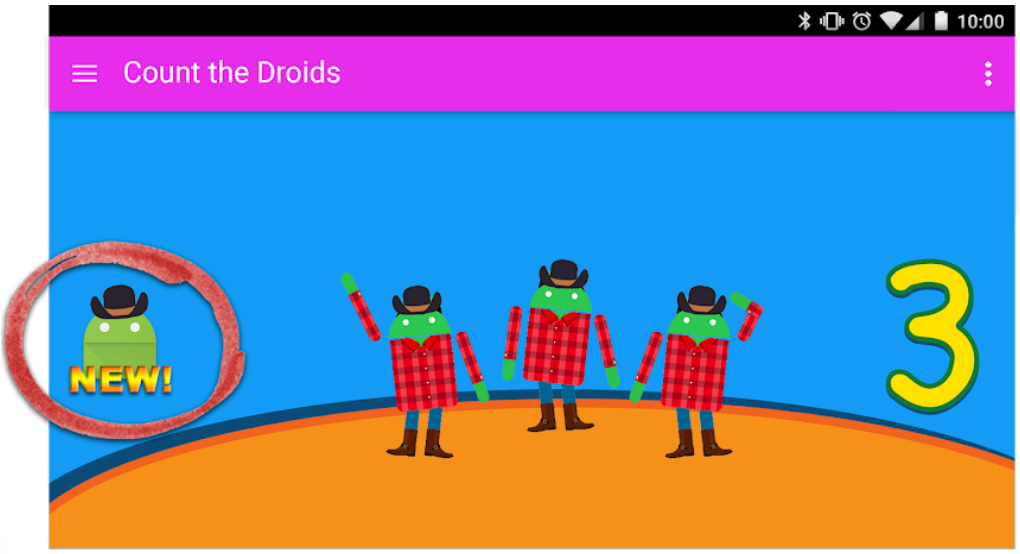
BP 5.5	Evite forçar o jogador a assistir anúncios em troca de recompensas.							Fitton & Read (2019)
BP 5.6	Evite exibir anúncios "intertisitial" de conteúdos fora do contexto do jogo.							Fitton & Read (2019)
BP 5.7	Evite exibir anúncios em formatos e conteúdos impróprios para a faixa etária do seu público				**X**	**X**		Fitton & Read (2019)

Fonte: Elaboração da autora

De forma geral, os anúncios exibidos em jogos que englobam público infantil não devem ser estruturados de maneira que induza ao clique acidental por parte de crianças ou adolescentes. A exibição de anúncios, nesse contexto, requer o cumprimento de critérios específicos, conforme estabelecido por políticas de plataformas de distribuição. As práticas apresentadas, nesta categoria, fazem referência a uma série de formatos de exibição consideradas impróprias para crianças, segundo indica orientações do *Google Play Console*:

Ao observar a tela do jogo, o usuário também deve ser capaz de distinguir, visualmente, os anúncios publicitários do conteúdo nativo do jogo (BP 5.1). A Figura 19 ilustra, por exemplo, um caso em que os elementos visuais nativos do jogo são utilizados de forma indevida para direcionamento de formatos publicitários. Assim, recursos como *offerwalls* e experiências de anúncio imersivas que confundem o usuário quanto à sua natureza comercial também são considerados problemáticos.

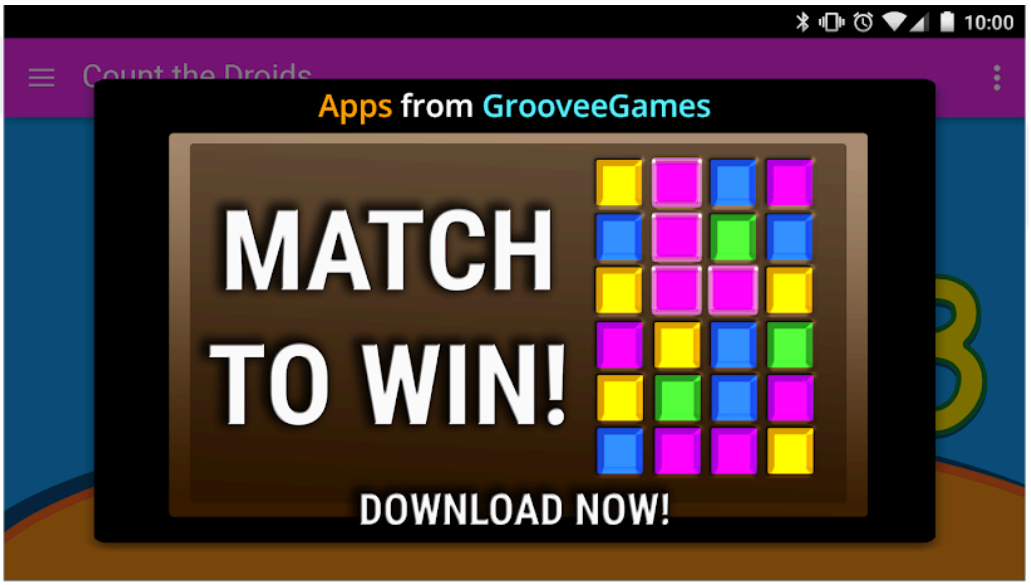
Figura 19 - Exemplo de anúncio com uso de conteúdo nativo do jogo



Fonte: *Google Play Developer,* 2024

Anúncios que ocupam a maior parte da tela (Figura 20) são considerados invasivos, interferem no uso normal do aplicativo e, frequentemente, não apresentam um botão claro para fechamento, por isso são considerados problemáticos (BP 5.2). Sempre deve ser possível fechar os anúncios após cinco segundos. Anúncios enganosos, que utilizam elementos como botões “fechar”, mas que, na prática, acionam outro anúncio. Podemos dizer que isso caracteriza um caso de *dark pattern* do tipo *bait and switch* (Gray et. al. 2018).

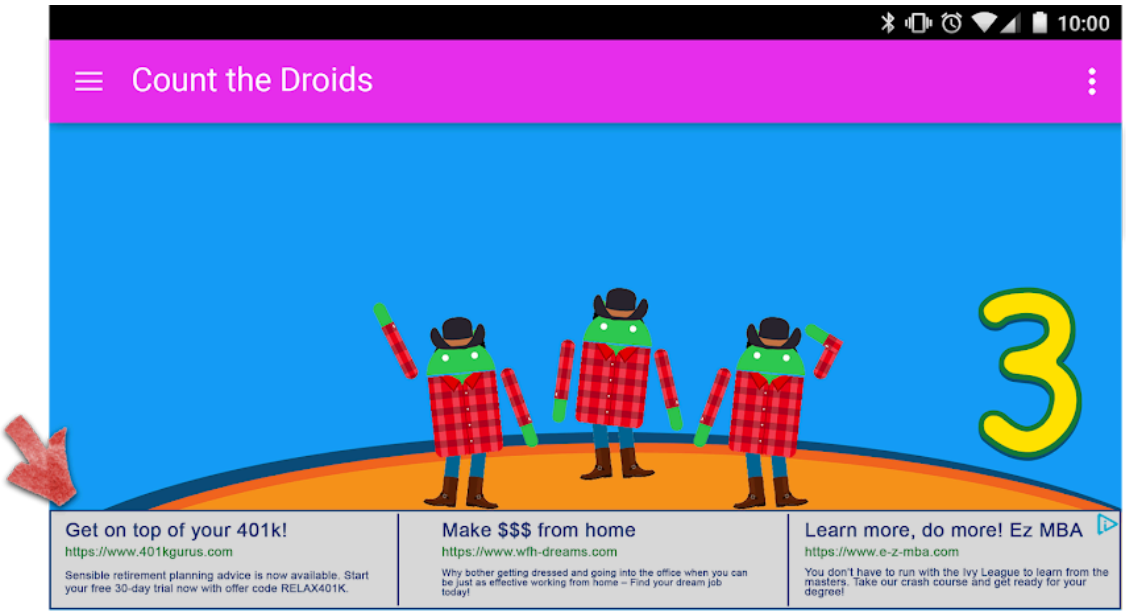
Figura 20 - Exemplo de anúncio invasivo



Fonte: *Google Play Developer*

Da mesma forma, considera-se que a inserção de múltiplas posições de anúncio em uma mesma tela (Figura 21), como a exibição simultânea de diversos banners ou vídeos publicitários (BP 5.3) e a publicidade *intersticial*, exibida imediatamente após a abertura do aplicativo (BP 5.4) interrompem a experiência fluida do usuário.

Figura 21 - Exemplo de anúncios múltiplos na mesma tela

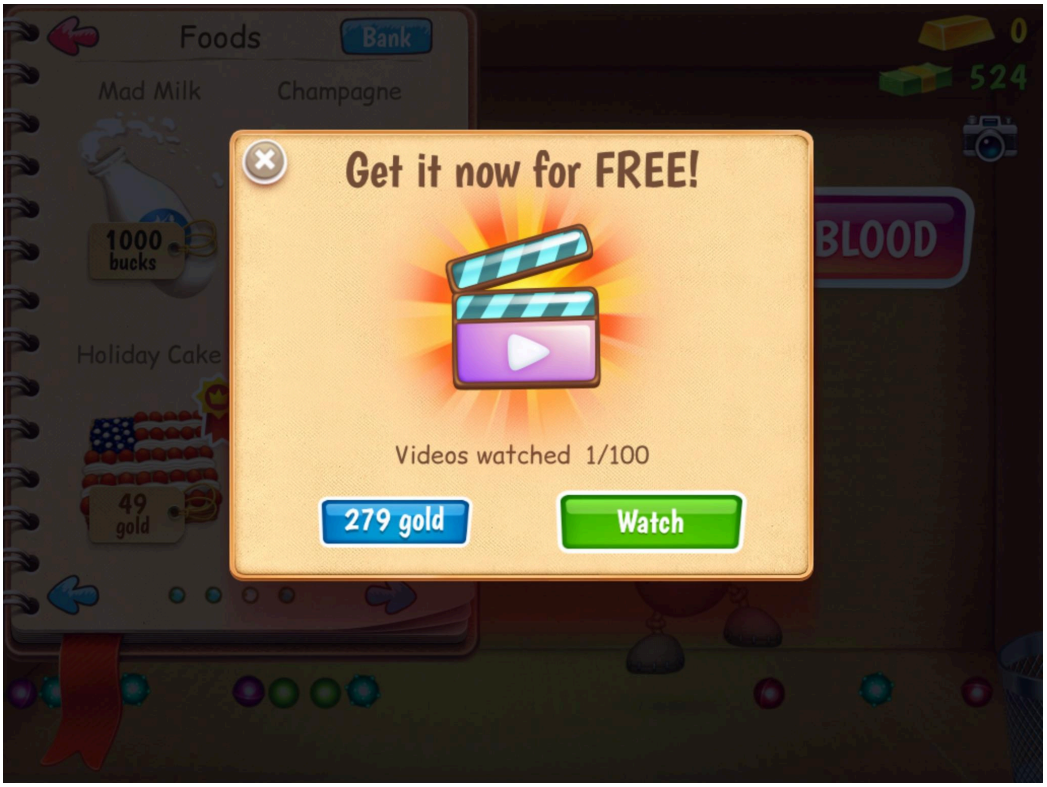


Fonte: *Google Play Developer*, 2024

Jogos, frequentemente, forçam os jogadores a assistir anúncios em vídeo para ganhar vidas, moedas ou desbloquear conteúdos, sem oferecer alternativas viáveis dentro do jogo, o que contraria a recomendação da prática BP 5.5. Na análise de Fitton & Read (2019), os adolescentes relataram frustração com anúncios que interrompem e bloqueiam o fluxo do jogo até serem concluídos.

Um exemplo abusivo desta má prática está no jogo *Kick the Buddy*, popular entre o público mais jovem. O jogo sugere que o jogador tem a possibilidade de assistir 100 anúncios para conseguir um item, forçando assim ou o gasto de moedas virtuais ou a exibição de anúncios (Figura 22).

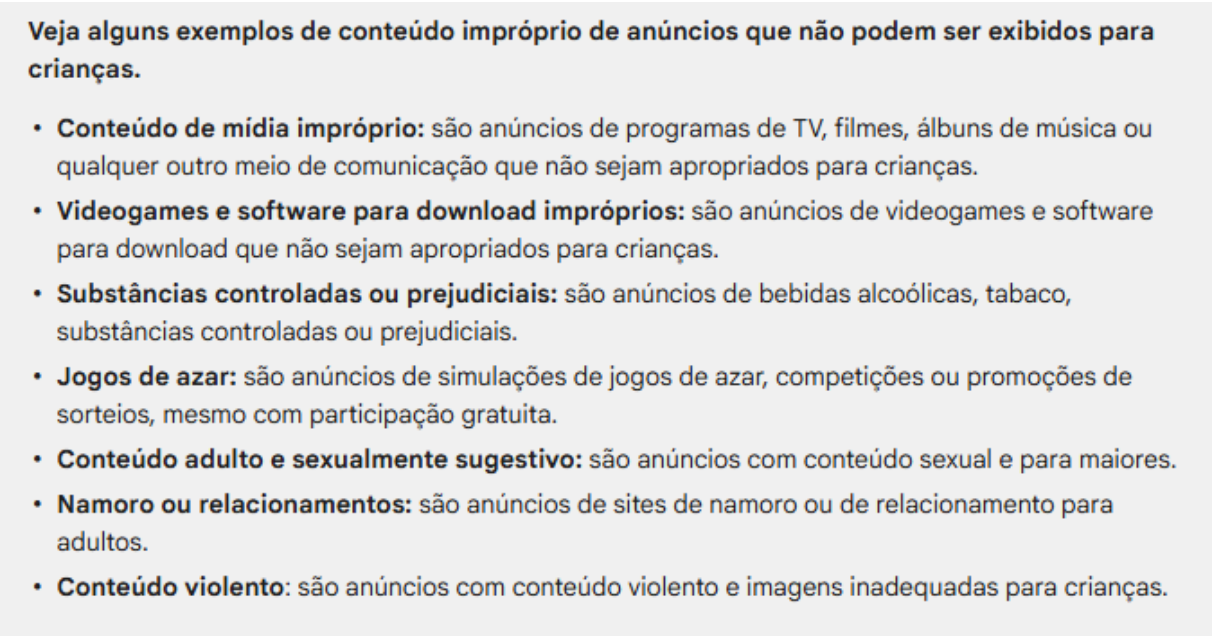
Figura 22 - Exemplo de *dark pattern* no jogo *Kick the Buddy*



Fonte: Reddit

Sobre a prática BP 5.6 e 5.7, a Figura 23 apresenta alguns tipos de conteúdos consideradas impróprias para usuários menores de 13 anos:

Figura 23 - Conteúdos impróprios de anúncios para crianças



Fonte: *Google Play Console,* 2024

No estudo de Fitton & Read (2019), adolescentes relataram serem impactados por anúncios de sites de namoro e conteúdos sensuais, dentro de jogos casuais, como *Episode* e *Love Island*.

Mesmo em jogos voltados ao público adulto, todos os formatos analisados até aqui, ainda podem ser considerados como padrões invasivos. Para esse público, no entanto, sua veiculação tende a ser mais aceita e flexibilizada. Assim, nos casos em que o jogo é destinado, exclusivamente, a menores de 13 anos, esses formatos são expressamente proibidos. Já quando o público-alvo inclui tanto crianças quanto adultos, essas restrições se aplicam apenas na veiculação de anúncios para menores ou para usuários cuja idade não pode ser determinada. Essa adequação de formatos e conteúdos deve ser feita através da tela neutra, mencionada no tópico 5.2.3.

5.2.6 Categoria 6 - Compras *in-game*

A Categoria 6 – Compras *in-game* foi organizada com base no conceito de que essas transações referem-se a operações monetárias realizadas dentro dos aplicativos, que permitem aos usuários acessar conteúdos ou recursos adicionais, como itens virtuais em jogos, assinaturas e upgrades premium (Google Play Store). Com base nesse entendimento, reunimos oito práticas relacionadas a esse tipo de transação, apresentadas na Tabela 13 a seguir.

Tabela 13 - Práticas candidatas da Categoria 6 - Compras in-game.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP. 6.1	Evite dificultar o cancelamento de compras ou assinaturas dentro do jogo.							Brignull (2010); Gray et al. (2018)
BP. 6.2	Evite demora para informar ao jogador que ele poderá ter custos adicionais por conta de alguma ação ou do seu engajamento.							Brignull, (2010); Gray et al. (2018); Fitton & Read (2019)
BP. 6.3	Evite adicionar itens não selecionados pelo jogador ao carrinho de compras dele. Exemplo: compra casada							Brignull (2010); Gray et al. (2018)
BP. 6.4	Evite sugerir compras ao jogador com base em compras anteriores.							Zagal et. al. (2013); Gray et al. (2018); Neely (2021)
BP. 6.5	Os usuários precisam conseguir diferenciar claramente "moedas" do jogo de valores monetários reais.				**X**			Gray et al. (2018); Fitton & Read (2019)
BP. 6.6	Evite induzir o jogador a pagar um valor monetário para acelerar ou melhorar seu progresso no jogo							Gray et al. (2018); Fitton & Read (2019)

BP. 6.7	Evite cobrar do jogador, além do valor pago inicialmente, algum outro valor adicional para que ele tenha acesso a features extras							Gray et al. (2018); Zagal et al. (2013)
BP. 6.8	Evite apresentar features de compras, de forma hierárquica, ao invés de paralelas, sugerindo que uma opção é melhor que a outra.							Gray et al. (2018)

Fonte: Elaboração da autora

Segundo Gray et al. (2018), as práticas indevidas de dificultar o cancelamento de compras ou assinaturas dentro do jogo (abordado na BP 6.1) e de não diferenciar claramente "moedas" do jogo de valores monetários reais (abordado na BP 6.5) relacionam-se à categoria denominada *Obstruction*.

Esta categoria refere-se a situações em que o processo é, propositalmente, tornado mais difícil do que o necessário, com o objetivo de desencorajar uma ação específica por parte do usuário, por exemplo, incluindo muitos passos para conclusão do mesmo (Figura 24). O design da interface é estruturado de modo a frustrar tentativas de cancelamento, ocultando opções, exigindo múltiplos passos ou apresentando alertas ambíguos que induzem à hesitação.

Figura 24 - Exemplo de Obstruction do iOS6 para limitar o rastreio de *ads*

Fonte: Gray, 2018.

Já no caso de *Obstruction* em contexto de compras (abordado em BP 6.5), a intenção é desconectar o jogador da noção de valor monetário real, induzindo a uma interação menos crítica com moedas virtuais, o que pode levar ao gasto inadvertido de recursos financeiros reais — especialmente prejudicial quando envolve usuários em desenvolvimento cognitivo, como crianças.

A Figura 25 ilustra um exemplo de interface de loja dentro de um jogo, onde os usuários compram UC (uma moeda virtual) utilizando dinheiro real (valores exibidos em reais). O design visual e de valor das moedas virtuais é tão similar aos dos valores monetários reais que pode gerar confusão, induzindo os jogadores a comprarem pacotes maiores com bônus (ex.: “FREE 50” ou “FREE 950”), criando a impressão de maior valor e incentivando gastos além do planejado. Especialmente porque a conversão entre reais e moedas virtuais não é intuitiva e exige cálculos mentais constantes.

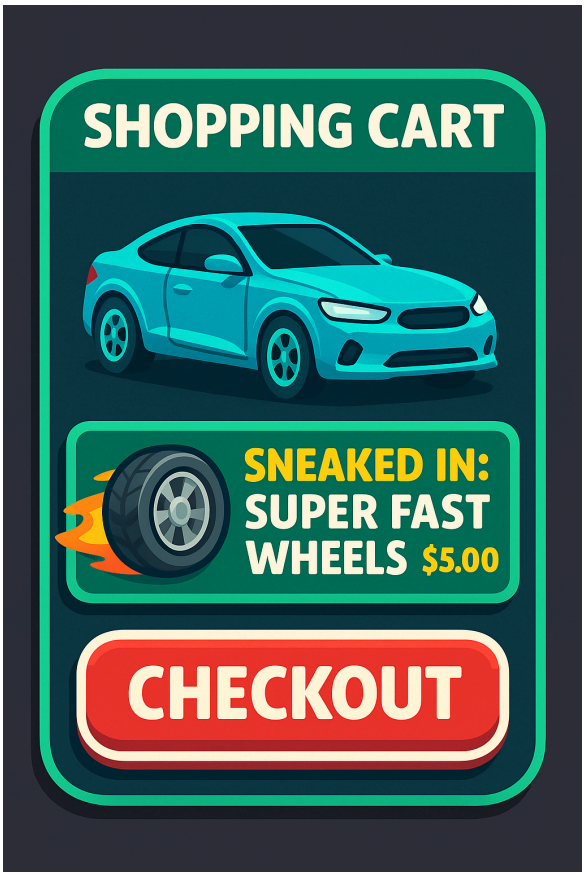
Figura 25 - Exemplo ilustrativo de padrão *Obstruction* no contexto de compras

Fonte: *Dark Side of UX*- Zeux Innovation, 2022.

Por sua vez, as práticas BP 6.2, BP 6.3 e BP 6.7 visam evitar padrões da categoria “*Sneaking"*, descrito por Gray et al. (2028) quem tem como propósito ocultar, disfarçar ou postergar a divulgação de informações relevantes ao usuário.

Essas táticas comprometem a clareza na comunicação de custos, levando o jogador a tomar decisões de compra sem plena consciência dos ônus envolvidos (Figura 26).

Figura 26 - Exemplo de prática *sneaking* em compra casada de itens



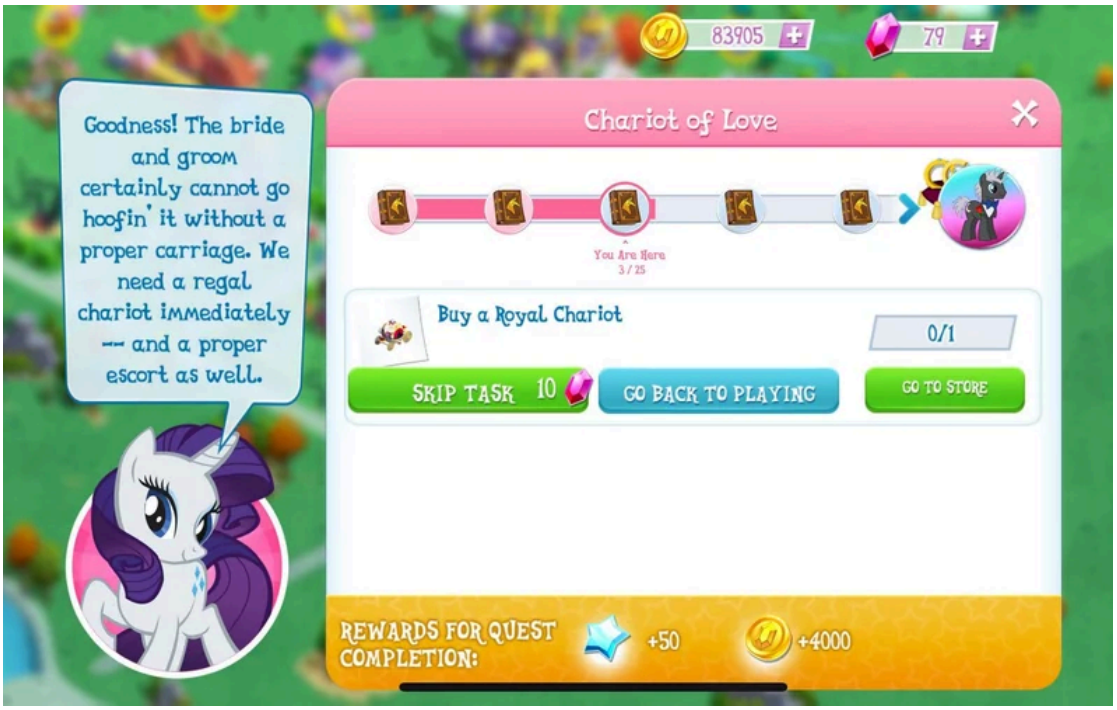
Fonte: Elaboração da autora

A prática BP 6.6 envolve evitar a indução ao pagamento para acelerar ou melhorar o progresso no jogo (modelo conhecido como *pay to skip ou pay to progress*), é duramente criticada por Zagal et al. (2020), por introduzir uma lógica de desigualdade entre jogadores pagantes e não pagantes, desequilibrando a experiência lúdica em favor da monetização. Por exemplo, *FarmVille* estimula que jogadores paguem para evitar esperar pela colheita ou pela ajuda de outros jogadores (Figura 27); assim como *My Little Pony*, jogo focado público jovens, induz o jogador a pagar por um item que apresenta como essencial para seu progresso (Figura 28).

Figura 27 - Exemplo de padrão *Pay to skip* em *FarmVille 2*

Fonte: Reddit

Figura 28 - Exemplo de *Pay to progress* em *My Little Pony*

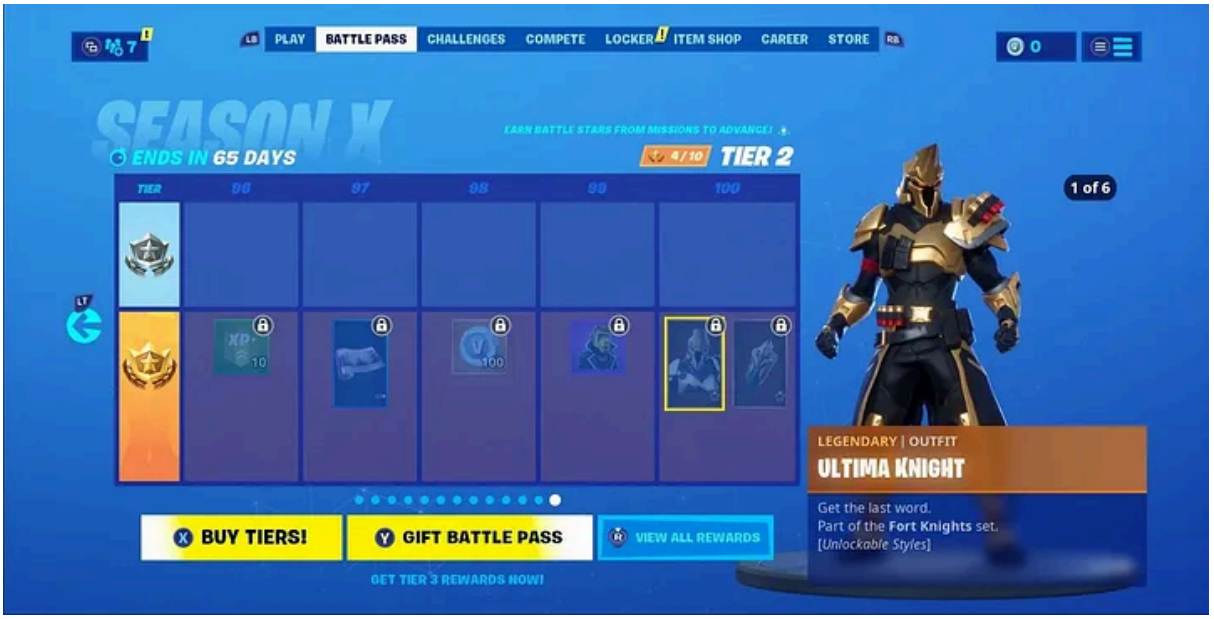


Fonte: Reddit

Para Fitton e Read (2019), trata-se de uma forma de pressão indireta ao consumo, na qual barreiras artificiais são criadas propositalmente para que o dinheiro real seja percebido como solução imediata, comprometendo a fluidez e o mérito do progresso *skill-based*.

A prática BP 6.7 desencoraja cobranças extras específicas para que o jogador possa usufruir de uma experiência completa, fato bastante recorrente em jogos *massively multiplayer online* (MMO), por exemplo, *Fortnite*, que oferece compras de passes de batalhas ou passes para eventos no jogo (Figura 29). “Após a compra, os jogadores têm um tempo limitado para desbloquear todas as recompensas. Isso os incentiva a continuar jogando e acumulando até que todas as recompensas sejam coletadas, caso contrário, seu dinheiro seria, aparentemente, desperdiçado” (Manker, 2023).

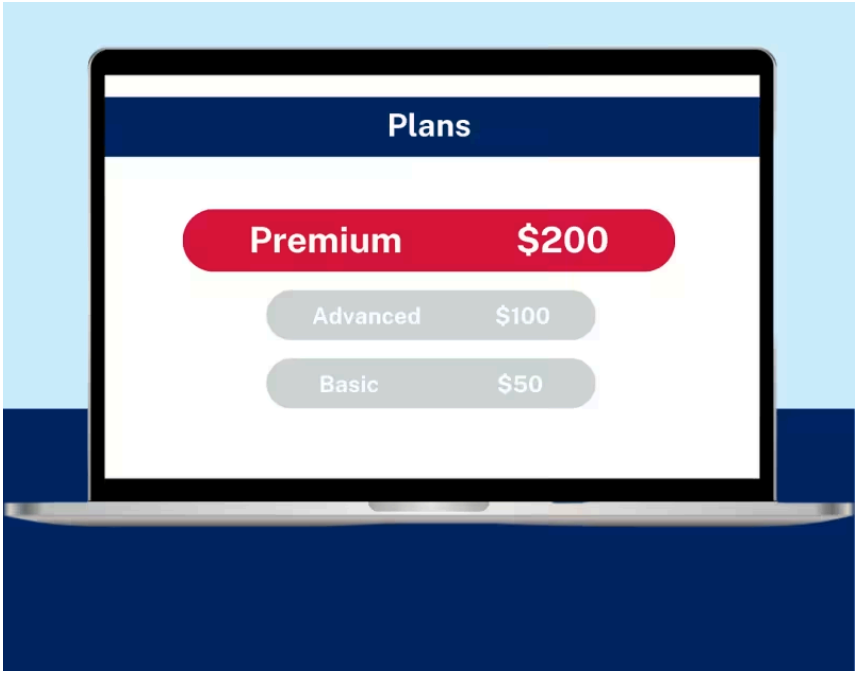
Figura 29 - Interface de passe de batalha no *Fornite Season 10*



Fonte: IGN, 2019.

Por fim, a prática BP 6.8, destaca que a apresentação hierárquica de funcionalidades de compra — em vez de uma disposição paralela e neutra —, representa, segundo Gray et al. (2018), uma forma de manipulação da interface do usuário, onde determinadas opções são destacadas visual ou interativamente em detrimento de outras (Figura 30).

Figura 30 - Exemplo ilustrativo de *dark pattern* de falsa hierarquia



Fonte: NSW Government

Essa técnica induz o jogador a acreditar que determinada escolha é superior ou única, comprometendo a equidade no processo de decisão e violando o princípio de neutralidade no *design* de escolhas.

5.2.7 Categoria 7 - *Game design*: geral

A Categoria 7 – *Game design*: geral foi organizada com base no entendimento de que game design, em uma perspectiva ampla, refere-se à criação de mecânicas e sistemas de jogo voltados à construção de experiências envolventes, as quais, por meio de decisões de *design*, podem influenciar o comportamento dos jogadores (Zagal et al, 2013). A partir desse conceito, reunimos seis práticas relacionadas a esse processo, apresentadas na Tabela 14 a seguir.

Tabela 14 - Práticas candidatas da Categoria 7 - Game design: geral.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 7.1	Evitar pressionar o jogador a jogar recorrendo ao sentimento de que, caso não o façam, estarão perdendo recompensas ou em desvantagem em relação a outros jogadores.				**X**			Zagal et al (2013); Fitton & Read (2019)
BP 7.2	Evite estimular ações e comportamentos no jogo que, na vida real, seriam considerados antiéticos.							Gray et al. (2018)
BP 7.3	Evite exigir ao jogador períodos de tempo ou datas específicas para jogar, dando flexibilidade ao jogador							Zagal et al. (2013)
BP 7.4	Evite exigir que o jogador realize tarefas monótonas de forma recorrente para progredir no jogo							Zagal et al. (2013)
BP 7.5	Evite deixar qualquer opção de feature pré-selecionada, influenciando a escolha do jogador.							Gray et al. (2018)
BP 7.6	Evite fazer perguntas enganosas que possam ter duplo sentido ou interpretação ambígua.							Brignull (2010); Gray et al. (2018)

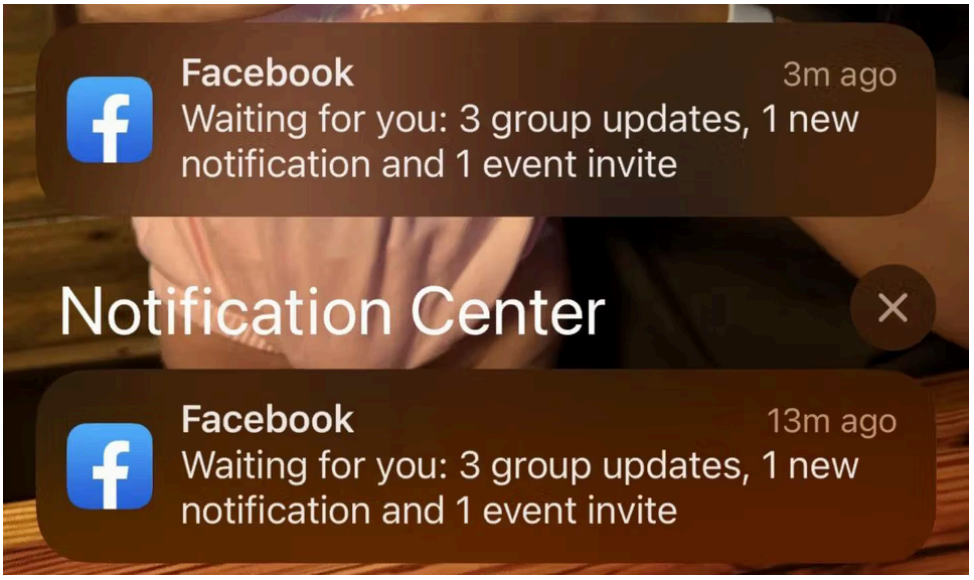
Fonte: Elaboração da autora

Fitton e Read (2019) aprofundam a discussão acerca dos conceitos nesta categoria. A prática BP 7.1, que tratar sobre evitar pressionar o jogador a jogar recorrendo a determinados sentimentos, é classificada pelos autores como uma forma de pressão comportamental indireta, comumente associada ao conceito de FOMO (Fear of Missing Out).

A grande maioria dos aplicativos, atualmente, criam o medo de perder algo, ao insinuar que algo está acontecendo enquanto você está *offline*, mas sem explicar em detalhes o que isso significa (Figura 31); ou sugerem que o jogador será

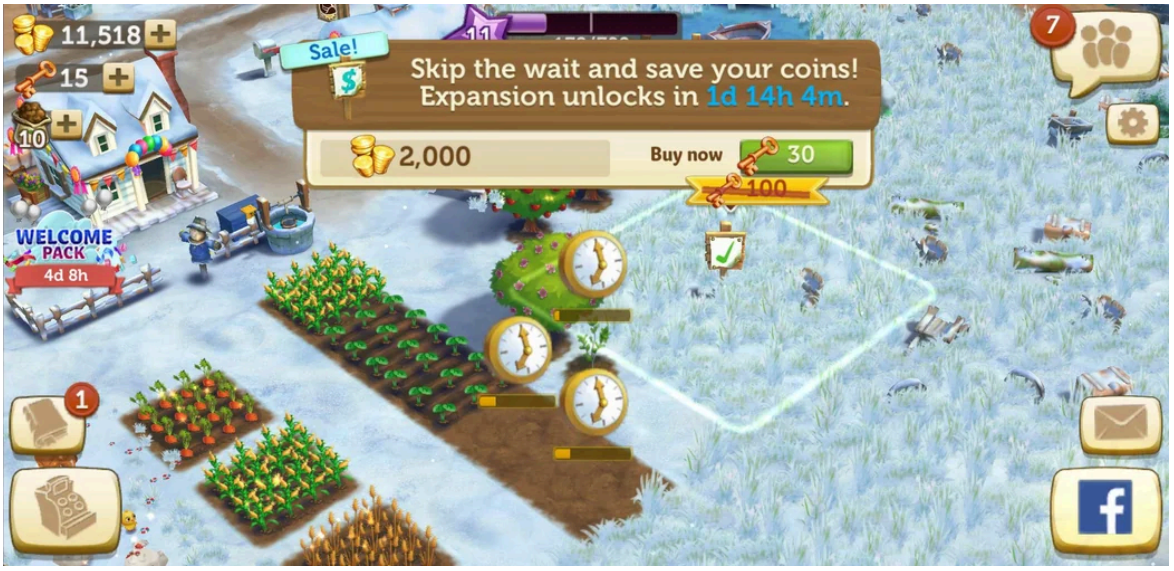
penalizado, por exemplo, perdendo moedas, caso não realize determinada ação (Figura 32).

Figura 31 - Exemplo de manipulação do jogador por notificações do *Facebook*



Fonte: Reddit

Figura 32 - Exemplo de manipulação do jogador em *FarmVille*



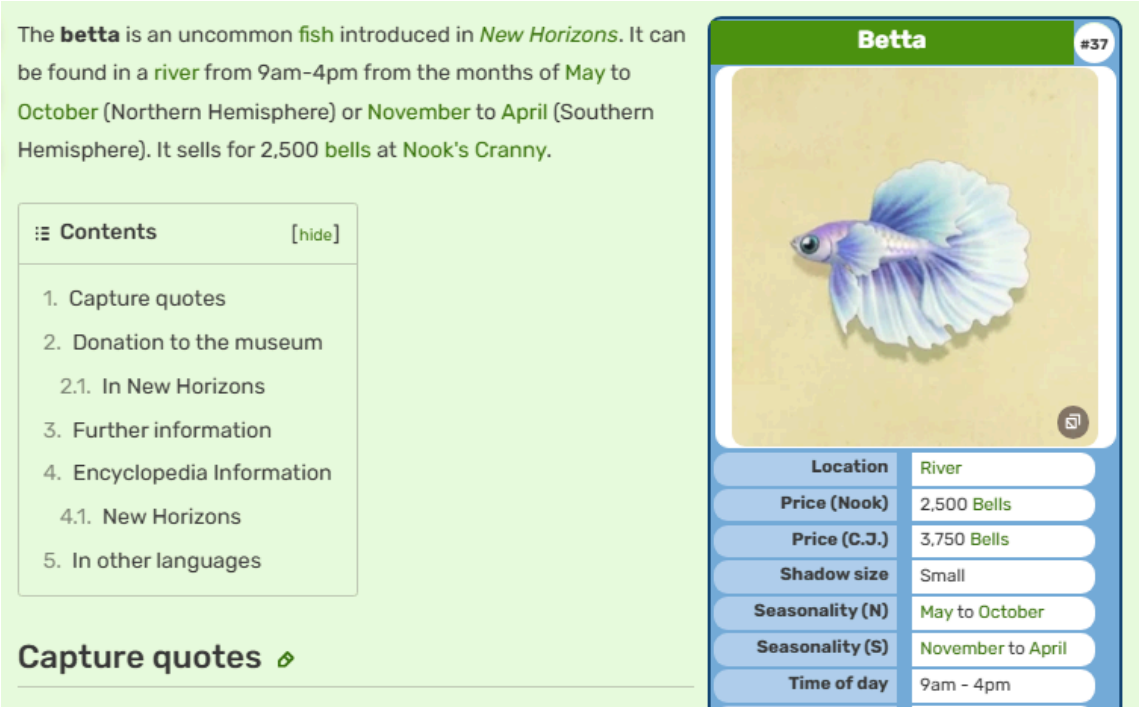
Fonte: Reddit

A prática BP 7.3 faz referência a inibir *game features* que, de acordo com a literatura, se enquadram na categoria *Temporal* de *dark patterns*, como exigir do jogador jogar em datas específicas. Jogos que impõem janelas fixas de tempo para

progressão ou eventos obrigatórios limitam a autonomia do jogador, podendo ser considerado um design não ético.

Por exemplo, o jogo *Animal Crossing: New Horizons* leva isso ao extremo, com o cronômetro do jogo sincronizado com a data e a hora no seu console. Certos tipos de peixes - como por exemplo, o *Betta* - só podem ser encontrados em uma determinada hora em determinados meses do ano, por hemisfério (Figura 33).

Figura 33 - Exemplo de *temporal dark pattern* em *Animal Crossing*



Fonte: Animal Crossing Fandom Wiki

Exigir que o jogador realize tarefas monótonas de forma recorrente para progredir no jogo - relativo ao que a prática BP 7.4 busca evitar - caracteriza-se como um padrão conhecido como *Grinding*. Fitton e Read (2019) criticam essa prática por representar uma forma de cansaço cognitivo imposto como barreira artificial ao progresso, podendo transformar o jogo em uma experiência tediosa e frustrante ao jogador. Por exemplo, *Pokémon GO* obriga o jogador a capturar os mesmos Pokémons - disfarçados por pequenas variações de nome e nível de combate - para evoluir ou melhorar outros (Figura 34).

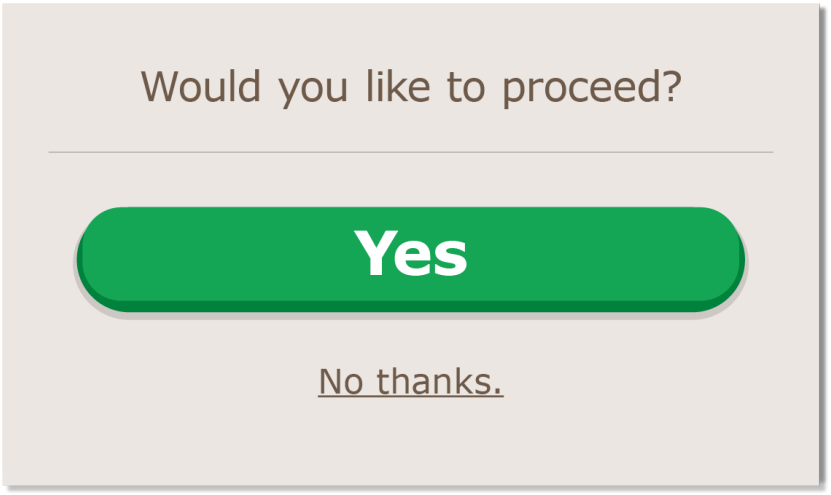
Figura 34 - Exemplo de padrão *Grinding* em *Pokémon Go*

Fonte: Dakinedi, 2016.

A prática BP 7.5 aborda o tópico referente ao uso de técnicas de *nudge* no design de interfaces. Essas técnicas consistem em estratégias de design que direcionam o comportamento do usuário, entretanto, se utilizadas de forma indevida, leva os usuário a tomar decisões alinhadas aos interesses do designer, muitas vezes de forma sutil e não consciente (THALER & SUNSTEIN, 2008).

Um exemplo clássico pode ser observado no Figura 35, em que o botão verde com a opção “sim” é visualmente destacado, enquanto a alternativa “não” aparece em letras pequenas e pouco visíveis. Essa assimetria de apresentação atua como um “empurrão” psicológico, induzindo o usuário a escolher “sim”, ainda que essa não fosse sua intenção inicial.

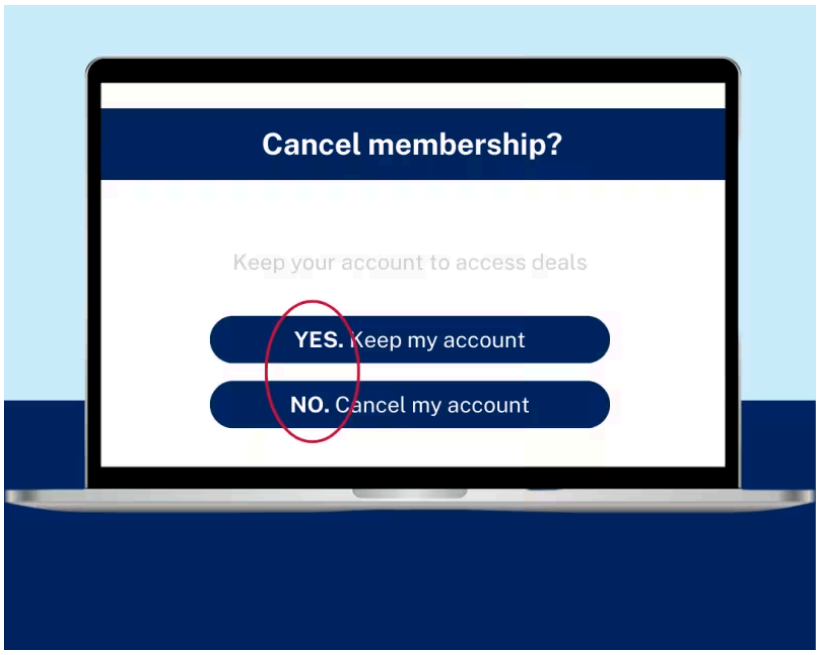
Figura 35 - Exemplo de interface com uso de *nudge* indevido



Fonte: ICO,2024

A prática BP 7.6 busca inibir o uso de perguntas ambíguas ou mal formuladas como uma forma de *dark pattern* verbal, que visa gerar confusão e induzir o jogador a escolhas não intencionais. Conforme caracterizado por Gray et al. (2018), esse padrão se enquadra na categoria *dark pattern* de *Trick question* e inclui uma pergunta que aparenta sugerir uma coisa, mas prática é outra; ou utiliza uma linguagem confusa, negativas duplas ou expressões direcionadas com o intuito de manipular as interações do usuário (Figura 36).

Figura 36 - Exemplo ilustrativo de *dark pattern Trick question*



Fonte: NSW Government

5.2.8 Categoria 8 - *Game design*: recompensas

Estruturamos a Categoria 8 – *Game design*: recompensas com base no entendimento de que recompensas, dentro dos jogos, são benefícios concedidos aos jogadores quando realizam determinadas ações ou alcançam objetivos específicos durante a experiência de jogo (Zagal, 2013). A partir desse conceito, reunimos quatro práticas relacionadas diretamente a essa *feature*, apresentadas na Tabela 15 a seguir.

Tabela 15 - Práticas candidatas da Categoria 8 - Game design: recompensas.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 8.1	Não condicionar o acesso ou recompensa da criança à divulgação de informações pessoais a mais do que o necessário.	**X**	**X**	**X**				
BP 8.2	Evite recompensar o jogador de forma aleatória ou inesperada para viciá-lo no jogo. Preferir recompensas regulares e previsíveis							Neely (2021)
BP 8.3	Evite oferecer recompensas ao jogador ou penalizá-lo em função dele(a) jogar diariamente							Zagal et al. (2013); Neely (2021)
BP 8.4	Evite usar recursos de recompensas como loot boxes, gambling ou quaisquer outros que possam ser classificados como jogos de azar						**X**	Neely (2021)

Fonte: Elaboração da autora

Sobre a prática BP 8.1, podemos dizer que todas as legislações de proteção à privacidade convergem, em proibir, de forma direta ou indireta, a prática de condicionar o acesso de crianças a funcionalidades ou recompensas à entrega de dados pessoais além do necessário. A COPPA, no entanto, é a mais explícita sobre esse ponto, ao vedar expressamente a coleta como condição para participação em jogos ou prêmios (COPPA, § 312.5(c)).

As práticas BP 8.2 e BP 8.4 alertam para o uso de sistemas de recompensa de forma aleatória ou fazendo uso de recursos com *loot box* e *gambling* como mecanismos de monetização predatória que exploram vulnerabilidades cognitivas e emocionais (NEELY, 2021), como mencionado no tópico 4.5.2. Tais estratégias, segundo a autora, desviam o foco do jogo da experiência lúdica para um ciclo de tentativa-recompensa viciante, afetando diretamente a autonomia do jogador e favorecendo padrões de dependência, semelhantes a jogos de azar.

Por exemplo, em *Overwatch 1*, *loot boxes* pagas com dinheiro real eram comuns (Figura 37). Contudo, após sofrer o jogo retaliações por associação a jogos de azar, esta *feature* foi banida, sendo, atualmente, estritamente cosmética, não alterando o gameplay e relacionadas a eventos sazonais (Zendle et. al, 2019).

Figura 37 - Tela de *loot boxes* compradas com dinheiro em *Overwatch 1*

Fonte: Reddit

Apesar disso, ainda há um forte incentivo psicológico: skins raras podem existir apenas em certos pacotes, disparando o mecanismo de recompensa aleatória que estimula repetição e gastos. Os desenvolvedores devem priorizar o desenvolvimento de sistemas de recompensas baseados em previsibilidade e estatística. Diferente de mecânicas aleatórias extremas, como *loot boxes*, sistemas de recompensa previsíveis e estatisticamente equilibrados oferecem ao jogador uma percepção de controle e justiça (BAUER & KINDER-KURLAND, 2021).

Ao aplicar modelos probabilísticos transparentes e ajustáveis, o game designer cria *loops* de progressão baseados em meritocracia e aprendizado, reduzindo frustrações e promovendo uma experiência mais alinhada ao conceito de *player-centered design* (SICART, 2008).

Mecânicas que penalizam ou recompensam jogadores com base em sua frequência de jogo (inibida pela prática BP 8.3) também são exemplos de design que promove comportamentos compulsórios em detrimento da liberdade de escolha (NEELY, 2021).

Recompensas diárias são uma feature comum em jogos online. Na maioria das vezes, o jogador precisa entrar em um jogo todos os dias para receber uma recompensa, como por exemplo, em *Brawl Stars* (Figura 38).

Figura 38 - Tela de recompensas diárias de login do *Brawl Stars*

Fonte: BrawlStarsLeak1, Twitter, 2022.

A cada dia que o jogador entra no jogo em sequência, melhor é a recompensa. Se um jogador perder um dia, não receberá a recompensa e poderá ter que recomeçar a sequência. Contudo, a recomendação de boa prática é de que o desenvolvedor deve sempre buscar priorizar a autonomia do jogador em decidir quando jogar.

5.2.9 Categoria 9 - *Game design: social features*

A Categoria 9 – *Game Design: social features* foi organizada com base na perspectiva de que social features, dentro dos jogos, referem-se a elementos de design que envolvem ou incentivam a interação entre jogadores (ZAGAL, 2013). A partir desse conceito, reunimos três práticas diretamente relacionadas a esse tipo de funcionalidade, apresentadas na Tabela 16 a seguir.

Tabela 16 - Práticas candidatas da Categoria 9 - Game design: social features.

		FONTE COLETADA						
ID	**PRÁTICA**	**COPPA**	**GDPR**	**LGPD**	**Google Play**	**App Store**	**PL 2628/22**	**Dark Patterns**
BP 9.1	Evite incentivar os jogadores a convidar amigos para ingressarem no jogo em troca de recompensas							Zagal et al. (2013); Gray et al (2018); Fitton & Read (2019)
BP 9.2	Evite forçar os jogadores a jogarem recorrendo ao sentimento de culpa ou senso de responsabilidade com amigos e/ou equipe dentro do jogo				**X**	**X**		Zagal et al. (2013); Gray et al (2018); Fitton & Read (2019)
BP 9.3	Evite enviar aos jogadores mensagens não solicitadas comunicando ações em nome de seus amigos ou sua rede de contatos							Zagal et al. (2013); Fitton & Read (2019)

Fonte: Elaboração da autora

Enfocando o contexto geral da categoria, é importante ressaltar que aplicativos e recursos com funcionalidades sociais que envolvam o compartilhamento de informações entre usuários requerem atenção especial no contexto da proteção infantil.

Torna-se necessário, portanto, implementar mecanismos de controle parental. Qualquer funcionalidade que envolva a troca de informações pessoais por parte da criança deve ser condicionada à ação prévia de um adulto responsável (ver Categoria 2 - Controle parental). Essa “ação de um adulto” refere-se a uma uma etapa projetada - em caráter de *parental gate* (já mencionado no tópico 5.2.2) - para verificação da idade do usuário, evitando que crianças forneçam dados falsos para acessar áreas destinadas a adultos, como por exemplo: solicitação de PIN ou senha dos pais, verificação por e-mail, uso de documento oficial ou dados de cartão de crédito para validação. (*Google Play Console*, 2024).

Sob a perspectiva dos *design dark patterns*, práticas como incentivar convites a amigos em troca de recompensas (inibida pela prática BP 9.1), estimular a

continuidade do jogo com base em culpa social (inibida pela prática BP 9.2) ou enviar mensagens não solicitadas em nome de contatos (inibida pela prática BP 9.3) representam formas de manipulação emocional, que comprometem a autonomia do usuário e violam princípios fundamentais de design ético.

Esses padrões são estruturados para explorar pressões sociais e sistemas de recompensa emocional para maximizar métricas de engajamento, frequentemente às custas do bem-estar do usuário (GRAY et al., 2018).

Empregar incentivar convites a amigos em troca de recompensas (BP 9.1) e estimular a continuidade do jogo com base em culpa social (BP 9.2) enquadram-se na categoria de *dark pattern* nomeado como *Social Capital based*. Esse tipo de padrão, muitas vezes, explora redes sociais como vetores de expansão do serviço, instrumentalizando as relações pessoais do jogador como recurso de monetização (GRAY et.al, 2018). No caso de jogos voltados ao público mais jovem, tal prática assume caráter ainda mais problemático, ao se apropriar de vínculos afetivos e da busca por pertencimento, aspectos centrais do desenvolvimento social de crianças e adolescentes.

Por exemplo, *FarmVille* exige que o jogador tenha “vizinhos” para que haja progresso perceptível em algumas áreas. Desta forma, eram constantemente encorajados a convidar amigos para receber energia, moedas, desbloquear fases ou ganhar bônus (Figura 39) . Alguns itens ou ações eram bloqueados a menos que o jogador convidasse um número mínimo de contatos (Zagal, 2018).

Figura 39 - Exemplo de *dark pattern Social Capital Based*, em *Farmville 2*

Fonte: Reddit

Outra prática perigosa, mencionada em BP 9.2, é a estratégia de manipulação emocional, gerando culpa e senso de responsabilidade no jogador. Por exemplo, O jogo *Animal Crossing* faz uso dessa estratégia de forma explícita, através de diálogos e reações de personagens NPC (Figura 40). Não apenas isso. Segundo relato de um jogador, em seu blog no artigo *My Love/Hate Relationship with Animal Crossing's Real Time Gameplay* (2018)*:*

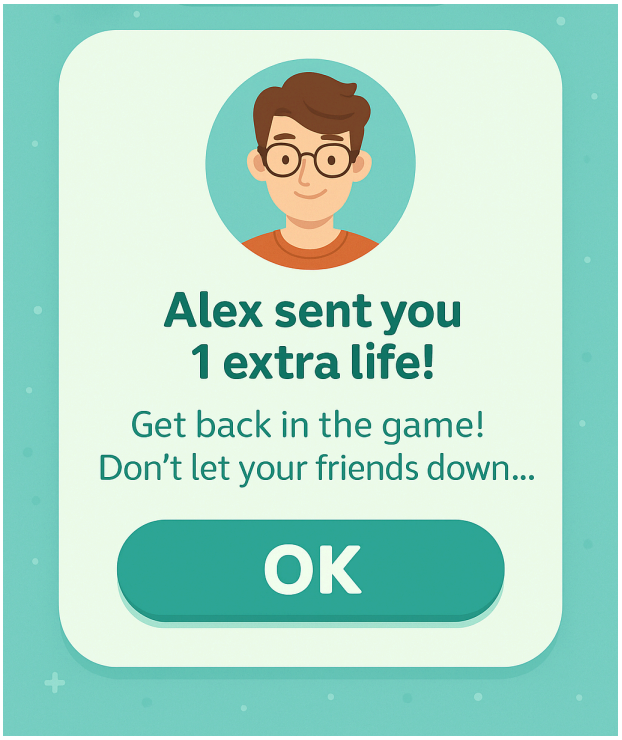
> Sempre que você passa um dia inteiro sem jogar, isso começa a ter efeitos negativos no seu jogo. Esses efeitos se acumulam quanto mais dias consecutivos você passa sem jogar. Ervas daninhas crescem, plantas morrem, baratas entram na sua casa e os moradores da cidade ficam frustrados e até vão embora (Ian, 2018).

Figura 40 - Exemplos de manipulação psicológica em *Animal Crossing*

Fonte: Manker, 2023; Ian, 2018.

O envio de mensagens não solicitadas que comunicam ações em nome de amigos ou contatos da rede do jogador (inibida pela prática BP 9.3) configura um padrão conhecido como *friend spam* ou *impersonation* (Figura 41). Trata-se de uma estratégia em que o jogo simula ações de outros usuários que nunca foram realizadas, induzindo o jogador a acreditar que seus amigos interagiram com o conteúdo de determinada forma.

Figura 41 - Exemplo ilustrativo de *dark pattern Friend Spam*



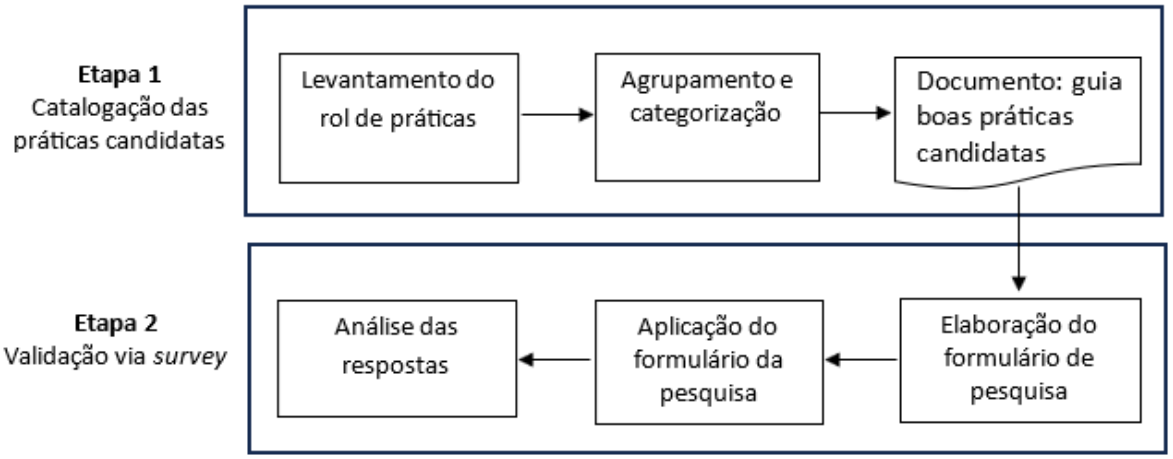
Fonte: Elaboração da autora

Essa prática resulta em uma distorção intencional da realidade social dentro do ambiente digital, violando princípios de transparência e confiança, ao enganar o usuário sobre o comportamento de sua rede social no jogo (FITTON; READ, 2019).

6. Etapa 2: Validação via *survey*

Tomando por base o documento guia de boas práticas candidatas (APÊNDICE A) construído ao final da etapa 1, iniciamos a etapa 2. Elaboramos o formulário de pesquisa (survey) para a coleta dos dados quantitativos. Após a aplicação do formulário de pesquisa, realizamos a análise dos resultados para inferir e analisar as práticas candidatas levantadas. Para melhor visualizar esse caminho, retomemos a Figura 2 (Fluxograma geral de etapas metodológicas), que apresentamos no capítulo 5.

Figura 2 - Fluxograma geral de etapas metodológicas



Fonte: Elaboração da autora

6.1 Método

Como método quantitativo de coleta de dados, escolhemos o método *survey* para a validação dos resultados obtidos na Etapa 1 por sua capacidade de coletar dados de forma sistemática, rápida e com alcance ampliado junto a um público-alvo diversificado. Segundo Gil e Neto, 2021:

> O survey constitui atualmente o método mais adotado pelos pesquisadores sociais interessados em coletar dados originais para descrever uma população grande demais para ser observada diretamente. De fato, o survey é adequado para investigar que as pessoas fazem, fizeram ou pretendem fazer, o que creem, valorizam, almejam, evitam etc. É, pois, delineamento apropriado para investigar fatos, crenças, sentimentos opiniões e atitudes. (GIL; NETO, 2021).

Essa abordagem permite verificar as percepções e níveis de concordância com os achados iniciais por meio de questionários padronizados. O método é

especialmente eficaz quando se busca generalizar conclusões a partir de uma amostra representativa, além de oferecer meios quantitativos para mensurar o grau de validação dos resultados. Por essas razões, acreditamos que o survey se apresenta como uma escolha metodologicamente sólida e alinhada aos objetivos desta fase da pesquisa.

6.1.1 Objetivo

O objetivo desta etapa foi validar as práticas candidatas a boas práticas, levantadas na etapa anterior, e verificar - junto aos desenvolvedores do mercado de jogos - se existe ou não um alinhamento acerca das práticas que seriam prioritárias para considerarmos um jogo o mais ético possível.

6.1.2 Elaboração do formulário

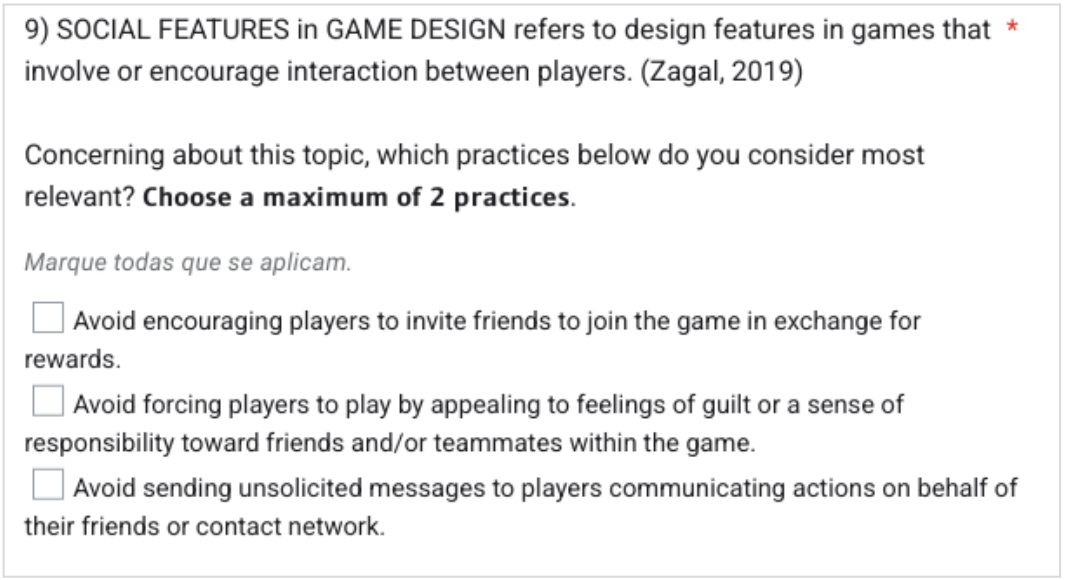
Tentamos duas abordagens para o survey. Primeiramente, apresentamos cada uma das 48 práticas candidatas e pedimos aos participantes que classificassem, numa escala de Likert, qual seu grau de concordância ou discordância em relação à afirmação apresentada. Observamos, no entanto, que essa abordagem teve pouca adesão de respostas, uma vez que o tempo de participação tornava-se muito longo em função do grande número de alternativas.

Em face disso, elaboramos uma segunda abordagem de formulário, onde formulamos uma pergunta para cada uma das categorias propostas no tópico 5.1.5.

Primeiro, antes das perguntas, propomos o seguinte contexto: *“Imagine que você está desenvolvendo um jogo para um público infantil e/ou menor de 16 anos. Neste contexto, listamos 9 categorias de práticas. Na questão relacionada a cada categoria, apresentaremos algumas opções de práticas. De acordo com sua experiência, você deve julgar quais delas você considera relevantes para ter em mente para seu produto”.*

Em seguida, apresentamos o conceito da categoria em questão e perguntamos: *“Sobre o tópico da categoria, quais as práticas que você considera mais relevantes?”*. Como alternativas, listamos as práticas referentes a cada uma das categorias, em formato de caixa de seleção, de forma que o participante pode escolher mais de uma alternativa, conforme mostra a Figura 42.

Figura 42 - Exemplo de pergunta do formulário aplicado ao *survey*



Fonte: Elaboração da autora.

Optamos por elaborar o formulário em inglês, como forma de viabilizar a participação de desenvolvedores estrangeiros no *survey*. Este formulário encontra-se anexado como Apêndice B do trabalho.

6.1.3 Participantes

Para a aplicação do survey, optamos por abranger um conjunto amplo e diversificado de perfis profissionais atuantes no mercado de jogos. Buscamos contemplar especialistas de diferentes áreas, como produtores, artistas, programadores, entre outros, com o objetivo de reunir dados que refletissem uma variedade de perspectivas e experiências.

Além disso, não limitamos a participação apenas a profissionais que desenvolvem jogos voltados, exclusivamente, para o público infantil. Como argumentado ao longo do trabalho, a configuração de públicos mistos é uma realidade recorrente, mesmo em projetos, originalmente, direcionados ao público adulto.

O único critério de exclusão adotado foi o tempo mínimo de experiência profissional. Definimos como requisito a atuação no setor por, no mínimo, quatro anos, por considerarmos esse intervalo de tempo suficiente para que o profissional tenha acumulado vivências e desenvolvido opiniões fundamentadas acerca das práticas abordadas.

O formulário de pesquisa foi hospedado no *Google Forms* e compartilhado por meio do LinkedIn, e-mail, WhatsApp e Telegram, entre 25 de novembro de 2024 e 7 de fevereiro de 2025. No total, tivemos 24 participantes, todos os quais concordaram expressamente em participar da pesquisa.

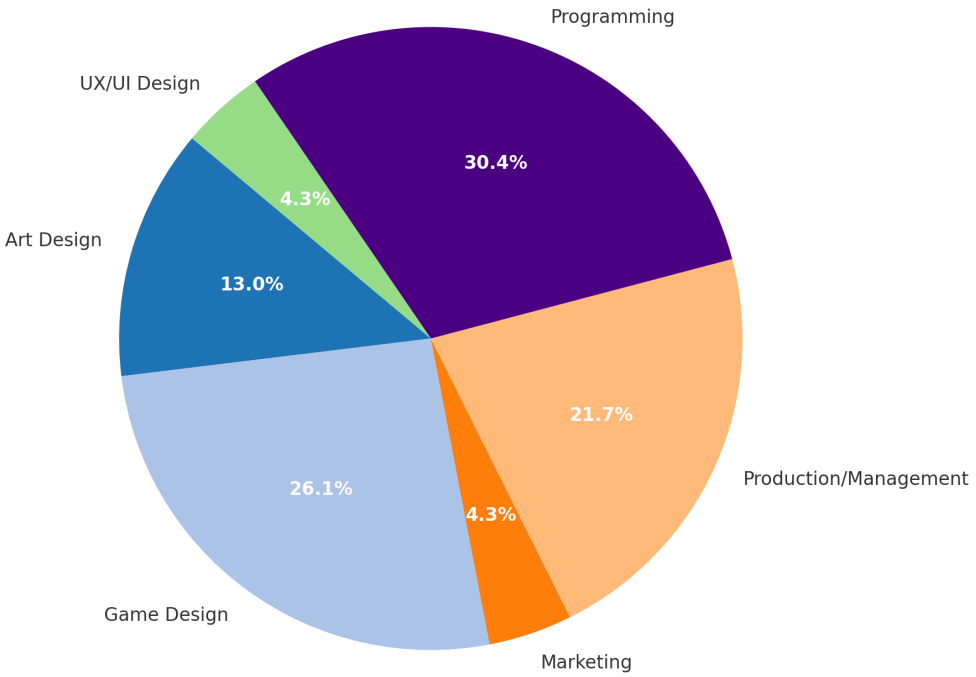
Antes de responder as perguntas centrais da pesquisa, os participantes responderam a cinco perguntas de perfil demográfico:

1) Há quantos anos você trabalha no mercado de jogos?
2) Qual a localização/país da empresa em que você trabalha?
3) Qual área de desenvolvimento de jogos mais se aproxima do seu trabalho atual?
4) Qual gênero de jogos você está desenvolvendo nos últimos anos?
5) Qual é o principal público-alvo dos jogos que você vem desenvolvendo?

Sobre o tempo de experiência, 26% dos participantes declararam ter de 4 até 7 anos de experiência no mercado de jogos; 26% de 7 a 10 anos; e 48% mais de 10 anos de experiência. Sobre a segunda pergunta, 69% declararam trabalhar em empresas estabelecidas no Brasil; 22% em empresas de países europeus (como Reino Unido, Espanha, Dinamarca e Suécia); 9% em empresas nos EUA.

A área de atuação dos profissionais mostrou-se bastante diversa, como podemos ver no Gráfico 3, com predominância de profissionais da área de programação (30%), de *game design* (26%) e de produção/gerenciamento (22%).

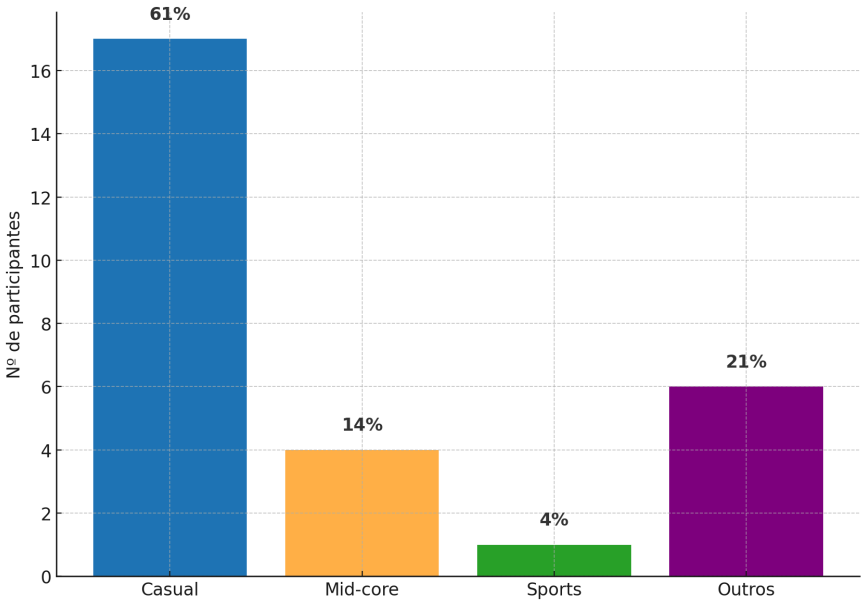
Gráfico 3 - Áreas de atuação profissional dos participantes da pesquisa.



Fonte: Elaboração da autora

Sobre a pergunta 4, relativa a qual gênero de jogos os participantes desenvolvem, apresentamos 5 alternativas, onde o participante poderia escolher mais de uma opção. As categorias de jogos apresentadas foram: casual (puzzle, arcade, simulação etc); mid-core (MMO, MOBA, RPG etc); sports; cassino; e outros. Mais de 60% dos profissionais declararam trabalhar em jogos casuais (Gráfico 4).

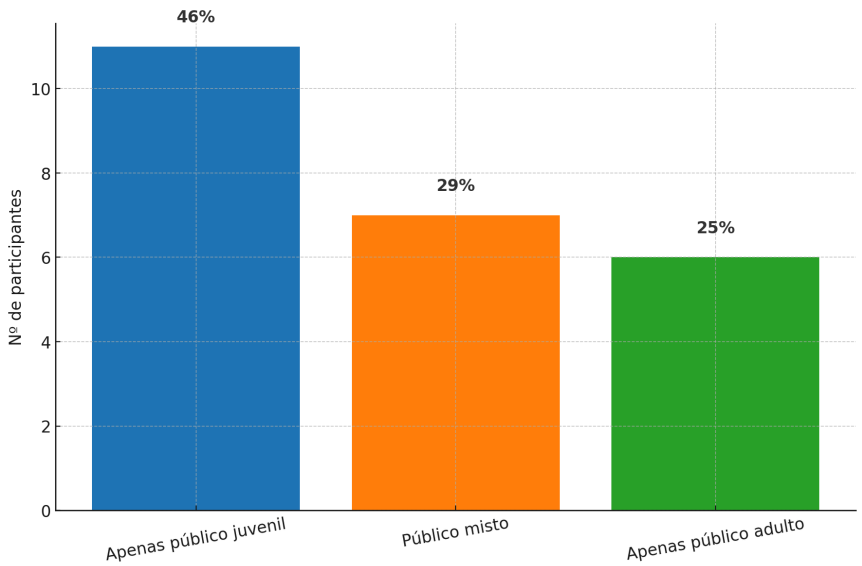
Gráfico 4 - Categorias de jogos desenvolvidas pelos participantes da pesquisa.



Fonte: Elaboração da autora

Na pergunta sobre o público-alvo para o qual desenvolve, apresentamos 3 alternativas: a) apenas para crianças e adolescentes (até 16 anos); b) para adolescentes e para o público em geral (maiores de 18 anos); c) apenas para o público em geral (maiores de 18). 46% disseram desenvolver apenas para crianças e adolescentes; 29% desenvolvem para públicos mistos; e 25% apenas para público adulto (Gráfico 5).

Gráfico 5 - Público-alvo dos jogos desenvolvidos pelos participantes da pesquisa.



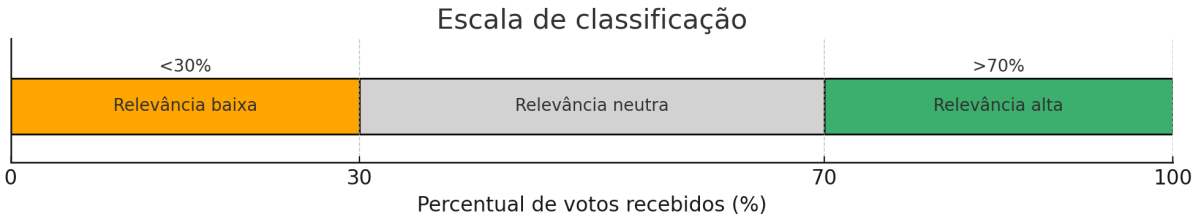
Fonte: Elaboração da autora

6.2 Resultados: Validação

Neste tópico, apresentamos os resultados obtidos a partir das respostas dos formulários, com o objetivo de verificar e validar a relevância das práticas candidatas enquanto práticas éticas. Em seguida, discutiremos os principais achados e interpretações desses dados.

Não identificamos na literatura, um método amplamente reconhecido para classificar variáveis com base em seu percentual de escolha pelos participantes. Diante disso, optamos por desenvolver e adotar uma escala própria de classificação, baseada na proporção de votos atribuídos a cada prática (Figura 43).

Figura 43 - Escala de classificação de relevância da prática



Fonte: Elaboração da autora

De acordo com esta escala, as práticas selecionadas por **menos de 30% dos participantes** foram classificadas como de **baixa relevância**; aquelas escolhidas **por mais de 70%** foram consideradas de **alta relevância**. Já as práticas que obtiveram **entre 30% e 70% dos votos** foram categorizadas como de **relevância neutra**, uma vez que, nesse intervalo, não é possível inferir com alto grau de certeza se há validação ou rejeição pela maioria do grupo.

Apesar de se tratar de uma escala arbitrária, consideramos que os critérios adotados são razoáveis. A classificação em três níveis de relevância – baixa, neutra e alta – facilita a análise comparativa e a priorização das práticas que demonstraram maior ou menor consenso entre os participantes; de forma que, a partir disso, possamos apontar alinhamentos, contradições e hipóteses acerca da adesão dos desenvolvedores frente às práticas propostas.

6.2.1 Categoria 1 - Gerenciamento de dados

Na Tabela 17 apresentamos o percentual de participantes que escolheram cada uma das práticas referentes a Categoria 1 - Gerenciamento de dados. As práticas validadas como de alta relevância foram: *“BP 1.1 - Não coletar dados excessivos ou desnecessários para a funcionalidade da sua aplicação”* (escolhida por 79%); e *“BP 1.3 - Não enviar para terceiros informações de identificação pessoal, localização ou informações do dispositivo”* (escolhido por 75%).

Já a prática *“BP 1.5 - Não usar cookies de rastreamento ou quaisquer outros recursos similares de rastreamento passivo”* (escolhido apenas por 8%) teve baixíssima relevância para os participantes.

Tabela 17 - Resultado do survey da Categoria 1- Gerenciamento de dados.

	Prática apresentada	% de votos	
BP 1.1	Não coletar dados excessivos ou desnecessários para a funcionalidade da sua aplicação.	79%	Alta relevância
BP 1.3	Não enviar para terceiros informações de identificação pessoal, localização ou informações do dispositivo.	75%	
BP 1.4	Permitir ao responsável a possibilidade de apagamento total dos dados fornecidos, em qualquer momento.	54%	Relevância neutra
BP 1.2	Manter os dados apenas no período de tempo razoável e justificável para o propósito para o qual foi coletado.	54%	
BP 1.6	Se você permitir que os usuários se registrem com um username, lembre-os de que eles devem evitar usar nomes reais ou identificadores de mídia social existentes.	50%	
BP1.7	Evite utilizar recursos ou estratégias subliminares para que o jogador compartilhe mais informações do que realmente pretende.	46%	
BP 1.5	Não usar cookies de rastreamento ou quaisquer outros recursos similares de rastreamento passivo.	8%	Baixa relevância

Fonte: Elaboração da autora

Diante desses resultados, observamos um **alinhamento sobre a importância dos limites de coleta e de compartilhamento** (BP 1.1 e BP 1.3). As práticas relacionadas à não divulgação de dados sensíveis e à minimização da coleta são claramente percebidas como essenciais.

Apesar de serem direitos dos titulares dos dados, os direitos de apagamento e limitação temporal do uso de dados ainda não são, majoritariamente, reconhecidos como prioritários (BP 1.4 e BP 1.2). Isso pode estar relacionado a desafios técnicos e/ou menor apelo sobre esses recursos no cenário prático.

Observa-se também uma relevância neutra na preocupação em fornecer um design mais informativo para usuários mais jovens; bem como resguardá-los de estratégias de design que possam induzi-lo à exposição (BP 1.6 e BP 1.7). Isso pode indicar que muitos profissionais ainda não percebem o grau de impacto do design nas escolhas dos usuários, especialmente de crianças e adolescentes; ou não levam em grande consideração sua capacidade ainda imatura de julgamento.

Apesar da alta sensibilidade à coleta ativa, **o rastreamento passivo ainda gera baixa preocupação** (BP 1.8). O resultado pode revelar uma possível falha de conscientização sobre os riscos e uma banalização do rastreamento passivo digital, prática frequente com usuários adultos.

6.2.2 Categoria 2 - Controle parental

A Tabela 18 apresenta o percentual de participantes que selecionaram cada uma das práticas pertencentes à Categoria 2 – Controle parental. Entre elas, apenas a prática *"BP 2.4 - Incluir parental gates em momentos estratégicos para impedir que as crianças realizem compras ou acessem links que as direcionem a sites, redes sociais ou outros aplicativos sem o conhecimento de seus pais ou responsáveis"* (escolhida por 83%) foi validada como de alta relevância. As demais práticas da categoria foram classificadas como de relevância neutra.

Tabela 18 - Resultado do survey da Categoria 2 - Controle parental.

	Prática apresentada	% de votos	
BP 2.4	Incluir *parental gates* em momentos estratégicos para impedir que as crianças façam compras ou sigam links de um aplicativo para sites, redes sociais ou outros aplicativos sem o conhecimento de seus pais ou responsáveis.	83%	Alta relevância
BP 2.2	Obter consentimento parental verificável antes de qualquer coleta, uso e/ou divulgação de informações pessoais de crianças, alocando de todos os esforços e recursos disponíveis.	58%	Relevância neutra
BP 2.1	Deixar explícito e acessível um link para acesso da política de privacidade do jogo na página inicial e em cada página em que informações pessoais das crianças são coletadas.	54%	
BP 2.3	Fornecer um meio razoável para que os pais revisem as informações pessoais coletadas de uma criança e se recusem a permitir seu uso ou manutenção.	50%	
BP 2.6	Não incluir, fora do *parental gate*, oportunidades de compra ou outras distrações para as crianças.	42%	
BP 2.5	Incluir um recurso para denunciar conteúdo inadequado no jogo.	37%	

Fonte: Elaboração da autora

Existe um **grande alinhamento sobre a proteção da criança, através do uso de *parental gates*** (BP 2.4). Esta prática, contudo, não é acompanhada da mesma forma à percepção sobre a relevância do consentimento parental verificável (como indica a prática BP 2.2), o que reflete uma certa contradição.

O *parental gate* é, em linhas gerais, uma barreira técnica, há muito, exigida como obrigatória pelas plataformas de distribuição em apps para crianças, o que resulta em uma certa familiaridade com o recurso por parte dos desenvolvedores.

Por outro lado, **o consentimento parental verificável ainda não é reconhecido como de fundamental relevância**, por quase metade dos participantes. Embora seja um dos pilares de proteção de dados de crianças e

adolescentes, previsto pelos instrumentos legais, esse tipo de consentimento talvez ainda seja visto como uma etapa apenas burocrática. Destacamos, portanto, aqui um certo desconhecimento desse mecanismo legal por parte dos profissionais da área.

Da mesma forma, a relevância neutra acerca da acessibilidade e da transparência da política de privacidade (BP 2.1) pode refletir a percepção de que essa seria, a rigor, apenas um documento pró-forma, burocrático e pouco acessado pelos usuários, quando, na realidade, são instrumentos fundamentais de conformidade legal e ética. A mesma hipótese vale para a inclusão de ferramentas para denúncia de conteúdo inadequado (como recomenda a prática BP 2.5).

6.2.3 Categoria 3 - Classificação de usuários

A Tabela 19 apresenta o percentual de participantes que selecionaram cada uma das práticas associadas à Categoria 3 – Classificação de Usuários. Dentre elas, apenas a prática "*BP 3.2 – Declarar, no momento do registro na loja de aplicativos, de forma precisa e transparente, os tipos de conteúdo presentes no jogo para fins de classificação"* (escolhida por 83%) foi validada como de alta relevância.

Por outro lado, a prática "*BP 3.3 – Verificar a idade do jogador antes do início da primeira sessão"* (escolhida apenas por 17%) obteve baixa adesão entre os participantes.

Tabela 19 - Resultados do survey da Categoria 3 - Classificação de usuários.

	Prática apresentada	% de votos	
BP 3.2	Declarar, no momento do registro em loja de apps, quais tipos de conteúdo podem ser encontrados no jogo de forma precisa e honesta para fins de classificação.	83%	Alta relevância
BP 3.4	Analisar se há conteúdos, conceitos, temas delicados inadequados à idade segmentada.	58%	Relevância neutra
BP 3.1	Definir, com clareza, a faixa etária do seu público alvo, antes da publicação do jogo.	37%	
BP 3.3	Antes do jogador iniciar sua primeira sessão, verificar sua idade.	17%	Baixa relevância

Fonte: Elaboração da autora

Observamos que **a transparência na comunicação com as lojas de aplicativos sobre o conteúdo do jogo tem forte apelo** (em consonância com a prática BP 3.2), mas acreditamos, por razões óbvias, de condição obrigatória para

elegibilidade na distribuição do produto. Por outro lado, práticas relativas à análise de conteúdo inadequado (como orienta a prática BP 3.4) não apresentam a mesma grandeza de relevância, o que demonstra uma nova contradição. Isso pode indicar uma **possível percepção - por parte dos desenvolvedores - de que sua responsabilidade ética limita-se à comunicação técnica e comercial junto ao *player* distribuidor**, não se estendendo ao usuário final a ser protegido com essa prática.

Reforçando essa hipótese, a prática relativa à verificação de idade, antes da primeira sessão (como orienta a prática BP 3.3) apresenta baixo apelo e relevância. Podemos supor que esta prática seja vista como um gargalo à experiência do usuário, quando, na realidade, deveria ser encarada como pré-requisito para que a experiência do jogo possa ser adaptada de forma segura.

6.2.4 Categoria 4 - Publicidade: geral

Na Tabela 20 apresentamos o percentual de participantes que escolheram cada uma das práticas referentes à Categoria 4 - Publicidade: geral. A única prática validada como de alta relevância foi *"BP 4.1 - Garantir que todos os SDKs de ads usados são adequados e certificados para crianças e estão em compliance com todas as leis aplicáveis"* (escolhida por 75%). As duas restantes mantiveram relevância neutra.

Tabela 20 - Resultados do survey da Categoria 4 - Publicidade: geral.

	Prática apresentada	% de votos	
BP 4.1	Garantir que todos os SDKs de ads usados são adequados e certificados para crianças e estão em *compliance* com todas as leis aplicáveis.	75%	Alta relevância
BP 4.2	Não usar táticas de publicidade impróprias para crianças, como o remarketing ou a publicidade com base em interesses.	58%	Relevância neutra
BP 4.3	Evite usar táticas agressivas de publicidade ou de compras.	54%	

Fonte: Elaboração da autora

Verificamos, portanto, uma **alta prioridade sobre a conformidade técnica dos SDKs de publicidade** (prática BP 4.1) o que, mais uma vez, pode configurar como condição obrigatória para elegibilidade na distribuição do produto, no caso de aplicativos.Também pode indicar a consciência dos desenvolvedores com os riscos envolvidos com o controle de anúncios impróprios, via terceiros.

Nenhuma das demais práticas que advertem acerca do uso de estratégias impróprias de publicidade (BP 4.2. e BP 4.3) atingiu um nível de relevância tido como significativo, indicando que - para quase metade dos profissionais participantes - essas **práticas relativas à publicidade agressiva ainda não, majoritariamente, consideradas problemáticas e arriscadas**. Possivelmente, o que está por trás disso é o interesse de lucro decorrente de modelos de negócios, muitas vezes, baseados apenas em mídia programática.

Essa hipótese pode ser corroborada pela baixa relevância acerca da prática de rastreamento passivo (BP 1.5), observado no tópico 6.2.1, uma vez que a publicidade faz uso, frequente, desses recursos para direcionamento de anúncios e monetização de sua base de usuários.

6.2.5 Categoria 5 - Publicidade: anúncios

A Tabela 21 apresenta resultado percentual de participantes que escolheram as práticas relativas à Categoria 5 – Publicidade: anúncios. Apenas a prática *"BP 5.7 - Evite exibir anúncios em formatos e conteúdos impróprios para a faixa etária do seu público"* (escolhida por 83%) foi validada como de alta relevância. Verificamos como de baixa relevância, a prática *"BP 5.5 – Evite forçar o jogador a assistir anúncios em troca de recompensas"* (escolhida apenas por 17%).

Tabela 21 - Resultados do survey da Categoria 5 - Publicidade: anúncios.

	Prática apresentada	% de votos	
BP 5.7	Evite exibir anúncios em formatos e conteúdos impróprios para a faixa etária do seu público	83%	Alta relevância
BP 5.4	Evitar exibir anúncios intersticiais e ofertas para compras *in-game* logo após a abertura. Os usuários precisam experimentar a funcionalidade do seu app ou jogo primeiro.	67%	Relevância neutra
BP 5.2	Evitar anúncios invasivos que ocupem a tela inteira ou interfiram no uso normal do app e/ou não ofereçam a opção de fechar, após 5 segundo, no máximo.	54%	
BP 5.3	Evitar mais de um anúncio em uma mesma página ou de forma subsequente.	42%	
BP 5.1	Diferenciar claramente anúncios do conteúdo do app, por exemplo destacando a monetização e a publicidade no conteúdo do app usando cores e estilos diferentes.	37%	
BP 5.6	Evite exibir anúncios "interstitial" de conteúdos fora do contexto do jogo.	33%	
BP 5.5	Evite forçar o jogador a assistir anúncios em troca de recompensas.	17%	Baixa relevância

Fonte: Elaboração da autora

Observamos uma **alta preocupação com a adequação do formato e conteúdo dos anúncios** (conforme prática BP 5.7), o que podemos supor que decorre das mesmas razões da alta relevância dada à conformidade dos SDK´s (BP 4.1), mencionado no tópico 6.2.4.

No entanto, **a percepção sobre a importância de evitar anúncios invasivos, sucessivos e fora do contexto do jogo ainda não é um consenso** entre os desenvolvedores (BP 5.2, BP 5.3 e BP 5.6) . Apesar de seu caráter nocivo e intrusivo dentro da experiência, a veiculação desse tipo de anúncio ainda parece ser bem aceita por parte dos desenvolvedores, provavelmente, por questões comerciais de rentabilidade.

Oferecer recompensas em troca da exibição de anúncios (como adverte a prática BP 5.5) ainda parece gerar pouca preocupação entre os desenvolvedores, possivelmente, por se tratar de uma estratégia amplamente adotada na monetização de experiências voltadas ao público adulto. Esse cenário pode indicar uma **percepção limitada, por parte dos desenvolvedores, quanto à necessidade de adaptar determinadas práticas - tradicionalmente aplicadas a jogos para adultos - quando direcionadas a usuários mais jovens**.

6.2.6 Categoria 6 - Compras *in-game*

A Tabela 22 apresenta resultado percentual de participantes que escolheram as práticas relativas à Categoria 6 – Compras *in-game*. Neste caso, um conjunto de três práticas foram validadas como de alta relevância: *“BP 6.1 - Evite dificultar o cancelamento de compras ou assinaturas dentro do jogo”* (escolhida por 79%)*; “BP 6.3 - Evite adicionar itens não selecionados pelo jogador ao carrinho de compras dele*” (escolhida por 71%) e *“BP 6.5 - Os usuários devem conseguir diferenciar, claramente, "moedas" do jogo de valores monetários reais”* (escolhida por 71%).

Outro conjunto de quatro práticas aparece como de baixa relevância, mas em proporções percentuais bem diferentes: *“BP 6.6 - Evite induzir o jogador a pagar um valor monetário para acelerar ou melhorar seu progresso no jogo”* e *“BP 6.7 - Evite cobrar do jogador, além do valor pago inicialmente, algum outro valor adicional para que ele tenha acesso a features extras”* receberam 29% dos votos cada. Isto é, próximo ao limiar de serem consideradas práticas de relevância neutra, segundo a escala adotada (ver Figura 13).

Já as práticas *“BP 6.4 - Evite sugerir compras ao jogador com base em compras anteriores“* e *“BP 6.8 - Evite apresentar features de compras, de forma hierárquica, ao invés de paralelas, sugerindo que uma opção é melhor que a outra”* foram consideradas irrelevantes, recebendo apenas 12% e 8% dos votos, respectivamente.

Tabela 22 - Resultados do survey da Categoria 6 - Compras *in-game.*

	Prática apresentada	% de votos	
BP 6.1	Evite dificultar o cancelamento de compras ou assinaturas dentro do jogo.	79%	Alta relevância
BP 6.3	Evite adicionar itens não selecionados pelo jogador ao carrinho de compras dele. Exemplo: compra casada	71%	
BP 6.5	Os usuários devem conseguir diferenciar, claramente, "moedas" do jogo de valores monetários reais.	71%	
BP 6.2	Evite demora para informar ao jogador que ele poderá ter custos adicionais por conta de alguma ação ou do seu engajamento	42%	Relevância neutra
BP 6.6	Evite induzir o jogador a pagar um valor monetário para acelerar ou melhorar seu progresso no jogo	29%	Baixa relevância
BP 6.7	Evite cobrar do jogador, além do valor pago inicialmente, algum outro valor adicional para que ele tenha acesso a features extras.	29%	
BP 6.4	Evite sugerir compras ao jogador com base em compras anteriores.	12%	
BP 6.8	Evite apresentar features de compras, de forma hierárquica, ao invés de paralelas, sugerindo que uma opção é melhor que a outra.	8%	

Fonte: Elaboração da autora

Nesse cenário, os desenvolvedores parecem se colocar no lugar do jogador, enquanto cliente. Assim, aparentemente, existe uma **rejeição de estratégias que caracterizem uma manipulação explícita e desonesta das decisões de compras no jogo ,** o que foi demonstrado pela priorização de escolha das práticas BP 6.1, BP 6.3 e BP 6.5.

Por outro lado, as **estratégias de manipulação mais sutil de compras ainda permanecem bem aceitas** por grande parte dos desenvolvedores (já que maioria não apontou as práticas BP 6.6 e BP 6.7 como relevantes). Uma das estratégias mais sutis, como por exemplo, a apresentação dos itens de compras de forma hierárquica é tão frequentemente empregada, que não configura nenhuma natureza de problematização (o que reforça pela baixa relevância da prática BP 6.8).

6.2.7 Categoria 7 - *Game design*: geral

A Tabela 23 apresenta resultado percentual de participantes que escolheram as práticas relativas à Categoria 7 - *Game design*: geral. Ambas as práticas *“BP 7.6 - Evite fazer perguntas enganosas que possam ter duplo sentido ou interpretação ambígua”* (escolhida por 83%) e *“BP 7.2 - Evite estimular ações e comportamentos*

no jogo que, na vida real, seriam considerados antiéticos" (escolhida por 71%) foram validadas como de alta relevância.

A prática *BP 7.5 – Evitar deixar qualquer opção de funcionalidade pré-selecionada, de modo a não influenciar a escolha do jogador* foi classificada como de baixa relevância, tendo sido selecionada por 21% dos participantes.

Tabela 23 - Resultados do survey da Categoria 7 - *Game design*: geral.

	Prática apresentada	**% de votos**	
BP 7.6	Evite fazer perguntas enganosas que possam ter duplo sentido ou interpretação ambígua.	83%	Alta relevância
BP 7.2	Evite estimular ações e comportamentos no jogo que, na vida real, seriam considerados antiéticos.	71%	
BP 7.1	Evitar pressionar o jogador a jogar recorrendo ao sentimento de que, caso não o façam, estarão perdendo recompensas ou em desvantagem em relação a outros jogadores.	46%	Relevância neutra
BP 7.3	Evite exigir ao jogador períodos de tempo ou datas específicas para jogar, dando flexibilidade ao jogador.	37%	
BP 7.4	Evite exigir que o jogador realize tarefas monótonas de forma recorrente para progredir no jogo.	33%	
BP 7.5	Evite deixar qualquer opção de feature pré-selecionada, influenciando a escolha do jogador.	21%	Baixa relevância

Fonte: Elaboração da autora

Percebemos que existe uma forte rejeição a manipulações textuais explícitas, ou até mesmo verbais. Logo, podemos apontar a **valorização de uma linguagem clara e honesta de comunicação com o usuário** (como reforçado pela prática BP 7.6). Já a relevância da prática BP 7.2 parece apontar para uma **consciência dos desenvolvedores sobre o impacto dos valores éticos e comportamentos retratados no jogo sob o comportamento das crianças**.

Em relação à prática apontada como de menor relevância (BP 7.5), que trata do *design* de interfaces com opções de compra previamente selecionadas, é possível associar esse resultado à hipótese de uma maior aceitação e flexibilidade, por parte dos desenvolvedores, em relação a práticas sutis de manipulação de consumo, argumento já discutido no tópico 6.2.6.

Por outro lado, **algumas estratégias de *game design* que recorrem à manipulação emocional ainda não são problematizadas por grande parte dos desenvolvedores** (estratégias essas inibidas pelas práticas BP 7.1, BP 7.3 e BP

7.4), provavelmente, porque estejam diretamente relacionadas às estratégias de retenção dos jogos.

Importante frisar que estratégias de retenção como essas podem impactar diretamente na rotina, sono e desenvolvimento de vícios. Muitos desenvolvedores, no entanto, ainda podem julgá-las como indispensáveis para conseguir um engajamento significativo, ignorando seus impactos no equilíbrio de atividades da rotina das crianças. Retomamos aqui, mais uma vez, o argumento sobre uma provável **falta de percepção, por parte dos desenvolvedores, acerca da necessidade de adaptar determinadas *game features* - tradicionalmente aplicadas a públicos adultos - quando direcionadas a crianças e adolescentes**.

6.2.8 Categoria 8 - *Game design*: recompensas

A Tabela 24 apresenta o percentual de participantes que selecionaram cada uma das práticas associadas à Categoria 8 – Game design: recompensas. Dentre elas, apenas a prática *"BP 8.1 – Não condicionar o acesso ou recompensa da criança à divulgação de informações pessoais a mais do que o necessário"* (escolhida por 87%) foi validada como de alta relevância.

Por outro lado, a prática *"BP 8.2 – Evite recompensar o jogador de forma aleatória ou inesperada para viciá-lo no jogo. Preferir recompensas regulares e previsíveis."* (escolhida apenas por 24%) obteve baixa adesão entre os participantes. Por último, a *"BP 8.3 - Evite oferecer recompensas ao jogador ou penalizá-lo em função dele(a) jogar diariamente"* recebeu apenas 4% dos votos, podendo ser considerada irrelevante pelos participantes.

Tabela 24 - Resultados do survey da Categoria 8 - *Game design*: recompensas.

	Prática apresentada	% de votos	
BP 8.1	Não condicionar o acesso ou recompensa da criança à divulgação de informações pessoais a mais do que o necessário.	87%	Alta relevância
BP 8.4	Evite usar recursos de recompensas como *loot boxes*, *gambling* ou quaisquer outros que possam ser classificados como jogos de azar.	62%	Relevância neutra
BP 8.2	Evite recompensar o jogador de forma aleatória ou inesperada para viciá-lo no jogo. Preferir recompensas regulares e previsíveis.	25%	Baixa relevância
BP 8.3	Evite oferecer recompensas ao jogador ou penalizá-lo em função dele jogar diariamente.	4%	

Fonte: Elaboração da autora

Verificamos um grande consenso sobre não condicionar o acesso ou ganho de recompensas em troca de dados pessoais (BP 8.1). Acreditamos que esse resultado encontra-se relacionado à perspectiva do alinhamento sobre a importância dos limites de coleta e de compartilhamento, abordado no tópico 6.2.1.

A maioria reconhece a relevância de evitar práticas como *loot boxes* e *gambling* (BP 8.4), mas a adesão ainda não podemos considerar como unânime. Isso é preocupante, dado que essas *features* são consideradas altamente danosas, principalmente para crianças. Ainda mais preocupante é a baixa relevância dada às práticas de recompensas aleatórias (BP 8.2), que, assim como os *loot boxes*, podem desencadear gatilhos nocivos de frustração e vício.

A prática de evitar recompensas ou penalizações condicionados ao engajamento (BP 8.3) é encarada, praticamente, como irrelevante. Isso evidencia que **mecânicas manipulativas de engajamento diário são vistas como práticas comerciais aceitáveis**, possivelmente, consideradas como indispensáveis para retenção do jogador.

6.2.9 Categoria 9 - *Game design*: *social features*

Na Tabela 25 apresentamos o percentual de participantes que escolheram as práticas contidas na Categoria 9 - *Game design: social features*. Nesse contexto, destacamos uma prática como de altíssima relevância, sendo escolhida por 92% dos participantes do *survey*: *"BP 9.3 - Evite enviar aos jogadores mensagens não solicitadas comunicando ações em nome de seus amigos ou sua rede de contatos"*.

Em contraposição a ela, temos a prática *“BP 9.1 - Evite incentivar os jogadores a convidar amigos para ingressarem no jogo em troca de recompensas.”* (escolhido apenas por 8%) que apresentou baixíssima relevância junto aos participantes.

Tabela 25 - Resultados do survey da Categoria 9 - *Game design*: social features.

	Prática apresentada	**% de votos**	
BP 9.3	Evite enviar aos jogadores mensagens não solicitadas comunicando ações em nome de seus amigos ou sua rede de contatos.	92%	Alta relevância
BP 9.2	Evite forçar os jogadores a jogarem recorrendo ao sentimento de culpa ou senso de responsabilidade com amigos e/ou equipe dentro do jogo.	62%	Relevância neutra
BP 9.1	Evite incentivar os jogadores a convidar amigos para ingressarem no jogo em troca de recompensas.	8%	Baixa relevância

Fonte: Elaboração da autora

Como podemos observar, existe quase um consenso geral acerca de evitar enviar mensagens não solicitadas em nome de amigos ou da rede de contatos do jogador (BP 9.3). Inferimos, assim, que esta forma de comunicação é considerada, pelos desenvolvedores, como uma estratégia de manipulação explicitamente abusiva.

Por outro lado, mais uma vez, verificamos que **o uso de algumas estratégias de *game design* que recorrem à manipulação emocional ainda são bem aceitas por parte dos desenvolvedores** (ao contrário do que orienta a prática BP 9.2), uma vez que também configura uma estratégia para reforçar o engajamento e a retenção do jogo .

Incentivar convites aos amigos em troca de recompensas (inibida pela prática BP 9.1) gera baixíssima preocupação. Aqui, podemos inferir que **a rede de contatos dos jogadores é considerada um capital de sumo interesse de exploração comercial,** sobrepondo-se a certas prerrogativas éticas.

6.3 Consolidação dos resultados por categoria e tipo de relevância

O resultado final da validação das práticas recomendadas foi obtido por meio de um *survey* aplicado a desenvolvedores de jogos digitais, que avaliaram a relevância de cada prática dentro de nove categorias temáticas. Ao todo, foram validadas 48 práticas recomendadas, classificadas de acordo com três níveis de relevância: alta, moderada e baixa.

A distribuição total das categorias por tipo de relevância foi: **13 práticas foram consideradas de alta relevância**, **24 de relevância moderada** e **11 de baixa relevância**. Podemos visualizar a contagem detalhada na Tabela 26 abaixo.

Tabela 26 - Resultado final de práticas por categoria e tipo de relevância

	Alta relevância	**Neutra relevância**	**Baixa relevância**
Categoria 1 - Gerenciamento de dados	2	4	1
Categoria 2 - Controle parental	1	5	0
Categoria 3 - Classificação de usuários	1	2	1
Categoria 4 - Publicidade: geral	1	2	0
Categoria 5 - Publicidade: anúncios	1	5	1
Categoria 6 - Compras *in-game*	3	1	4
Categoria 7 - *Game design*: geral	2	3	1
Categoria 8 - *Game design*: recompensas	1	1	2
Categoria 9 - *Game design*: *social features*	1	1	1
Total por nível de relevância	**13** (27%)	**24** (50%)	**11** (23%)

Fonte: Elaboração da autora

Como podemos verificar, cerca de 27% das 48 práticas recomendadas foram validadas, como de alta relevância, através do *survey.* Isto não significa dizer que as demais possam ser descartadas.

Ainda há uma grande concentração de práticas consideradas como de relevância neutra (50% no total). Categorias que apresentam grande concentração deste tipo - como Controle parental; Publicidade: anúncios; e, Gerenciamento de dados - podem sugerir uma maior incerteza ou desconhecimento sobre o tema abordado por cada uma delas, susceptíveis de debates mais aprofundados.

7. Limitações e aprimoramentos de pesquisa

Este trabalho apresenta contribuições relevantes para a discussão ética no desenvolvimento de jogos digitais voltados a crianças e adolescentes. Como toda pesquisa científica, contudo, também apresenta limitações que precisam ser reconhecidas, pois impactam a generalização dos resultados; a aplicabilidade do guia proposto; e, a validade interna e externa do estudo.

Uma das principais limitações refere-se ao método utilizado para validação das práticas candidatas, baseado na aplicação de um *survey online* com desenvolvedores. Embora essa abordagem tenha possibilitado o acesso a percepções de profissionais atuantes no setor, a amostra obtida foi limitada em número e pode não refletir a diversidade do ecossistema de desenvolvedores, especialmente no que diz respeito à distribuição geográfica: ao porte das empresas; às áreas de atuação; ou, ao grau de familiaridade dos participantes com legislações e princípios éticos.

Além disso, por tratar-se de uma pesquisa com adesão voluntária, é possível que tenha ocorrido um viés de autosseleção, no qual os respondentes mais sensibilizados com o tema tenham-se engajado com maior frequência. Isso pode ter influenciado os resultados, gerando uma percepção inflacionada de adesão às boas práticas éticas.

Outro ponto a ser considerado diz respeito ao fato de que a validação realizada se baseou em percepções subjetivas sobre a relevância das práticas propostas, e, não, em sua implementação empírica em produtos reais. Dessa forma, os resultados obtidos refletem julgamentos individuais dos participantes sobre a importância das práticas, mas não fornecem garantias sobre sua aplicação concreta no cotidiano de desenvolvimento de jogos.

As práticas elencadas neste trabalho foram extraídas a partir de documentos legais, normativos e acadêmicos disponíveis até a data de realização da pesquisa. Isso significa que o guia pode não abranger práticas mais recentes ou inovações que tenham surgido após esse período. Por se tratar de um campo em constante transformação, novas legislações, mecanismos regulatórios e abordagens de design podem demandar atualizações frequentes do conteúdo.

Também é importante destacar que o próprio conceito de "prática ética" carece de padronização na literatura e pode ser interpretado de maneiras distintas

por diferentes agentes envolvidos no ecossistema dos jogos, como legisladores, desenvolvedores, pais ou crianças. O foco desta dissertação esteve voltado, principalmente, aos desenvolvedores independentes, o que pode limitar a aplicabilidade das recomendações a contextos organizacionais mais complexos, como grandes estúdios ou corporações internacionais que operam sob estruturas legais e técnicas mais robustas.

Diante dessas limitações, o guia proposto deve ser compreendido como um instrumento de apoio e sensibilização, e não como um padrão normativo ou manual técnico definitivo. Seu uso deve estar sempre atrelado à análise crítica do contexto; à atualização contínua frente às transformações legais e tecnológicas; e, à busca constante por soluções mais justas, transparentes e seguras para o público infantojuvenil.

Como perspectivas de aprimoramento para estudos futuros, destaca-se a importância de realizar pesquisas longitudinais que acompanhem a adoção e os efeitos concretos das práticas sugeridas ao longo do ciclo de vida de jogos reais. Também seria pertinente ampliar o escopo de participação dos desenvolvedores, incorporando perfis variados de empresas, países e plataformas, bem como investir em estudos qualitativos, como entrevistas em profundidade ou estudos de caso, que possam oferecer uma visão mais contextualizada dos fatores que facilitam ou dificultam a adoção de boas práticas éticas no desenvolvimento de jogos digitais voltados a crianças e adolescentes.

8. Considerações finais

Refletir sobre a violação dos direitos da criança no ambiente virtual e a necessidade de regulamentar práticas éticas no *design* de jogos digitais voltados, direta ou indiretamente, ao público infantojuvenil constitui uma pauta de grande relevância no cenário contemporâneo. Diante da crescente presença de crianças e adolescentes como usuárias ativas e engajadas no mercado de jogos torna-se urgente discutir direcionamentos que assegurem um ambiente digital mais justo, seguro e apropriado para os menores de idade. Nesse contexto, promover essa discussão é indispensável para promover e fortalecer a responsabilidade social do setor.

Ao longo desta pesquisa, evidenciamos fatores de desalinhamento entre princípios éticos, exigências legais e a prática cotidiana dos desenvolvedores, que ainda carecem de suporte de caráter complementar e técnico, adequados para orientar suas decisões de *design* e operação.

Nosso objetivo maior foi propor um guia de boas práticas éticas que pudesse servir como suporte de orientação para os desenvolvedores independentes de jogos. Com este propósito em mente, revisamos as soluções apresentadas pelos mecanismos reguladores e as referências da literatura, particularmente voltadas aos *design dark patterns*. Com este conhecimento em mãos, compomos uma lista de práticas candidatas as quais validamos junto a um grupo de profissionais especialistas da área de jogos, através de um survey.

A principal contribuição original deste trabalho reside na revisão técnica, multidisciplinar e integrada das principais referências legais, normativas e acadêmicas sobre privacidade e ética digital, compilando-as em um guia prático e acessível para o desenvolvimento de jogos voltados a crianças e adolescentes.

Ao organizar essas práticas em categorias didáticas e aplicáveis, o resultado não apenas sintetiza conhecimento disperso, mas também se torna uma ferramenta versátil: servindo tanto como material educativo para conscientização sobre boas práticas, quanto como *checklist* para auxiliar desenvolvedores na implementação concreta de mecanismos éticos. Acreditamos que essa abordagem pode contribuir para reduzir a lacuna entre a teoria regulatória e a prática do mercado, promovendo inovação responsável no setor de jogos digitais.

Ressaltamos que as práticas levantadas como guia, nesta pesquisa, não excluem outras que, eventualmente, possam surgir, adaptando-se às necessidades dos usuários e inovações tecnológicas.

Por meio da aplicação do *survey*, conseguimos levantar hipóteses interessantes e destacar algumas conclusões centrais que nos ajudam a compreender a perspectiva dos desenvolvedores acerca das práticas éticas propostas.

Em primeiro lugar, observamos que a noção de responsabilidade ética do desenvolvedor tende a se limitar às exigências impostas pelos *players* distribuidores, desconhecendo, muitas vezes, de quais prerrogativas legais para proteção de crianças e adolescentes decorrem essas exigências.

Apesar da uma tendência à rejeição de estratégias de manipulação explícita, os desenvolvedores tendem a ser flexíveis quanto ao uso de estratégias de manipulação mais sutis. Os resultados também apontam uma percepção limitada, por parte dos desenvolvedores, sobre a necessidade de adaptação de determinadas *features* do jogo, quando o público-alvo inclui crianças e adolescentes.

Como já era previsto, confirmamos que os interesses voltados à retenção e à monetização exercem forte influência sobre os critérios adotados pelos desenvolvedores para definir quais práticas são consideradas mais ou menos aceitáveis. Nesse contexto, acreditamos que promover a adoção de práticas mais éticas e alinhadas à proteção e ao melhor interesse da criança e do adolescente passa, inevitavelmente, por repensar os modelos de negócio vigentes no setor.

Cabe aqui o questionamento: até que ponto o mercado estaria disposto a flexibilizar suas estratégias comerciais e investir na inovação de abordagens mais responsáveis, ainda que isso envolva riscos financeiros?

Não podemos ter a ingenuidade de pensar que a mera proposição de um guia irá mudar as práticas da indústria, mas acreditamos que oferecemos uma contribuição nesse sentido. Como reflexão, fica a necessidade de, no futuro, pensarmos em mecanismos que incentivem a adesão às boas práticas por parte de empresas e desenvolvedores.

Como contribuições futuras, pretendemos divulgar essas práticas e suas discussões por meio de artigos científicos. Esperamos, assim, que esse instrumento alcance os desenvolvedores independentes de jogos e possibilite a construção de pontes para outras pesquisas e avanços no setor.

Uma proposta promissora para trabalhos futuros consiste na utilização do guia de boas práticas éticas como base para auditoria empírica de jogos digitais populares entre crianças e adolescentes. Essa auditoria envolveria a seleção de um ou dois títulos amplamente conhecidos no mercado e a análise sistemática de suas funcionalidades, interfaces e políticas, a fim de verificar quais práticas recomendadas no guia são efetivamente adotadas e quais estão ausentes ou em desacordo. Essa abordagem permitiria não apenas validar a aplicabilidade do guia em contextos reais, mas também revelar padrões recorrentes de risco, identificar boas práticas consolidadas na indústria e apontar oportunidades de melhoria.

Além disso, vislumbramos que este trabalho de pesquisa também possa colaborar para a criação de um possível programa de treinamento e capacitação gratuito e *online*, em português, para os desenvolvedores de jogos do mercado brasileiro, assim como o programa *KidAware*, oferecido pela *Super Awesome*. Ao oferecer conteúdos acessíveis e em língua portuguesa, o programa pode democratizar o acesso ao conhecimento técnico e normativo.

Acreditamos, por fim, que este trabalho de pesquisa constitui uma contribuição de grande valia para promoção de uma cultura de desenvolvimento de jogos mais ética e alinhada à proteção de crianças e adolescentes, reforçando a importância da conformidade com princípios fundamentais como o *privacy by design*, a transparência e o melhor interesse da criança e do adolescente em ambientes digitais interativos.

REFERÊNCIAS

ALBUQUERQUE, M. T. **GameGuts: um framework para ajudar o desenvolvedor a escolher, representar, acessar e apresentar dados de gameplay**. Tese (Doutorado) – Centro de informática, UFPE, 2016.

ARIEL EZRACHI; STUCKE,M. Trechos escritos para o Relatório da Comissão Europeia sobre plataformas online e o mercado digital único, IN: EUROPEAN UNION COMMITTEE. **Online Platforms and the Digital Single Market.** House of Lords: publications. parliament.uk 2016. Disponível em: https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12908.htm.

ARUNESH, Mathur et al. **What Makes a Dark Pattern... Dark?** In: CHI ’21: Conference on Human Factors in Computing Systems, Yokohama, 2021. ACM. https://doi.org/10.1145/3411764.3445610

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Balanço 4 anos de atuação da ANPD**. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/anpd-balanco-4-anos.pdf

BARASSI, Veronica. ***Child | Data | Citizen: How Tech Companies Are Profiling Us from Before Birth.*** Cambridge: MIT Press, 2020.

BAUER, Martina; KINDER-KURLANDA, Katharina. *Fairness and Transparency in Digital Games: A Player-Centered Perspective on Loot Boxes and Reward Systems.* In: **Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS)**, 2021. p. 2675–2684.

BIONI, B. *Tratamento de dados pessoais de crianças e adolescentes na LGPD: limites e possibilidades*. In: Doneda, D., & Monteiro, F. (Orgs.). **Lei Geral de Proteção de Dados Pessoais: Comentada.** Thomson Reuters Brasil. 2021

BRIGNULL, H. **Dark Patterns – Deceptive User Interfaces**. 2010. Disponível em: https://www.darkpatterns.org

CAVOUKIAN, A. **Privacy by Design: The 7 Foundational Principles**. Information and Privacy Commissioner of Ontario, 2009. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

CHIU, K.; CHAN, K. Using data mining for dynamic level design in games. **Foundations of Intelligent Systems.** ISMIS 2008. Part of the Lecture Notes in Computer Science book series (LNCS), volume 4994.Springer, Berlin, Heidelber. 2008.Disponível em https://link.springer.com/chapter/10.1007/978-3-540-68123-6_69.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **TIC Kids Online Brasil 2024: principais resultados**. São Paulo: CGI.br, 2024. Disponível em: https://cetic.br/media/analises/tic_kids_online_brasil_2024_principais_resultados.pdf

DEVELOPERS GOOGLE. **Building for Kids**. 2019. Disponível em: https://developer.android.com/google-play/guides/families

EKAMBARANATHAN, A. et al. **“Money makes the world go around”: Identifying barriers to better privacy in children's apps**. In: CHI ’21: Conference on Human Factors in Computing Systems, 2021. ACM. https://doi.org/10.1145/3411764.3445753

EPIC GAMES. **Como faço para completar o processo de consentimento dos pais?** Disponível em: https://www.epicgames.com/help/pt-BR/c-Category_EpicGamesStore/c-EpicAccounts/como-faco-para-completar-o-processo-de-consentimento-dos-pais-a000085549.

EUROPEAN DATA PROTECTION BOARD (EDPB). **About EDPB**. 2024. Disponível em: https://edpb.europa.eu/about-edpb/about-edpb_en

EZRACHI, A.; STUCKE, M. E. **Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy**. Harvard University Press, 2016.

FEDERAL TRADE COMMISSION (FTC). **Children’s Online Privacy Protection Rule ("COPPA")**. 2022. Disponível em: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

FERNANDES, Elora; MEDON, Filipe. **Proteção de crianças e adolescentes na LGPD: desafios interpretativos**. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, v. 4, n. 2, p. 1–20, maio/ago. 2021.

FITTON, D.; READ, J. C. **Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps**. In: IDC ’19: Interaction Design and Children, 2019. ACM. https://doi.org/10.1145/3311927.3323132

FLORIDI, Luciano. **Information ethics: its nature and scope**. ACM SIGCAS Computers and Society, v. 36, n. 3, p. 21–36, 2006.

GAZETA DO POVO. **Multas milionárias: Google rastreou usuários pelo GPS e TikTok expôs crianças.** Gazeta do Povo – Ideias, 2023. Disponível em: https://www.gazetadopovo.com.br/ideias/multas-milionarias-google-rastreou-usuarios-pelo-gps-e-tiktok-expos-criancas/.

GIL, Antonio Carlos; REIS NETO, Aline Crespo dos. **Survey de experiência como pesquisa qualitativa básica em Administração.** *Revista de Ciências da Administração*, Florianópolis, v. 22, n. 56, p. 125–137, 2020. Disponível em: https://periodicos.ufsc.br/index.php/adm/article/view/74026

Google Play Console. (n.d.). *Política de Programa para Desenvolvedores - Política de Família: exemplos de violações comuns*. Google Play Console – Suporte para desenvolvedores. Disponível em: https://support.google.com/googleplay/android-developer/answer/9893335#zippy=%2Cexemplos-de-viola%C3%A7%C3%B5es-comuns

GRAY, C. M. et al. **The Dark (Patterns) Side of UX Design**. In: CHI ’18: Conference on Human Factors in Computing Systems, 2018. ACM. https://doi.org/10.1145/3173574.3174108

HAN, J.; KAMBER, M.; PEI, J. **Data Mining: Concepts and Techniques**. 3. ed. Estados Unidos: Morgan Kaufmann, 2012.

INSTITUTO ALANA; INTERNETLAB. **O direito das crianças à privacidade: obstáculos e agendas de proteção**. São Paulo, 2020.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. The global landscape of AI ethics guidelines. **Nature Machine Intelligence**, [S. l.], v. 1, n. 9, p. 389–399, 2019. DOI: https://doi.org/10.1038/s42256-019-0088-2.

KIDSAFE SEAL PROGRAM. **About the Program**. 2024. Disponível em: https://www.kidsafeseal.com/about.html

LANZI, Pier L. et.al. Tuning mobile game design using data mining. **Games Innovation Conference** (IGIC), 2013. Disponível em: https://www.researchgate.net/publication/261423141_Tuning_mobile_game_design_using_data_mining.

LATERÇA, Priscilla Silva et al. (Coords.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

LEMOS, A.; SILVA, P. R. Apps infantis: vigilância, ludicidade e estratégias de adesão. Comunicação & Educação, São Paulo, PUC-SP, v. 23, n. 1, 2018. Disponível em: https://revistas.pucsp.br/comunicacaoeducacao/article/view/38509.

LESSIG, Lawrence. **Code: version 2.0**. New York: Basic Books, 2006.

LICCARDI, I. et.al. Can apps play by the COPPA Rules? **Twelfth Annual Conference on Privacy, Security and Trust,** 2014. 978-1-4799-3503-1/14/ IEEE. Disponível em: https://people.csail.mit.edu/ilaria/papers/LiccardiPST14.pdf

LIEVENS, E. Children's rights and digital technologies. In: MILKAITE, Ingrida; LIEVENS, E.et. al. (org.). **Children's rights in the digital age: new challenges**. Londres: Routledge, 2018. p. 332–349.

LIVINGSTONE, S. et.al. Children's data and privacy online Growing up in a digital age: an evidence review. **LSE Media and Communication**. London School of Economics and Political Science, 2018. Disponível em: https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

LIVINGSTONE, S. et al. **Digital design for children: Protecting rights in a platform world**. Journal of Children and Media, v. 16, n. 1, p. 1–16, 2022.

LIVINGSTONE, S.; O'NEILL, B. Children's rights online: challenges, dilemmas and emerging directions. In: VAN DER HOF, Simone et al. (org.). **Minding minors wandering the web: regulating online child safety**. Berlin: Springer, 2014. p. 19–38.

LIVINGSTONE, S.; THIRD, A. **Child rights by design: children's rights and digital technologies**. International Journal of Children's Rights, v. 31, n. 1, 2023.

LIVINGSTONE, S., THIRD, A. **Children and young people's rights in the digital age: An emerging agenda**. New Media & Society, 19(5), 657–670.2017

MANKER, Camryn. **Uncovering deceptive patterns in video games**. UX Collective, [s.d.]. 2023. Disponível em: https://uxdesign.cc/uncovering-deceptive-patterns-in-video-games-4ed0b5b9aa68.

MANTELERO, A. **Personal data for decisional purposes in the age of analytics**. Computer Law & Security Review, v. 30, n. 6, p. 569–578, 2014. https://doi.org/10.1016/j.clsr.2014.09.006

MENEZES, C. L.; ALBUQUERQUE, R. M. Apps infantis e publicidade disfarçada: o papel da mediação parental. **Revista Argumentum**, Vitória, UFES, v. 12, n. 2, p. 134–149, 2020. Disponível em: https://periodicos.ufes.br/argumentum/article/view/31297.

MOREIRA, A.V.; VICENTE FILHO, V.; RAMALHO, G.L. Understanding mobile game success: a study of features related to acquisition, retention and monetization. **SBC Journal on Interactive Systems**, v.5, n. 2, p. 2–12, 2014. Disponível em https://seer.ufrgs.br/jis/article/view/45696/31858.

NASCIMENTO, C.; FERNANDES, L**.** Mediando o uso da tecnologia: práticas parentais frente à infância conectada. **Anais do XXXIV Simpósio Brasileiro de Informática na Educação (SBIE 2021).** 2021. Disponível em: https://sol.sbc.org.br/index.php/sbie/article/view/17007.

NEELY, E. L. **Come for the Game, Stay for the Cash Grab: The Ethics of Loot Boxes, Microtransactions, and Freemium Games**. Games and Culture, p. 1–20, 2019. https://doi.org/10.1177/1555412019887658

ODIERNA, B. A. **Identificação e validação dos tipos de jogadores por meio do seu gameplay. 2018**. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Presbiteriana Mackenzie, São Paulo, 2018. Disponível em: https://dspace.mackenzie.br/handle/10899/24485.

ODIERNA, B.; SILVEIRA, I. Player Game Data Mining for Player Classification. SBC – Proceedings of SBGames, 2018 ISSN: 2179-2259. Disponível em:http://www.sbgames.org/sbgames2018/files/papers/CulturaShort/188176.pdf.

PRIVO COPPA Safe Harbor Seal Program. 2024. Disponível em: https://www.privo.com

REYES, Irvin et al. **Won't Somebody Think of the Children? Examining COPPA Compliance at Scale**. Proceedings on Privacy Enhancing Technologies, n. 3, p. 63–83, 2018. Disponível em: https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf

ROBLOX. ***Como denunciar violações de regras.*** Central de Ajuda Roblox, [s.d.]. 2025. Disponível em: https://en.help.roblox.com/hc/pt-br/articles/203312410-Como-denunciar-viola%C3%A7%C3%B5es-de-regras.

SANDOVAL, Melannie. **Child Privacy in the Digital Era: Is COPPA Enough?"** *Joint PIJIP/TLS Research Paper Series*. 131. 2024. https://digitalcommons.wcl.american.edu/research/131

SEIF EL-NASR, M.; KLEINMAN, E. Data-driven game development: Ethical considerations. In: **Proceedings of the 15th International Conference on the Foundations of Digital Games** (FDG '20). ACM.2020.

SEVERINO, A.J. **Metodologia do trabalho científico**. 24. ed. rev. e atual. São Paulo: Cortez, 2016.

SICART, Miguel. **Defining Game Mechanics**. Game Studies, v. 8, n. 2, 2008. Disponível em: https://www.researchgate.net/publication/273946596_Defining_Game_Mechanics

SMITH, G. Understanding Procedural Content Generation: A Design-Centric Analysis of the Role of PCG in Games. In: **Proceedings of the SIGCHI Conference on Human Factors in Computing Systems**. ACM. 2014.

SOLOVE, D. J. **Privacy self-management and the consent dilemma**. Harvard Law Review, v. 126, n. 7, p. 1880–1903, 2012.

STODDEN, V. Regulatory harmonization and the costs of non-conformity. In: **Policy Challenges of the Digital Economy.**2014.

TAKAHASHI, D. **Google Play's new policies for kids' apps aim to improve safety**. VentureBeat, 2021.

TEFFÉ, C. S.de; LATERÇA, P. S.; FERNANDES, E.; BRANCO, S. (Coords.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021 (E-book)

TOGELIUS, J.; YANNAKAKIS, G. N.; STANLEY, K. O.; BROWNE, C. Procedural Content Generation: Goals, Challenges and Actionable Steps. In: **Artificial and Computational Intelligence in Games** (Dagstuhl Follow-Ups, Vol. 6). Schloss Dagstuhl–Leibniz-Zentrum für Informatik. 2016.

VALENTINO-DeVRIES, J. et al. **How Game Apps That Captivate Kids Have Been Collecting Their Data**. The New York Times, 2018. Disponível em: https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html

VAN DER HOF, S.; LIEVENS, E.; MILKAITE, I. The Rights of the Child in the Digital Environment: From Empowerment to Protection. In: LIEFAARD, T.; DOEK, J. E. (Eds.). **Litigating the Rights of the Child**. Springer, 2020. p. 455–475. https://doi.org/10.1007/978-94-6265-391-0_19

WIMMER, M. *A proteção de dados pessoais e os desafios da implementação da LGPD no Brasil*. In: Doneda, D. & Monteiro, F. (Orgs.), **Lei Geral de Proteção de Dados Pessoais: Comentada.** São Paulo: Thomson Reuters.2021.

ZAGAL, J. P. et al. **Dark Patterns in the Design of Games**. In: FDG 2013: Foundations of Digital Games Conference, 2013.

Zendle, D., Meyer, R., & Over, H. *Adolescents and loot boxes: Links with problem gambling and motivations for purchase*. **Royal Society Open Science**, v.6, n.6, 2019. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6599795/.

ZEUX INNOVATION. **The dark side of UX**. Zeux Innovation, [s.d.]. 2022. Disponível em: https://www.zeuxinnovation.com/articles/the-dark-side-of-ux/.

APÊNDICE A

Documento: Guia de boas práticas

	CATEGORIA	ID	PRÁTICA	FONTE	ORIENTAÇÕES COMPLEMENTARES
1	Gerenciamento de dados	BP 1.1	Não coletar dados excessivos ou desnecessários para a funcionalidade da sua aplicação.	Fontes legais	a) Criar ícones e alertas reconhecíveis para indicar “preciso de ajuda”. b) Usar mensagens de áudio ou vídeo para incentivar a criança a buscar um adulto. c) Direcionar a criança a ferramentas de apoio online apropriadas à idade. d) Adaptar a linguagem e funcionalidade conforme as faixas etárias: ● 2–5 anos: recursos visuais e sonoros simples; ● 6–9 anos: reforço visual e encaminhamento com apoio de adulto; ● 10–12 anos: incentivo à autonomia com suporte; ● 13+ anos: recursos de controle e denúncia diretamente acessíveis e) Fornecer recursos para exercício de direitos e acompanhamento de solicitações: ● “Baixar todos os meus dados” – direito de acesso ● “Apagar meus dados” – direito ao apagamento ● “Interromper o uso dos meus dados” – direito à limitação/oposição ● “Corrigir meus dados” – direito à retificação
		BP1.2	Manter os dados apenas no período de tempo razoável e justificável para o propósito para o qual foi coletado.		
		BP1.3	Não enviar para terceiros informações de identificação pessoal, localização ou informações do dispositivo.		
		BP1.4	Permitir ao responsável a possibilidade de apagamento total do dados fornecidos, em qualquer momento.		
		BP1.5	Não usar cookies de rastreamento ou quaisquer outros recursos similares de rastreamento passivo.	Fontes legais, Google Play, App Store	
		BP1.6	Se você permitir que os usuários se registrem com um username, lembre-os de que eles devem evitar usar nomes reais ou identificadores de mídia social existentes.	Google Play, App Store	
		BP1.7	Evite utilizar recursos ou estratégias subliminares para que o jogador compartilhe mais informações do que realmente pretende.	Fontes legais e estudos *dark patterns*	

2	Controle parental	BP2.1	Deixar explícito e acessível um link para acesso da política de privacidade do jogo na página inicial e em cada página em que informações pessoais das crianças são coletadas.	Fontes legais, Google Play, App Store	a) Elaborar uma política de privacidade, focando em: ● Adotar uma linguagem clara, acessível para crianças e seus responsáveis. ● Garantir transparência - informar quais dados são coletados, por quê, como são usados e com quem são compartilhados. ● Explicitar as medidas de segurança adotadas contra acessos indevidos ou vazamentos. ● Informar o prazo de retenção dos dados e quando serão excluídos. b) Revisar e atualizar periodicamente a política de privacidade c) Se possível, implementar notificações just-in-time para informar sobre coleta de dados no momento da interação d) Alguns métodos recomendados, pela lei, para obtenção de consentimento parental verificável são: Formulário assinado e enviado por correio ou eletronicamente ● Transação monetária simbólica, por cartão de crédito, com notificação ao titular da conta ● Contato telefônico ou por videochamada com equipe treinada ● Verificação de identidade por documento oficial (a ser excluído após validação). e) Randomizar perguntas e questões do *parental gate* para evitar memorização pela criança
		BP2.2	Obter consentimento parental verificável antes de qualquer coleta, uso e/ou divulgação de informações pessoais de crianças, alocando de todos os esforços e recursos disponíveis.	Fontes legais, Google Play, App Store	
		BP2.3	Fornecer um meio razoável para que os pais revisem as informações pessoais coletadas de uma criança e se recusem a permitir seu uso ou manutenção.	Fontes legais, Google Play, App Store	
		BP2.4	Incluir *parental gates* em momentos estratégicos para impedir que as crianças façam compras ou sigam links de um aplicativo para sites, redes sociais ou outros aplicativos sem o conhecimento de seus pais ou responsáveis.	Google Play, App Store	
		BP2.5	Incluir um recurso para denunciar conteúdo inadequado no jogo.	App Store	
		BP2.6	Não incluir, fora da parental gate, oportunidades de compra ou outras distrações para as crianças.	Google Play, App Store	

					Nota: O *parental gate* não substitui a obtenção do consentimento parental verificável. São instrumentos com finalidades distintas.
3	Classificação de usuários	BP 3.1	Definir, com clareza a faixa etária do seu público alvo, antes da publicação do jogo.	Google Play, App Store	a) Para facilitar a avaliação da faixa etária do jogo, use classificações oficiais como IARC e realize testes com públicos distintos; b) A tela neutra para verificação de idade deve ser: imparcial e não indutiva, por exemplo, solicite mês e ano de nascimento, sem pre-seleções. O usuário deve selecionar manualmente a data de nascimento via menu suspenso; c) A fim de evitar burlar as informações da tela neutra, pode-se implementar etapas adicionais de verificação (ex.: dados de responsável, pagamento, telefone, e-mail).
		BP 3.2	Declarar, no momento do registro em loja de apps, quais tipos de conteúdo podem ser encontrados no jogo de forma precisa e honesta para fins de classificação.		
		BP 3.3	Antes do jogador iniciar sua primeira sessão, verificar sua idade.		
		BP 3.4	Analisar se há conteúdos, conceitos, temas delicados inadequados à idade segmentada.		
4	Publicidade: geral	BP.4.1	Garantir que todos os SDKs de ads usados são adequados e certificados para crianças e estão em *compliance* com todas as leis aplicáveis.	Fontes legais, Google Play, App Store	a) Para avaliar a adequação dos SDK´s recomenda-se identificar: quais dados estão sendo coletados; a finalidade da coleta; e para onde os dados são transmitidos; b) Em jogos focados em menores de 13 anos, limitar-se o uso de SDKs e APIs de anúncios autocertificados para crianças; c) Em jogos com público misto, não utilizar SDKs ou APIs não certificados, exceto se protegidos por uma tela neutra de verificação de idade; d) Evitar práticas agressivas de publicidade abrange: ● Não usar mensagens de pressão emocional (ex.: “última chance!”, “seus amigos já compraram”) ● Gatilhos sociais e comparações entre usuários
		BP.4.2	Não usar táticas de publicidade impróprias para crianças, como o remarketing ou a publicidade com base em interesses.	Google Play, App Store	
		BP.4.3	Evite usar táticas agressivas de publicidade ou de compras no aplicativo.	Google Play, App Store	

					● Anúncios persistentes e invasivos
5	Publicidade: anúncios	BP 5.1	Diferenciar claramente anúncios do conteúdo do app, por exemplo, destacando a monetização e a publicidade no conteúdo do app usando cores e estilos diferentes.	Google Play, App Store e estudos *dark patterns*	a) Evitar o uso de elementos visuais iguais ou parecidos do jogo para mascarar features de anúncios; b) Evitar anúncios invasivos abrange: ● Não exibir anúncios que ocupem grande parte da tela ou impeçam a interação com o jogo ● Os anúncios devem ter botão visível para fechamento após, no máximo, 5 segundos ● Anúncios que simulam botões “fechar”, mas que redirecionam para outro conteúdo são considerados dark patterns c) Reduzir interrupções e sobreposições de anúncios para preservar a fluidez da experiência; d) A adaptação dos anúncios, conforme a idade do usuário, deve ser feita com base na tela neutra de verificação etária (ver Categoria 3) **Nota:** As recomendações aplicam-se tanto a usuários identificados como crianças; quanto a usuários que a idade não pode ser determinada (então, considera-se como criança)
		BP 5.2	Evitar anúncios invasivos que ocupem a tela inteira ou interfiram no uso normal do app e/ou não oferecem a opção de fechar, após 5 segundo, no máximo.	Google Play, App Store e estudos *dark patterns*	
		BP 5.3	Evitar mais de um anúncio em uma mesma página ou de forma subsequente.	Google Play, App Store e estudos *dark patterns*	
		BP 5.4	Evitar exibir anúncios intersticiais e ofertas para compras no app logo após a abertura. Os usuários precisam experimentar a funcionalidade do seu app ou jogo primeiro.	Google Play e App Store	
		BP 5.5	Evite forçar o jogador a assistir anúncios em troca de recompensas.	Estudos *dark patterns*	
		BP 5.6	Evite exibir anúncios "interstitial" de conteúdos fora do contexto do jogo.	Estudos *dark patterns*	
		BP 5.7	Evite exibir anúncios em formatos e conteúdos impróprios para a faixa etária do seu público.	Google Play, App Store e estudos *dark patterns*	

6	Compras in-game	BP.6.1	Evite dificultar o cancelamento de compras ou assinaturas dentro do jogo.	Estudos *dark patterns*	a) Evitar designs que: ● Ocultem opções de cancelamento ● Exijam múltiplos passos desnecessários para execução de uma tarefa ● Exibam alertas ambíguos que induzam à hesitação b) Garantir clareza e transparência na comunicação de custos e condições de pagamento c) Não ocultar, disfarçar ou adiar informações relevantes sobre compras ou cobranças d) Não priorize a criação de barreiras artificiais e financeiras de progresso que comprometam a experiência *skill-based*; e) Não destacar demais, visualmente, uma opção de compra, induzindo-a como “preferida” ou “superior”.
		BP.6.2	Evite demora para informar ao jogador que ele poderá ter custos adicionais por conta de alguma ação ou do seu engajamento.		
		BP.6.3	Evite adicionar itens não selecionados pelo jogador ao carrinho de compras dele. Exemplo: compra casada.		
		BP.6.4	Evite sugerir compras ao jogador com base em compras anteriores.		
		BP.6.5	Os usuários precisam conseguir diferenciar claramente "moedas" do jogo de valores monetários reais.	Google Play, App Store e estudos *dark patterns*	
		BP.6.6	Evite induzir o jogador a pagar um valor monetário para acelerar ou melhorar seu progresso no jogo.	Estudos *dark patterns*	
		BP.6.7	Evite cobrar do jogador, além do valor pago inicialmente, algum outro valor adicional para que ele tenha acesso a features extras.		
		BP.6.8	Evite apresentar features de compras, de forma hierárquica, ao invés de paralelas, sugerindo que uma opção é melhor que a outra.		

7	Game design: geral	BP 7.1	Evitar pressionar o jogador a jogar recorrendo ao sentimento de que, caso não o façam, estarão perdendo recompensas ou em desvantagem em relação a outros jogadores.	Google Play e estudos *dark patterns*	a) Evitar criar gatilhos emocionais do tipo *fear of missing out*; b) Buscar priorizar a autonomia do jogador sobre quando deseja jogar, não impondo “eventos obrigatórios”; c) Evite nudges manipulativos de interface, como por exemplo, destaques visuais assimétricos (opção “continuar” em grande destaque vs. botão “não continuar” pequeno e apagado); d) Garantir que as estrutura gramatical das frases seja clara e diretas, compreensíveis para diferentes tipos de leitores
		BP 7.2	Evite estimular ações e comportamentos no jogo que, na vida real, seriam considerados antiéticos.	Estudos *dark patterns*	
		BP 7.3	Evite exigir ao jogador períodos de tempo ou datas específicas para jogar, dando flexibilidade ao jogador.		
		BP 7.4	Evite exigir que o jogador realize tarefas monótonas de forma recorrente para progredir no jogo.		
		BP 7.5	Evite deixar qualquer opção de feature pré-selecionada, influenciando a escolha do jogador.		
		BP 7.6	Evite fazer perguntas enganosas que possam ter duplo sentido ou interpretação ambígua.		

8	Game design: recompensas	BP 8.1	Não condicionar o acesso ou recompensa da criança à divulgação de informações pessoais a mais do que o necessário.	Fontes legais	a) Priorizar a adoção de sistemas de recompensas baseados em previsibilidade e modelos estatísticos; b) Buscar priorizar a autonomia do jogador sobre quando deseja jogar, não impondo “eventos obrigatórios”;
		BP 8.2	Evite recompensar o jogador de forma aleatória ou inesperada para viciá-lo no jogo. Preferir recompensas regulares e previsíveis.	Estudos *dark patterns*	
		BP 8.3	Evite oferecer recompensas ao jogador ou penalizá-lo em função dele jogar diariamente.		
		BP 8.4	Evite usar recursos de recompensas como loot boxes, gambling ou quaisquer outros que possam ser classificados como jogos de azar.	Fontes legais e estudos *dark patterns*	
9	Game design: social features	BP 9.1	Evite incentivar os jogadores a convidar amigos para ingressarem no jogo em troca de recompensas.	Estudos *dark patterns*	a) Implantar etapas de validação por um adulto para permitir acesso a funcionalidades que envolvam troca de informações pessoais com terceiros: PIN ou senha dos pais, verificação por e-mail, documento oficial, dados de cartão de crédito; b) Não priorize a exploração dos vínculos sociais do jogador, em detrimento ao progresso *skill-based*; c) Evite enviar notificações excessivas que possam ter caráter de spam
		BP 9.2	Evite forçar o jogadores a jogarem recorrendo ao sentimento de culpa ou senso de responsabilidade com amigos e/ou equipe dentro do jogo.	Google Play, App Store e estudos *dark patterns*	
		BP 9.3	Evite enviar aos jogadores mensagens não solicitadas comunicando ações em nome de seus amigos ou sua rede de contatos.	Estudos *dark patterns*	

APÊNDICE B

Formulário aplicado ao *survey*

Developing games for kids: thinking about practices*

Graduate Program in Computer Science
- UFPE
Student: Natália R. Barreto
Prof. Dr. Geber Ramalho

We invite you to participate in the study "Best Practices for an Ethical Development of Games for Kids" which aims to identify ethically recommendable practices in digital game development for children and teenagers. Current laws, store policies, and academic literature suggests some best practices, but to what extent they make sense from the developer point of view?

Responses are anonymous and will be analyzed for a master's dissertation. Thank you for your participation!

*This questionnaire is a summarized and revised version of the original questionnaire "Developing games for youngers: Good & Bad practices".

Estimatedtime: **15-20 minutes**.

1. How many years have you worked in the gaming market? *

   Marcar apenas uma oval.

   - ◯ 4-7 years
   - ◯ 7-10 years
   - ◯ More than 10 years

2. What is the location/country of the company you work for? *

3. Which area of game development most closely matches your current office job? *

Marcar apenas uma oval.

- ◯ Production/Management
- ◯ Game Design
- ◯ Programming
- ◯ Marketing
- ◯ Art Design
- ◯ Data Analysis/Data Science

4. Which genre of games are you currently developing in last years? *

Marque todas que se aplicam.

- ☐ Casual (puzzle, arcade, simulation etc)
- ☐ Mid-core (MMO, MOBA, RPG etc)
- ☐ Sports
- ☐ Casino
- ☐ Other

What is the main group of players of the games you have been developing? *

Marcar apenas uma oval.

- ◯ Just for kids & teens (up to 16)
- ◯ Teens (13-16 years) and general public (+18)
- ◯ Just for general public (18+)

HOW MUCH DO YOU AGREE?

Thank you for the previous information! You have reached the second part of the questionnaire.

Imagine that you are developing a game for an audience of children and/or under 16´s. In this context, we´d listed 9 categories of practices. In the question related to each category, we´ll present some options of practices. According to your experience, you should judge which ones would you consider relevant to keep in mind for your product.

1) DATA MANAGEMENT refers to the collection, processing, storage, and use of * personal data in a transparent manner, respecting the privacy rights of individuals, and implementing security measures to prevent violations or minimize potential harm. (COPPA/GDPR).

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 4 practices**.

Marque todas que se aplicam.

- [ ] Do not collect excessive or unnecessary data for the functionality of your application.
- [ ] Maintain data only for a reasonable and justifiable period of time for the purpose for which it was collected.
- [ ] Do not send personally identifiable information, location, or device information to third parties.
- [ ] Allow the responsible party the option to delete all provided data at any time.
- [ ] Do not use cookies or any other similar passive tracking features.
- [ ] If you allow users to register with a username, remind them to avoid using real names or existing social media identifiers.
- [ ] Avoid using subliminal features or strategies that cause the player to share more information than they actually intend to.

2) PLAYER CLASSIFICATION refers to the system used by online stores to categorize and evaluate apps based on content appropriateness, age suitability, and user feedback. (Google Play Store) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 2 practices**.

Marque todas que se aplicam.

- [ ] Clearly define the age range of your target audience before the game is published.
- [ ] Declare, at the time of app store registration, what types of content can be found in the game in a precise and honest manner for classification purposes.
- [ ] Verify the player's age before they start your first session player.
- [ ] Analyze whether there are any content, concepts, or sensitive themes inappropriate for the targeted age group.

3) PARENTAL CONTROL refers to the practices and mechanisms that allow parents or guardians to control and monitor the online activities of their minor children. (COPPA) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 4 practices**.

Marque todas que se aplicam.

- [ ] Clearly and accessibly provide a link to the game's privacy policy on the homepage and on every page where personal information from children is collected.
- [ ] Obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, utilizing all available efforts and resources.
- [ ] Provide a reasonable means for parents to review the personal information collected from their child and refuse its use or maintenance.
- [ ] Include parental gates at strategic moments to prevent children from making purchases or following links from the app to websites, social media, or other apps without their parents' or guardians' knowledge.
- [ ] Include a feature to report inappropriate content in the game.
- [ ] Do not include, outside of the parental gate, purchase opportunities or other distractions for children.

4) ADVERTISING refers to any practice or marketing activity aimed at promoting products or services. (COPPA) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 2 practices**.

Marque todas que se aplicam.

- [ ] Ensure that all ad SDKs used are appropriate and certified for children and comply with all applicable laws.
- [ ] Do not use inappropriate advertising tactics for children, such as remarketing or interest-based advertising.
- [ ] Avoid using aggressive advertising or in-app purchase tactics.

5) ADS in ADVERTISING refers to any promotional content displayed within apps, including graphic ads, videos, and other forms of advertising designed to promote products or services. (Google Play Store) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 4 practices**.

Marque todas que se aplicam.

- [ ] Clearly differentiate ads from the app content, for example, by highlighting monetization and advertising within the app using different colors and styles.
- [ ] Avoid intrusive ads that take up the entire screen or interfere with normal app usage and/or do not offer the option to close after 5 seconds at most.
- [ ] Avoid displaying more than one ad on the same page or in succession.
- [ ] Avoid showing interstitial ads and in-app purchase offers immediately after opening the app. Users should experience the functionality of your app or game first.
- [ ] Avoid forcing players to watch ads in exchange for rewards.
- [ ] Avoid displaying interstitial ads for content that is out of context with the game.
- [ ] Avoid displaying ads in formats and content that are inappropriate for your target age group.

6) IN-APP PURCHASES refers to the monetary transactions made within apps that allow users to access additional content or features, such as virtual items in games, subscriptions, and premium upgrades. (Google Play Store) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 4 practices**.

Marque todas que se aplicam.

- [ ] Avoid making it difficult to cancel purchases or subscriptions within the game.
- [ ] Avoid delaying the notification to the player that they may incur additional costs due to some action or engagement.
- [ ] Avoid adding items not selected by the player to their shopping cart. For example: product bundling.
- [ ] Avoid suggesting purchases to the player based on previous purchases.
- [ ] Users should be able to clearly distinguish "game coins" from real-world monetary values.
- [ ] Avoid prompting the player to pay a monetary amount to speed up or improve their progress in the game.
- [ ] Avoid charging the player, in addition to the initial payment, any extra fee to access additional features.
- [ ] Avoid presenting purchase features in a hierarchical manner instead of parallel options, implying that one is better than the other.

7) GAME DESIGN refers to the creation of game mechanics and systems to provide engaging experiences, which, through design decisions, may influence player behavior. (Zagal, 2019) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 4 practices**.

Marque todas que se aplicam.

- [ ] Avoid pressuring the player to play by creating the feeling that, if they don't, they will miss out on rewards or be at a disadvantage compared to other players.
- [ ] Avoid encouraging actions and behaviors in the game that, in real life, would be considered unethical.
- [ ] Avoid requiring players to play at specific times or on specific dates, offering flexibility instead.
- [ ] Avoid requiring players to perform repetitive, monotonous tasks in order to progress in the game.
- [ ] Avoid leaving any feature options pre-selected, influencing the player's choice.
- [ ] Avoid asking misleading questions that could have double meanings or ambiguous interpretations.

8) REWARDS in GAME DESIGN refers to the benefits that players receive when performing certain actions or achieving specific goals within a game. (Zagal, 2019) *

Concerning about this topic, which practices below do you consider most relevant? **Choose a maximum of 2 practices**.

Marque todas que se aplicam.

- [ ] Do not condition a child's access or reward on the disclosure of personal information beyond what is necessary.
- [ ] Avoid rewarding the player in random or unexpected ways to get them hooked on the game. Prefer regular and predictable rewards.
- [ ] Avoid offering rewards to the player or penalizing them based on daily play.
- [ ] Avoid using reward mechanisms such as loot boxes, gambling, or any others that may be classified as games of chance.

9) SOCIAL FEATURES in GAME DESIGN refers to design features in games that involve or encourage interaction between players. (Zagal, 2019) *

Concerning this topic, which practices below do you consider most relevant? **Choose a maximum of 2 practices**.

Marque todas que se aplicam.

- [ ] Avoid encouraging players to invite friends to join the game in exchange for rewards.
- [ ] Avoid forcing players to play by appealing to feelings of guilt or a sense of responsibility toward friends and/or teammates within the game.
- [ ] Avoid sending unsolicited messages to players communicating actions on behalf of their friends or contact network.