GUIA

LGPD E GAMES

NÚMERO 9/10

A Year in Privacy

Autores:

Ana Clara Moreira Pinheiro

Gustavo Luz

Juliana Almeida

Mariana Pires Monteiro

Matheus Botsman Kasputis

Natália Góis Ribeiro

Rafaella Resck Braoios

Revisão Técnica:

Fernando Bousso

Odélio Porto Júnior

Projeto Gráfico:

Fernanda Muchon

Lucas Bittencourt

‹voltar para o índice

Introdução

Este Guia analisa os principais elementos e riscos de privacidade e proteção de dados presentes nas práticas de mercado atuais da indústria dos games. Em primeiro lugar, é analisado o perfil do tratamento de dados pessoais na indústria e avaliado como determinados modelos de negócio, tecnologias e dispositivos para coleta de dados pessoais podem impactar a privacidade e proteção dos dados dos jogadores. Em sequência, são descritos os principais fluxos de dados pessoais existentes entre os players da indústria, envolvendo marketplaces e fornecedores de tecnologias. Por fim, há aprofundamento em casos práticos em que houve a concretização de riscos mais comuns e usos indevidos de dados pessoais envolvendo jogadores.

‹voltar para o índice

01 Perfil do Tratamento de Dados Pessoais na Indústria de Games

1.1. Modelos de negócio e jogabilidade

Apenas em 2021, um total de 2.66 bilhões de jogadores gastaram, em conjunto, o correspondente a 116 bilhões de dólares em games, especificamente nas versões mobile.[1] Há diferentes modelos de negócio para monetização de games, de modo que cada um atende a um nicho específico de jogadores e ganham níveis distintos de popularidade. De forma geral, os jogos podem ser divididos em:

- *paid games;*
- *free games;*
- *freemium games;*
- *paymium games.*

Os *paid* games são aqueles em que o usuário paga para a aquisição do jogo e passa a ter acesso, em geral, ilimitado ao seu conteúdo, sendo este o modelo mais antigo e tradicional do mercado.

No que se refere ao segundo modelo, os free games, a monetização ocorre principalmente por meio da veiculação de publicidade nos jogos. O acesso e o aproveitamento do jogo em si são gratuitos para o usuário, sendo este o alvo de publicidade de terceiros. Para a monetização dos free games, importa o número de impressões e conversões a partir da publicidade feita nas plataformas.

Os *freemium* games, por sua vez, correspondem aos jogos disponibilizados gratuitamente, mas que condicionam a evolução e o aprimoramento da experiência dos jogadores a microtransações dentro do jogo. Os *freemium* games são gratuitos apenas em certa medida, pois a liberação de determinados conteúdos no jogo só ocorre mediante pagamento (p. ex.: expansões de conteúdo, itens para os personagens do jogo etc.). Como exemplo disso, vale ressaltar o caso que foi recentemente noticiado sobre a criança de 11 anos que gastou cerca de 30 mil reais no cartão do seu pai em compras feitas no jogo Roblox[2].

Já os *paymium* games podem envolver tanto a compra inicial do jogo como pagamentos posteriores por meio de micro transações (para acesso a determinados conteúdos) e/ou por meio de assinatura com pagamentos regulares.

---

1 LAPERDRIX, Pierre et al. The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem. ACM Web Conference 2022, abr. 2022, Lyon, p. 2. Disponível em: <https://hal.archives-ouvertes.fr/hal-03559973/document>. Acesso em 16 set. 2022.

2 Johns, TIM. Dad horrified at £4,642 gaming app bill. The Jeremy Vine Show. BBC NEWS. Disponível em: <https://www.bbc.com/news/business-53272411>. Acesso em: 16 set. 2022.

Independentemente do modelo de monetização, a captação de dados pessoais passa a ser um recurso cada vez mais utilizado e necessário para tornar o jogo um serviço contínuo. **Quanto mais se conhece quem está do outro lado da tela, maiores são as chances de obter o engajamento do usuário.**

Entendendo o perfil dos jogadores, as empresas distribuidoras (*publisher*[3]) e/ou desenvolvedoras (*developer*[4]) conseguem atender aos interesses e expectativas, bem como influenciar de forma direta e indireta o comportamento do seu público-alvo. Partindo deste ponto, uma das maiores problematizações que circundam o tema é que grande parte deste público se trata de crianças e adolescentes.

Em razão disso, o debate regulatório de jogos é tema presente em diversos países, como as restrições impostas pela China às empresas de tecnologia devido a restrições de uso de games online por menores de idade para combate ao vício[5], e regulamentações como a Portaria MJSP nº 502/2021 sobre classificação indicativa, publicada pelo Ministério de Justiça e Segurança Pública do Brasil.

1.2. Dispositivos e tecnologias para a coleta de dados pessoais

A indústria de games se vale de diversos tipos de dispositivos e meios tecnológicos para fornecer seus serviços, sendo os principais por meio computadores, consoles domésticos (videogames) e smartphones.

De fato, a 9ª edição da Pesquisa Games Brasil, conduzida em 2022, demonstra que os smartphones foram o dispositivo mais utilizado entre os jogadores brasileiros em 2021, seguido dos computadores (23,3%) – na soma entre desktops e notebooks – e, finalmente, dos consoles domésticos (20%).[6] Tais dados refletem a transformação da indústria de games e a multiplicidade de meios de acesso a jogos disponível atualmente.

Ao mesmo tempo em que os meios de acesso se ampliam, os dados pessoais dos jogadores passam a ser coletados também por diferentes formas, a depender do dispositivo utilizado. A indústria ainda nascente de hardware de

3 Empresa responsável pela publicação/lançamento do jogo, distribuição, e, eventualmente, financiamento de empresas desenvolvedoras.

4 Empresa responsável pelo desenvolvimento/criação direta do jogo. Em determinados casos, uma mesma empresa pode ser tanto uma publisher como developer.

5 MACHKOVECH, SAM. Dozens of Chinese phone games now require facial scans to play at night. Arstechnica, 07 jul. 2021. Disponível em: <https://arstechnica.com/gaming/2021/07/chinas-largest--game-publisher-uses-facial-scans-to-enforce-youth-curfew/>. Acesso em 16 set. 2022.

6 Pesquisa Games Brasil. Pesquisa de Games Brasil. 2022, p. 12. Disponível em: < https://www.pesquisagamebrasil.com.br/pt/edicao-gratuita/>. Acesso em 15 set. 2022.

realidade virtual tem experimentado novas formas de disponibilização de jogos, principalmente por meio de óculos de realidade virtual, o que permite novas formas de coleta de dados pessoais dos jogadores.[7]

Como exemplo de nova experiência de jogabilidade e realidade virtual, pode-se citar o jogo Pokémon Go, que permite a coleta da geolocalização de jogadores, pois o jogo se integra com a localização física da pessoa. É comum também a coleta de dados de voz, por meio do microfone, em funcionalidades como abas de conversas e chats online.

Registra-se, ainda, alguns dispositivos que buscaram maior integração com o jogador, como foram os casos de *Kinect* (Microsoft), *Wii* (Nintendo) e *Playstation Move* (Sony). Estes dispositivos funcionavam por meio de mecanismos de controle sensível e captura de movimentos dos jogadores, coletando dados como voz, vídeo, gestos, expressões faciais e geolocalização[8]

1.3. Finalidades de uso e tratamento por inferência

Nos últimos anos, os modelos de negócios da indústria de games passaram por consideráveis mudanças. Com o objetivo de se adaptar à demanda da indústria de jogos, tornaram-se crescentes os investimentos no desenvolvimento de ferramentas que permitem o monitoramento dos hábitos e comportamento dos jogadores.

Em um primeiro momento, os esforços da indústria estiveram concentrados em coletar dados de usuários a partir de métodos tradicionais, como a realização de pesquisas e entrevistas junto aos jogadores.

Com o advento da internet e o desenvolvimento de tecnologias de realidade virtual, tornou-se possível o monitoramento de usuários à distância e a coleta de dados como, por exemplo, voz, biometria facial, rastreamento ocular *(eye tracking*) e geolocalização.

Além das informações fornecidas diretamente pelo usuário ao criar uma conta no jogo e interagir com outros participantes – como, por exemplo, nome, data de nascimento, localização, perfil em redes sociais, cartão de crédito e histórico de conversas –, as tecnologias adotadas por jogos (conforme descrito no subcapítulo 1.2 acima) também são capazes de revelar informações sobre o usuário a partir da análise de padrões comportamentais e combinações estatísticas. Tais análises permitem inferir a identidade, idade e gênero,

7 RASCHKE, Philip et. al. Surveilling the Gamers: Privacy Impacts of the Videogame Industry. [S. l.: s. n.], jul. 2021. Disponível em: <https://www.researchgate.net/publication/353025657_Surveilling_the_Gamers_Privacy_Impacts_of_the_Video_Game_Industry>. Acesso em 20 set. 2022.

8 RUSSEL, N. Cameron; REIDENBERG, Joel R.; MOON, Sumyung. Privacy in Gaming. Fordham Law Legal Studies. Nova York, 19 mar. 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147068> Acesso em 15 set. 2022.

emoções, habilidades e conhecimentos, perfil de consumo, situação financeira, traços da personalidade e informações sobre a saúde do jogador.

A título de exemplo, as informações acima podem ser inferidas a partir da análise do estilo de jogo do usuário – *i.e.*, o curso das suas ações em jogos de estratégia, perfil de direção em jogos de corrida, tendência à compra de itens adicionais no jogo. Além disso, é possível identificar o jogador a partir do cruzamento dos nomes de usuário adotados em diferentes jogos e outras informações coletadas.

A coleta de dados pessoais pode ocorrer em diversos momentos durante a jornada do usuário nas plataformas de jogos, servindo para o atingimento de interesses primários das empresas desenvolvedoras dos jogos – como, por exemplo, para customização e melhorias de jogabilidade, solução de erros ou falhas na operação do software, detecção de trapaças/*cheats* etc.

É possível, entretanto, que a coleta de dados pessoais dos usuários ocorra também para finalidades secundárias, como, por exemplo, para conhecimento das características psicológicas e vulnerabilidades dos jogadores, que permitam o desenvolvimento de estratégias com objetivo de, entre outros:

- incentivar a compra de itens virtuais e conteúdo premium;
- aumentar as microtransações realizadas pelos usuários durante as rodadas dos jogos;
- elevar o tempo dedicado pelo jogador aos seus títulos favoritos; e
- ofertar produtos e serviços (publicidade direcionada) ao usuário durante a sua jornada nos jogos considerando seus hábitos de consumo, idade e gênero, por exemplo.

Outros usos possíveis dos dados pessoais coletados durante a jornada do usuário estão relacionados aos compartilhamentos dessas informações com terceiros, tais como redes de *streaming* de jogos, birôs de dados, ferramentas de análise de dados, instituições governamentais e plataformas de publicidade, que poderão tratar os dados pessoais para finalidades próprias, conforme aplicável.

‹voltar para o índice

02 O Fluxo de Dados Entre os Agentes da Indústria

2.1. Marketplaces e regulação privada

As desenvolvedoras, distribuidoras e outros agentes da indústria de games têm de se preocupar com ecossistemas jurídico-regulatórios de proteção de dados pessoais das mais diversas jurisdições onde disponibilizarão os seus jogos. Não só isso, também devem ficar atentas às mais diversas regulações privadas aderidas pelos *marketplaces* (p. ex.: Apple Store e Google Play), incluindo políticas e diretrizes para desenvolvedores, que contêm regras de privacidade e proteção de dados específicas.

Recomendações da Unicef
Além de todas as disposições específicas das diretrizes dos marketplaces, destacamos como boa prática as Recomendações da Unicef para a indústria de games na avaliação de impacto às crianças[9], pois trazem quesitos concretos para uma implementação mais protetiva de uso de dados pessoais nos jogos, bem como para o desenvolvimento de comunidades mais acolhedoras e adequadas para cada faixa etária de jogadores.

Abaixo, destacamos alguns dos principais *marketplaces* de games e suas disposições específicas de privacidade e proteção de dados.

APPLE APP STORE

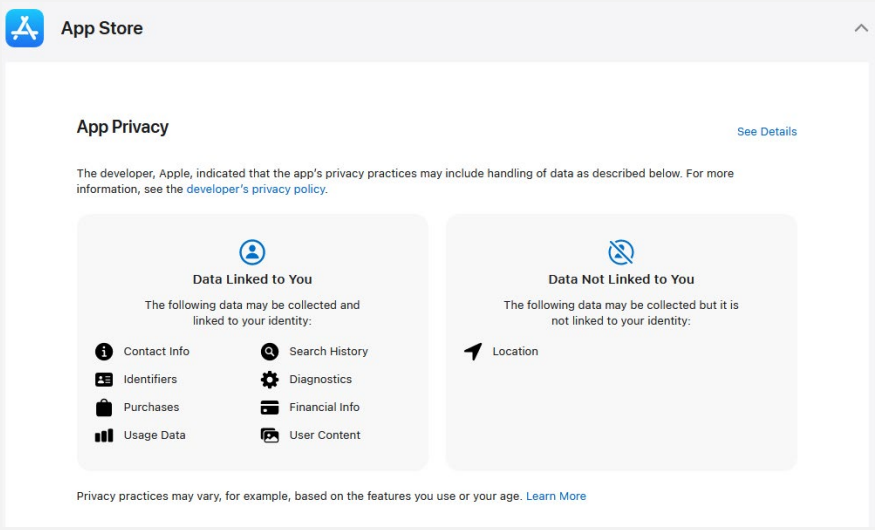
A Apple utiliza kit de desenvolvimento de software (*software development kit* - SDK) proprietário além de sistemas operacionais e hardware próprios para ter – e manter – estrito controle sobre o desenvolvimento e os recursos utilizados pelos apps e games em seu marketplace.[10] A App Store tem a pretensão de ser uma loja de apps e games segura e confiável aos seus usuários, com as aplicações passando por processo prévio de aprovação.

Em atualizações mais recentes de seus sistemas operacionais, a Apple determinou em suas diretrizes[11] algumas medidas centrais para que os usuários sejam mais bem informados e protegidos, quais sejam:

9 UNICEF. Recommendations for The Online Gaming Industry on Assesssing Impact on Children. Abril, 2020. Disponível em: <https://sites.unicef.org/csr/css/Recommendations_for_Online_Gaming_Industry.pdf>. Acesso em 21 set. 2022.
10 FEIJOO, Claudio et al. Mobile gaming: Industry challenges and policy implications. Telecommunications Policy, v. 36, n. 33, abr. 2012, p. 04. Disponível em: <https://core.ac.uk/download/pdf/148663771.pdf>. Acesso em 20 set. 2022.
11 Apple. Apple App Store Guidelines. Disponível em: <https://developer.apple.com/app-store/guidelines/>. Acesso em 20 set. 2022.

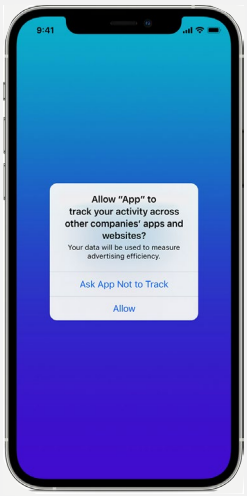
A. *Privacy labels* (rótulos de privacidade)

De acordo com a Apple, a máxima em termos de privacidade é a transparência.[12] Para facilitar a compreensão de quais dados são utilizados, a Apple determina que sejam criados rótulos simples de privacidade, que descrevem quais tipos de dados pessoais do titular são utilizados . Por exemplo, o rótulo de privacidade da própria App Store:



B. Solicitação de permissões, em especial para rastreamento

Constantemente, o usuário de apps encontra um pop-up em que o desenvolvedor solicita a permissão para uso de algum tipo de dado pessoal, por exemplo, de geolocalização. Além dessas permissões usuais, a Apple implementou um *framework* de transparência sobre rastreamento cruzado em apps e sites utilizados pelo usuário por meio do smartphone, que ocorre para fins de publicidade direcionada[13]:



12 Apple. Apple Privacy Labels. Disponível em: <https://www.apple.com/privacy/labels/>. Acesso em 20 set. 2022.

13 Apple. Apple Support – If an app asks to track your activity. Disponível em: <https://support.apple.com/en-us/HT212025>. Acesso em 20 set. 2022.

Ademais, as diretrizes de desenvolvedor da Apple determinam que, a não ser que seja permitido por lei ou para fins de melhoria do app e oferecimento de publicidade, o desenvolvedor não deve compartilhar dados pessoais sem a obtenção prévia de consentimento do usuário.

C. Obrigatoriedade de botão com solicitação de exclusão de conta

A solicitação de exclusão de contas deve ser facilitada, devendo o desenvolvedor dispor de um botão para essa finalidade. A Apple determina que o desenvolvedor ofereça a exclusão permanente da conta e de todos osdados associados ao app, inclusive pessoais – ressalvados os casos em que o desenvolvedor deva reter dados que se façam necessários para o cumprimentodas leis aplicáveis. Importante notar que a opção de desabilitar ou desativar temporariamente a conta é insuficiente para essa diretriz específica da Apple.

D. Obrigatoriedade de link para a política de privacidade

As diretrizes para desenvolvedores determinam de forma expressa que haja um link acessível para a política de privacidade tanto no app como na App Store.

E. Crianças

Utilizando do padrão GDPR e COPPA (*Children's Online Privacy Protection Act*, legislação estadunidense), a Apple determina em suas diretrizes que os apps direcionados para crianças não devem incluir analytics e publicidade de terceiros. Há diversas outras diretrizes mais específicas da Apple, inclusive sobre design.

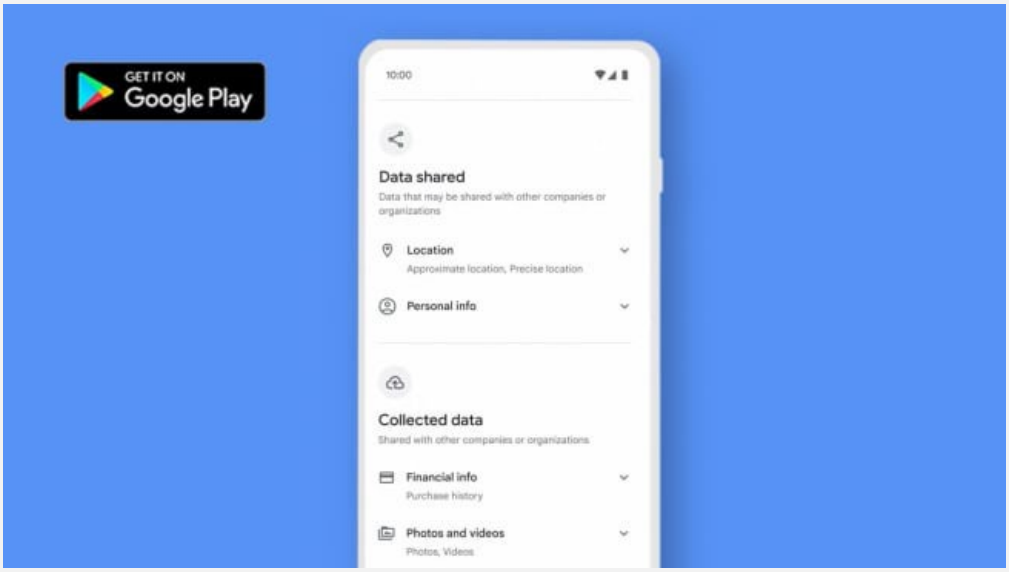
GOOGLE PLAY STORE

Com relação às diretrizes da Google Play Store, destacamos as seguintes:

A. Segurança dos dados

Bem semelhante aos *privacy labels* da App Store, o Google determina que os desenvolvedores disponham de uma seção clara e precisa nos apps, que detalhe a coleta, o uso e o compartilhamento de dados do usuário, em linha com a política de privacidade.[14]

14 Google. Fornecer informações para a seção "Segurança dos dados" do Google Play. Disponível em <https://support.google.com/googleplay/android-developer/answer/10787469?hl=pt-BR>. Acesso em 21 set. 2022.



B. Obrigatoriedade de link para a política de privacidade

Todos os apps precisam incluir um link para a política de privacidade no campo designado na Google Play Store e outro link ou texto de acesso facilitado à política no próprio app.[15] Porém, apps que atestam não utilizar de dados pessoais não precisam cumprir com esse requisito.

C. Publicidade direcionada

Para fins de publicidade direcionada[16], o Google exige que haja informações claras e documentadas na política de privacidade do app, sendo vedado o uso de dados de localização para uso publicitário. Ademais, o Google proíbe a utilização de anúncios invasivos, sendo vedado forçar um usuário a clicar em um anúncio ou enviar informações pessoais para fins publicitários antes de usar o app por completo.

Se um usuário solicitou opt-out de publicidade direcionada, sua preferência deve ser respeitada pelos desenvolvedores de apps.

Vale destacar que o uso do identificador de publicidade do Android só é permitido para publicidade e análise de perfil do usuário, sendo vedada a conexão do identificador do Android com outros identificadores permanentes, como o código IMEI de um celular, o que possibilitaria a identificação do usuário.

---

15 Central de Políticas do Play Console. Privacidade, fraude e uso indevido de dispositivos > Dados do usuário. Disponível em: <https://support.google.com/googleplay/android-developer/answer/10144311?hl=pt-BR&ref_topic=9877467>. Acesso em 21 set. 2022.

16 Central de Políticas do Play Console. Monetização e anúncios > Anúncios. Disponível em: <https://support.google.com/googleplay/android-developer/answer/9857753>. Acesso em 21 set. 2022.

D. Alterações nas configurações do dispositivo

Apps que fazem alterações nas configurações do dispositivo sem o consentimento prévio e expresso do usuário não são permitidos.[17] Por exemplo, é vedado que apps modifiquem as configurações ou os recursos do dispositivo, como um serviço para terceiros ou para fins de publicidade, ou que induzam os usuários a remover ou desativar apps de terceiros ou modificar configurações ou recursos do dispositivo.

E. Crianças

Em geral, a publicidade é permitida pelo Google. Mas se crianças forem um dos públicos-alvo do app, este app não pode incluir um SDK que não foi aprovado para uso em apps feitos para crianças.[18] Ou seja, os SDKs devem ser certificados pelo Google Play cumprindo com, dentre outros requisitos específicos, não se utilizar de localização exata, não tratar determinados dados, como o identificador de publicidade do Android e outros dados específicos relacionados ao aparelho que a criança utiliza etc.

Destacamos que o conteúdo também deve ser apropriado para a faixa etária das crianças e que não ocorra práticas de publicidade direcionada e *remarketing* nos apps.

MICROSOFT STORE

As diretrizes da Microsoft[19] tem como principais pontos:

A. Classificação adequada

Games devem estar categorizados de acordo com gêneros e categorias apropriadas com base nas funções e recursos oferecidos pelo app.

B. Obrigatoriedade de link para a política de privacidade

A Microsoft ressalta que a transparência é central, especialmente no quesito de uso de dados pessoais. Portanto, exige que haja link para a política de privacidade do game, podendo ser hospedada dentro do game ou o link ser externo.

---

17 Central de Políticas do Play Console. Privacidade, fraude e uso indevido de dispositivos > Comportamento enganoso. Disponível em: >https://support.google.com/googleplay/android-developer/answer/9888077?hl=pt-BR&ref_topic=9877467>. Acesso em 21 set. 2022.

18 Central de Políticas do Play Console. Família > Como criar apps para crianças e famílias. Disponível em: <https://support.google.com/googleplay/android-developer/answer/9893335>. Acesso em 21 set. 2022.

19 Microsoft. Microsoft Store Policies. Disponível em: <https://learn.microsoft.com/en-us/windows/uwp/publish/store-policies>. Acesso em 21 set. 2022.

C. Exigência de criptografia

A Microsoft exige a utilização de métodos modernos de criptografia para que um app ou game realize a coleta, armazenamento e transmissão de dados pessoais.

D. Consentimento

- Para oferecimento de compras na Microsoft Store: os desenvolvedores, com o consentimento do usuário e após o download inicial do game, podem viabilizar o oferecimento, dentro do game, de (i) outros games e apps desenvolvidos pela mesma desenvolvedora, desde que sejam oferecidos pela própria Microsoft Store também, e (ii) compras dentro do app (in-app purchases) diversas, como extensões e adicionais que melhoram a funcionalidade do jogo.
- Para alteração de quaisquer configurações dos dispositivos: o consentimento deverá ser obtido para que quaisquer configurações, especialmente de interface com o usuário (UI), sejam alteradas nos sistemas operacionais da Microsoft.

E. Vedação de uso de dados sensíveis

A Microsoft veda a utilização de dados sensíveis, definidos exemplificativamente como dados de saúde e dados financeiros, a não ser que tais dados sejam necessários para os recursos do app; nesse caso, o consentimento prévio e expresso é exigido.

F. Segurança

Os games não devem comprometer a segurança dos seus usuários ou dos dispositivos, devendo ser adequadamente testados e certificados para disponibilização na Microsoft Store. Nenhum recurso de segurança do dispositivo deverá ser desabilitado ou alterado e o usuário deve ser extensamente informado sobre questões de segurança do app.

G. Desinstalação

O game deve comunicar de forma clara e permitir que um usuário desinstale e remova o app do dispositivo de forma simples. Não há diretrizes específicas sobre a exclusão de conta ou de dados pessoais

FACEBOOK GAMING

Motivados pelo acordo final da Meta com o FTC[20] (*Fair Trade Commission*, o regulador de concorrência, consumidor e proteção de dados dos EUA), a Meta reforçou suas práticas e exigências de privacidade. Destacamos, entre elas[21]:

- Orientações mais claras aos desenvolvedores sobre o uso e o compartilhamento de dados.
- Construir novas ferramentas e controles para responsabilização dos desenvolvedores;
- Aqui, se destaca o processo anual de Verificação de Uso de Dados exigido pela Meta, no qual os desenvolvedores devem analisar os tipos de dados aos quais têm acesso por meio das APIs da Plataforma do Facebook e confirmar que seu uso de dados está em conformidade com os termos e políticas e com as leis aplicáveis. Essa medida é basilar nos esforços *de accountability* da Meta.
- Personalização dos processos de integração e de análise do aplicativo para melhorar a experiencia dos desenvolvedores.
- Incentivo à melhoria na experiência do usuário pelo oferecimento de orientações adicionais sobre as políticas de uso de dados para proporcionar aos usuários uma experiência positiva em seu aplicativo.
- Os Termos da Meta foram atualizados para definir uma estrutura em dois níveis para os dados que os desenvolvedores recebem: dados da plataforma e dados restritos da plataforma. Isso serve para limitar as informações que os desenvolvedores podem compartilhar com terceiros sem o consentimento explícito dos usuários e fortalece a proteção dos dados do usuário no ecossistema do Facebook Gaming e da Meta.
- A política para exclusão de dados está mais clara, destacando que os desenvolvedores devem excluir os dados quando "eles não forem mais necessários para fins comerciais legítimos, se o desenvolvedor parar de operar o produto ou serviço, se solicitar a exclusão ou se os dados forem recebidos pelo desenvolvedor por erro".
- Exigência de notificação de violação de dados, com início imediato de solução do incidente e cooperação com a Meta.

Destacamos que a Meta dispõe de diretrizes claras sobre como deve ocorrer a obtenção de um consentimento válido para uso de cookies, nos termos do GDPR.[22] Ademais, há diretrizes específicas sobre viabilizar login em games, com enfoque no oferecimento de explicações/contexto quando da solicitação de permissões.[23]

---

20 Meta. Final FTC Agreement Represents a New Level of Accountability for Privacy. Abril, 2020. Disponível em: <https://about.fb.com/news/2020/04/final-ftc-agreement/>. Acesso em 21 set. 2022.

21 Meta for Developers. Simplificação dos nossos Termos da Plataforma e Políticas do Desenvolvedor. Junho, 2020. Disponível em: <https://developers.facebook.com/blog/post/2020/07/01/platform-terms--developer-policies/>. Acesso em 21 set. 2022.

22 Meta for Developers. Guia de consentimento para uso de cookies. Disponível em: <https://developers.facebook.com/docs/privacy>.

23 Meta for Developers. Melhoras práticas - Jogos. Disponível em: < https://developers.facebook.com/docs/games/build/legacy-web-games/best-practices#providecontextforpermissions>. Acesso em 21 set. 2022.

2.2. Cadeia de desenvolvimento de jogos

O desenvolvimento de games nem sempre é realizado exclusivamente por uma só empresa. Muitas etapas da cadeia de desenvolvimento de um jogo, como a (i) criação, produção e publicação, (ii) entrega, distribuição e acesso, (iii) uso, consumo e interação e (iv) monitoramento e aprimoramento, podem contar com a participação de fornecedores para operacionalizar algumas funções, incluindo *APIs/SDKs, game engines*[24]*, business intelligence e microtargeting*.

Para fins de redução de custos, é comum a utilização de ferramentas de terceiros no desenvolvimento de jogos. Em determinados casos, os terceiros que oferecem essas ferramentas podem ter interesses nos dados pessoais dos jogadores e ter acesso direto a tais dados em razão dos serviços desenvolvidos.

Dentro do ecossistema de games, a coleta de dados, análise de dados, *profiling* dos jogadores e publicidade estão intrinsecamente ligados e há uma infinidade de atores, que podem ser divididos em quatro categorias principais[25]:

- Desenvolvimento de jogos;
- Operações;
- Crescimento;
- Análise de mercado.

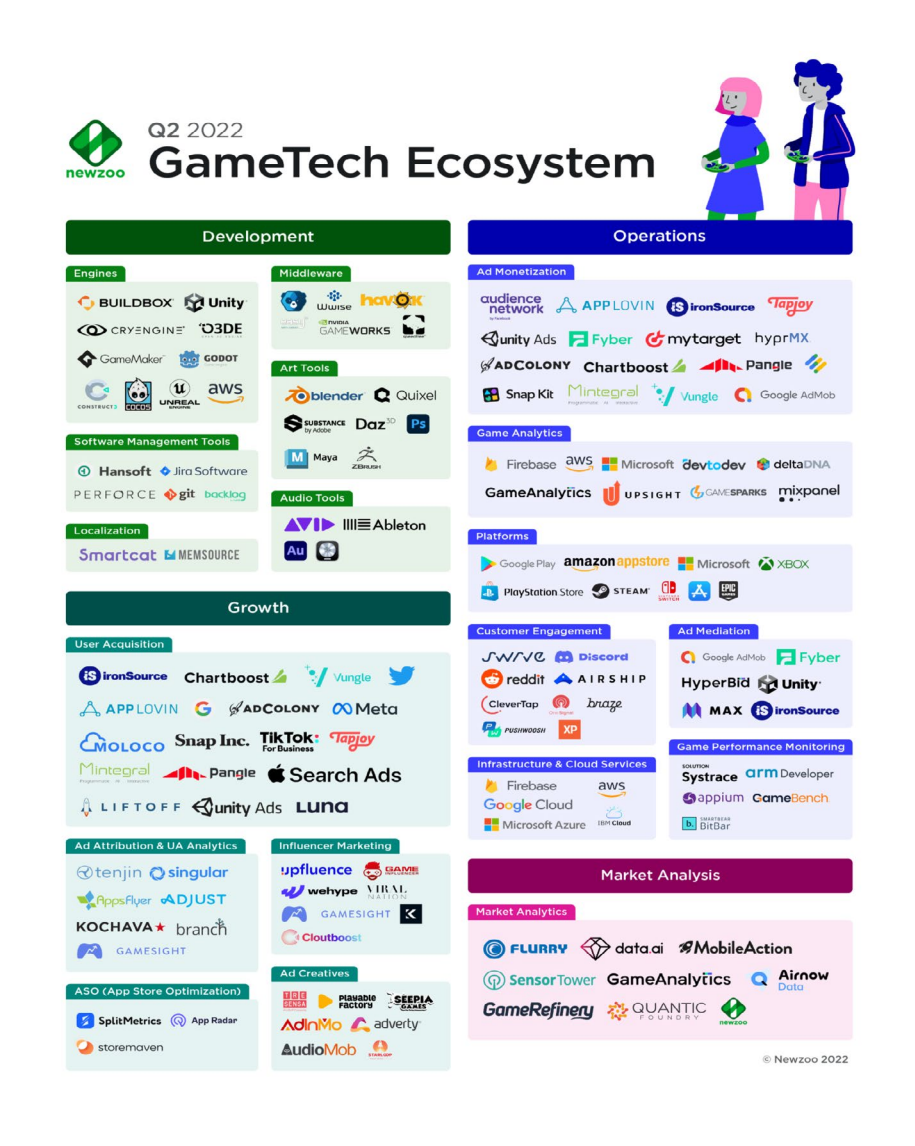
Os jogos têm se tornado tão universais e complexos que novas tecnologias – e até mesmo subsetores inteiros – surgiram para apoiar no seu desenvolvimento. O diagrama da GameTech, elaborado pela Newzoo, é um exemplo da profundidade e da escala desse ecossistema, exemplificando as tecnologias e análises que empresas usam para dar suporte à criação de jogos[26].

---

24 Software projetado para auxiliar no desenvolvimento de jogos, fornecendo principalmente ferramentas de renderização para gráficos 2D ou 3D, mecanismos de física e detecção de colisão para uso na estrutura do jogo, animação, sons, entre outros.

25 DATA ETHICS.EU. Op. cit.

26 Newzoo. Newzoo Gametech Ecosystem. 31 Mai. 2022. Disponível em: <https://newzoo.com/insights/infographics/gametech-ecosystem-map-technology-game-creation-supply-chain>. Acesso em 15 de set. 2022.



Fonte: https://newzoo.com/insights/infographics/gametech-ecosystem-map-technology-game-creation-supply-chain/

Qualquer desenvolvimento, lançamento e aprimoramento de um game bem-sucedido requer a cooperação de diferentes atores em cada uma dessas etapas[27]. Portanto, a preocupação em relação ao compartilhamento de dados pessoais dos jogadores é um passo essencial para diminuir o risco de tratamento de dados indevidamente e até mesmo incidentes.

Os games coletam e geram enormes quantidades de informações sobre seus jogadores, muitas das quais podem ser consideradas críticas. Esses dados incluem voz, aparência física, sua localização, rede social, e detalhes das ações do jogador no jogo, que podem ser analisadas para criar perfis aprofundados das habilidades cognitivas e da personalidade de um jogador. Tais informações podem ter usos dentro e fora do ecossistema de games[28].

Estima-se que cada aplicativo envia dados para pelo menos 10 terceiros em média[29].

27 FEIJOO, Claudio et. al. Op cit.

28 DATA ETHICS.EU. Op. cit.

29 Ibid.

Basicamente, as empresas de desenvolvimento de jogos podem compartilhar dados pessoais de jogadores de forma bastante ampla e para diversas finalidades, como[30]:

- Cumprimento da lei;
- Monitoramento de comportamento;
- Resolução de problemas de serviço;
- Aprimoramento no desenvolvimento do jogo;
- Garantia de pagamento;
- Viabilização da comunicação entre jogadores;
- Fornecimento de informações publicitárias e promocionais aos jogadores.

É possível identificar o compartilhamento de dados pessoais entre os diversos atores responsáveis pelo desenvolvimento e operacionalização dos games, como programadores individuais sob contrato (em qualquer lugar do mundo), plataformas, processadores de pagamento, ferramentas de SDK e API, serviços de infraestrutura e nuvem, *call centers* para suporte técnico, provedores, *middleware*, ferramentas de gerenciamento de arte, áudio e software e ferramentas de engajamento em tempo real. Os dados podem ainda ser compartilhados com anunciantes para promover e aprimorar a micro segmentação de anúncios, por meio da análise dos interesses dos usuários e de suas atividades durante uma partida de jogo.

No entanto, muitas vezes informações claras sobre o compartilhamento de dados pessoais podem ser difíceis de serem obtidas até mesmo para os desenvolvedores de jogos, uma vez que muitos games usam ferramentas e serviços fornecidas por terceiros, principalmente por SDKs, os quais podem compartilhar informações com outros terceiros de forma pouco transparente.[31]

Devem ser realizadas due diligences em privacidade e proteção de dados previamente à contratação de cada um dos fornecedores, visando avaliar o grau de conformidade com a legislação de proteção de dados aplicável.

Além da avaliação de fornecedores no momento da contratação, é importante ainda gerenciar, de forma contínua e periódica, a conformidade dos fornecedores à legislação aplicável a proteção de dados. Conduzir análises de segurança e patrocinar manutenção e monitoramento contínuos fazem parte do ciclo de monitoramento do fornecedor.

30 Office of the Privacy Commissioner of Canada. Op cit.

31 RUSSEL, N. Cameron; REIDENBERG, Joel R.; MOON, Sumyung. Op cit.

Conjuntamente, é fundamental que as empresas de desenvolvimento de jogos e outros atores do ecossistema definam as condições de uso de dados pessoais relativos aos jogadores. Após a avaliação de conformidade do fornecedor/terceiro, o contrato entre as partes deve conter cláusulas de proteção de dados pessoais adequadas.

A compreensão sobre a função de cada agente em relação aos dados pessoais tratados é crucial para garantir a conformidade com a legislação de proteção de dados, uma vez que as obrigações variam dependendo se o agente atua como controlador, controlador conjunto ou operador[32]. A questão chave é qual ou quais atores dentro do ecossistema de games determinam as finalidades para as quais os dados são tratados e os meios de tratamento.

Em relação à segurança dos dados pessoais, ainda que seja um aspecto mais técnico e menos jurídico, deve-se assegurar que todos os sistemas e equipamentos que são utilizados para desenvolver e armazenar os games possuam níveis mínimos de segurança. Isso inclui não apenas a proteção contra-ataques de terceiros, mas também implementação de mecanismos de governança na própria empresa, realizando treinamento com colaboradores, limitando e controlando acesso a materiais sensíveis etc.

Por fim, uma vez que os fluxos de dados pessoais vão além do desenvolvedor e distribuidor, dar transparência aos jogadores sobre o compartilhamento com terceiros é fundamental. Em muitos casos os jogadores podem ter dificuldade em compreender quem realmente são os agentes de tratamento utilizando os seus dados, mesmo depois de ler as políticas de privacidade relevantes. Portanto, a linguagem das políticas de privacidade deve ser o mais acessível e didática possível.[33]

32 Information Commissioner's Office. Controllers and processors. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/>. Acesso em 16 de set. de 2022.
33 RUSSEL, N. Cameron; REIDENBERG, Joel R.; MOON, Sumyung. Op cit.

‹voltar para o índice

03 Game Over: os Riscos Comuns Relativos à Segurança da Informação

Segundo informações obtidas em 2020 pela Akamai[34], empresa de tecnologia com expertise em soluções de segurança digital, o setor de jogos foi o que teve maior crescimento no índice de ataques, com um volume de ameaças maiores em 340% do que o registrado em 2019. Contra os jogadores, o aumento foi de 224% nas tentativas de intrusão a contas a partir de credenciais vazadas. Golpes desse tipo, somados ao uso de e-mail de phishing para roubo de informações, foram os maiores golpes em 2020.

Por exemplo, em julho de 2022, uma brecha afetou o site Neopets, levando à exposição de informações de 69 milhões de pessoas, bem como ao acesso indevido ao código-fonte e sistemas internos do game[35]. O responsável pelo vazamento divulgou uma pequena amostra do conteúdo de banco de dados na *dark web*, que continha informações como nomes, e-mail, gênero, datas de nascimento, senhas criptografadas, dados de localização e informações do perfil de cada jogador. É preciso levar em consideração que o público-alvo deste jogo é majoritariamente infantil, o que pode tornar as consequências do incidente ainda mais danosas.

De acordo com o Relatório sobre o Direito das Crianças à Privacidade, do Instituto Alana em parceria com o InternetLab[36], crianças estão especialmente sujeitas ao uso indevido de seus dados e a riscos digitais, como manipulação comportamental – e por isso é tão importante garantir que mecanismos de segurança sejam implementados durante o desenvolvimento e disponibilizaçãodo game.

34 AKAMAI. Gaming – Segurança não é um jogo solo. 2020, p. 15. Disponível em: <https://www.akamai.com/pt/thank-you/soti-security-gaming-you-cant-solo-security-report>. Acesso em 15 set. 2022.

35 DEMARTINI, Felipe. Vazamento do game Neopets expõe 69 milhões de pessoas. CanalTech, 22 jul. 2022. Disponível em: < https://canaltech.com.br/seguranca/vazamento-do-game-neopets-expoe-69-milhoes-de-pessoas-221389/ >. Acesso em 15 set. 2022.

36 INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020. Disponível em: < https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-ala-na_criancas-privacidade_PT_20210214-4.pdf >. Acesso em 16 set. 2022.

‹voltar para o índice

04 Recomendações e Boas Práticas à Indústria

Com base nas questões levantadas acima, seguem os principais pontos de atenção em relação a privacidade e proteção de dados para as empresas do ecossistema de games:

1. Considerar aspectos de privacidade e proteção de dados desde as etapas iniciais de desenvolvimento do game, adotando metodologias como o *privacy by design* e *privacy by default*.

2. Realizar avaliações prévias de privacidade e de proteção de dados pessoais dos fornecedores, principalmente quanto ao uso de SDKs e APIs.

3. Avaliar as regras de privacidade e proteção de dados das lojas de aplicativos e demais marketplaces nos quais o jogo será disponibilizado.

4. Aplicar medidas adequadas de segurança da informação, considerando as principais ameaças e vulnerabilidades identificadas na indústria e a sensibilidade dos dados pessoais tratados, visando, sobretudo, à detecção e prevenção de riscos.

5. Implementar programas de conscientização junto aos colaboradores envolvidos no desenvolvimento dos games.

6. Considerando o crescimento no índice de ataques à indústria, elaborar campanhas informativas aos jogadores para conscientização e promoção de práticas de segurança.

7. Adotar medidas de transparência reforçadas para as atividades de tratamento de dados realizadas com base em inferências ou em usos secundários, garantindo maior controle individual aos jogadores.

8. Considerar a adoção de medidas específicas direcionadas ao tratamento de dados crianças e adolescentes, com base em seu melhor interesse, considerando a vulnerabilidade e o estágio de desenvolvimento em que se encontram.

9. Preparar análises de risco, como Relatórios de Impacto à Proteção de Dados, para o jogo em si ou para novas funcionalidades, principalmente se houver dados pessoais sensíveis ou de crianças.

Conclusão

Como exposto, a indústria de games é um segmento crescente e estruturado em torno de diversos modelos de negócio, baseados em diferentes categorias de jogos e estratégias de monetização, de maneira que o modelo escolhido pelo desenvolvedor tem impacto direto na privacidade e tratamento de dados pessoais dos jogadores. Jogos podem coletar um volume significativo de dados pessoais de seus jogadores para diversas finalidades (publicidade, aumento de engajamento, desenvolvimento de novos produtos e serviços, etc).

Além disso, a ampliação dos meios disponíveis para jogar – como smartphones e dispositivos de realidade virtual ou aumentada – diversificam as possibilidades de coleta de dados pessoais. Essas novidades motivam o uso secundário de dados pessoais pelos desenvolvedores para finalidades mais sofisticadas, como inferências sobre a saúde, medição de habilidades, conhecimentos, e hábitos de consumo dos jogadores.

A indústria de games, também, é bastante horizontalizada em serviços secundários indispensáveis, como, por exemplo, para inteligência de negócio, marketing, desenvolvimento de software e segurança da informação. É comum, portanto, que haja o compartilhamento de dados pessoais dos jogadores com os terceiros responsáveis por essas atividades em conjunto com as desenvolvedoras dos games. Nesse cenário vale destacar as plataformas para oferta de games no mercado (marketplaces) - como a Apple App Store, Google Play – que exigem requisitos específicos de privacidade e proteção de dados pessoais.

Esses fatores, somados aos riscos de segurança da informação, requerem tanto de desenvolvedores como de jogadores a adoção de certos cuidados e ações preventivas para evitar incidentes de segurança envolvendo dados pessoais.

Assim, verifica-se que o ecossistema de desenvolvimento de games exige a atuação de diversos atores para que os dados pessoais dos jogadores sejam utilizados de forma adequada, em conformidade com as legislações de proteção de dados pessoais aplicáveis.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br