

# **Paradoxo da privacidade na Amazônia: Como usuários de smartphone cuidam de sua privacidade e segurança on-line**

## **Privacy Paradox: How smartphone users take care of their online privacy and security**

Hinton Hennington Portilho Bentes Neto

*Mestrando do Programa de Pós-Graduação em Ciência da Informação (PPGCI) na Universidade Federal do Pará (UFPA). Administrador, Diretor da Conselho de Jovens Empresários da Associação Comercial do Estado do Pará (2009-2013), Presidente do Sindicato dos Administradores do Estado do Pará (2013-2016), Diretor do Instituto de Estudos Sustentáveis e Tecnológicos da Amazônia, Professor da Faculdade Estácio de Castanhal. Especialista em Gestão de Empreendimentos Agroindustriais – Universidade do Estado do Pará.*  
Email: [hinton@amazoniatec.com.br](mailto:hinton@amazoniatec.com.br)

Raffael Amado da Silva Vieira

*Publicitário, atualmente é professor do Curso Superior de comunicação Social da Faculdade Estácio do Pará, Curso de Design de Moda de Faculdade Estácio do Pará e do curso de Design Gráfico de Faculdade Estácio do Pará; Coordenador da Agência Experimental de Publicidade e Propaganda (CARBONO) da Faculdade Estácio do Pará. Especialista, mestrando em Administração e Desenvolvimento Empresarial da Universidade.*  
Email: [raffael.vieira@estacio.br](mailto:raffael.vieira@estacio.br)

Haslã dos Santos Duda

*Diretor Faculdade Estácio do Pará, Especialista, mestrando em Administração e Desenvolvimento Empresarial da Universidade.* Email: [hasla.duda@estacio.br](mailto:hasla.duda@estacio.br)

Antonio Augusto Goncalves

*Atualmente é professor do programa de Mestrado em Administração da Universidade Estácio de Sá e chefe da área de Tecnologia de Informação do Instituto Nacional do Câncer. Foi Gerente de Processos e Sistemas de Bancos e Seguradoras. É membro do comitê de Pesquisa de Iniciação Científica da UNESA. Bolsista de produtividade em pesquisa da UNESA. Possui Projeto de auxílio a Pesquisa aprovado pela FAPERJ (APQ1). Doutor em Engenharia de Produção pela COPPE - Universidade Federal do Rio de Janeiro.*  
Email: [antonio.goncalves@estacio.br](mailto:antonio.goncalves@estacio.br)

### **Resumo**

*A popularização dos smartphones tem evoluído bastante nas primeiras décadas do século XXI, o que gerou também a oportunidade mercadológica para o uso deste tipo de equipamento para o entretenimento, o objetivo deste artigo é realizar um levantamento do comportamento dos gamers de smartphones do Estado do Pará na preservação da privacidade de seus dados e sua segurança on-line, sendo que a metodologia da pesquisa foi baseada no modelo netnográfico aplicados em redes sociais, especificamente em grupo de gamers de jogos online, o resultado evidenciou a existência do paradoxo da privacidade nestes grupos de usuários de smartphones uma vez que 30% jogam por mais de 3 horas diárias e 77% não utiliza aplicativo de análise estática e 10% dos respondentes armazenam senhas no smartphone sem qualquer criptografia, sendo assim pode-se concluir que o paradoxo da privacidade é uma ação que ocorre concomitante entre o saber o que deve ser feito e realmente realizar a ação, mesmo sabendo que a omissão poderá acarretar sérios problemas futuros na preservação da informações pessoais.*

### **Palavras-Chave**

*Informação; Telefonia móvel; Sistema de informação.*

## Abstract

*The popularization of smartphones has evolved considerably in the first decades of the 21st century, which also generated the market opportunity for the use of this type of equipment for entertainment, the purpose of this article is to conduct a survey of the behavior of smartphone gamers in the State of Pará in preserving the privacy of your data and your online security, and the research methodology was based on the netnographic model applied in social networks, specifically in a group of online game gamers, the result evidenced the existence of the privacy paradox in these groups of smartphone users since 30% play for more than 3 hours a day and 77% do not use a static analysis application and 10% of respondents store passwords on the smartphone without any encryption, thus it can be concluded that the paradox of privacy is an action that occurs concurrently between knowing what should be done and actually carrying out the action. No, even though the omission could cause serious future problems in the preservation of personal information.*

## Keywords

*Information; Mobile telephony; Information system.*

## Introdução

Durante as primeiras décadas do século XXI foi possível identificar um significativo crescimento do número de usuários de smartphones pela população mundial e brasileira e consequentemente as empresas prestadoras de serviço buscam ferramentas para que o cliente permaneça mais tempo on-line possível e uma das alternativas encontradas foi a oferta de serviços e aplicativos a estes usuários Harris e Blair (2006).

Estudos como este são importantes uma vez que eles buscam demonstrar a convergência que a sociedade tem realizado ao longo das primeiras décadas do século XXI e a conectividade com os dispositivos tecnológicos as mais diferentes questões que antes eram rotineiras e independentes como a mobilidade urbana, alimentação e gastronomia, cuidados com o sono e saúde conforme estudado por Arruda Filho; Gammarano e Barreto (2019), Bilali e Allahyari (2018) e Aledavood, Torous, Hoyos (2019).

As projeções do Instituto Brasileiro de Geografia e Estatística (IBGE) para a população brasileira em 2020 são entre 209 a 217 milhões de pessoas, já para o Estado do Pará são mais de 8.500 milhões e o número de usuários de smartphones segundo a Agência Nacional de Telecomunicações (ANATEL), postado em seu Portal de Transparência<sup>1</sup>, já foram realizados no Brasil 227,21 milhões de acessos de telefonia móvel (Serviço Móvel Pessoal – SMP) e no Estado do Pará 4,5 milhões de acessos até o mês de fevereiro de 2020, onde neste mesmo período houve o consumo por 32,6 milhões de usuários no Brasil e no Pará 334 mil pessoas de banda larga.

Agora quando avaliado o contexto da relação do usuário de smartphones com a preservação da segurança de dados quando se encontra on-line é possível identificar um comportamento chamado de “*paradoxo da privacidade*”, que seria uma contraposição entre a conduta de preservação da privacidade frente ao seu procedimento conforme visto em Barth; Jong; Junger Hartel; Roppelt (2019).

Neste contexto é importante salientar que a avaliação de produtos de segurança da informação para computação em nuvem possui uma metodologia em constante mudança, uma vez que todos os processos recorrem em testes e execução e análise de padrões e especificações de segurança conforme indicado por Mohr e Walter (2019).

Estudos recentes a interrelação que existe em jogos nas redes virtuais desenvolvidas tanto para consoles como smarthphones e estes tendo acesso à internet, compartilhando

---

<sup>1</sup> <https://www.anatel.gov.br/paineis/acessos> - Acessado em 26 de março de 2020

experiências de jogos entre gerações e alguns deles inclusive gratuitos em um primeiro momento, e o jogador evolui a relação business-to-consumer com a aquisição de bens virtuais demonstra a sua interrelação e até mesmo caso de dependências como visto em Gammarano (2018) e Balakrishnan; Griffiths (2019)

Dentre as muitas lacunas existentes na literatura, este trabalho visa contribuir que empresas de varejo com base no entendimento de jogos possam analisar o padrão de comportamento, preferência de consumo e tendências visando perspectivas e anseios de seus clientes, Arruda Filho; Gammarano (2018).

Tendo em vista estes números robustos de crescimento tanto do número de usuários de serviços ligados a telefonia móvel, conseqüentemente vemos a possibilidade de um crescente número de usuários de aplicativos, assim buscou-se fazer analisar como este perfil business-to-consumer, usuários de jogos de smartphone, pode ser impacto a luz do paradoxo da privacidade.

Sendo nossa questão problema principal a identificação do comportamento de usuários de jogos de smartphone frente a questão de sua privacidade e nosso objetivo de pesquisa visa responder a questões sobre como estes gamers preservam, ou não, sua segurança on-line.

Muito tem sido debatido pelo tema de segurança da informação e tecnologias ligadas ao smartphone, todavia não consta na literatura estudos direcionados para um estudo comportamental sobre os hábitos e costumes de usuários de aplicativos de jogos para smartphone e como estes cuidam de sua privacidade e segurança on-line dentro da Amazônia brasileira, sobretudo do Estado do Pará a luz do paradoxo da privacidade.

Alinhado a estes conceitos o paradoxo da privacidade e a segurança da informação vem como teorias principais para este trabalho visando consolidar a temática sobre o comportamento do gamer, ou seja, usuário de smartphones que o utiliza para jogos on-line, ainda não havia sido aferido de forma a rarear as conexões entre os conceitos teóricos e as comprovações quantitativas, podendo fazer assim um levantamento do gap entre o que o gamer sabe que deve ser feito com o real comportamento do mesmo.

Para estudo foi recorrido um procedimento de pesquisa quantitativa para o diagnóstico da conduta e da salvaguarda e segurança on-line dos dados contidos nos smartphones do gamers que vivem no Estado do Pará.

Este experimento incorreu através procedimentos netnográfico com entrevistas estruturadas de modo experimental de caso único aplicado nas redes sociais utilizadas para encontro destes usuários.

Sobre os resultados desta pesquisa, foi possível ver que realmente a geração alpha, possui uma interatividade grande frente aos jogos eletrônicos, cerca de 27% como esperado, assim como as gerações Z, Y, X que já iniciaram e vivem este tipo de conectividade entre o dia-a-dia e o uso dos smartphones demonstram uma participação de 23%, contudo neste levantamento de perfil gamer até mesmo a geração baby-boomer se fez presente com 3% na pesquisa, demonstrando que realmente o uso de jogos eletrônicos é de interesse de todas as gerações. Mas quando se analisam estes dados de forma mais aprofundada como veremos a seguir a questão da preservação da informação ainda é muito tímida em um contexto geral.

## **Revisão da Literatura**

Quando se realiza uma pesquisa neste perfil é importante alinhar os conceitos principais para que seja possível nortear o levantamento, assim como consolidar os conceitos de forma técnica além da aplicação dos dados estatísticos que serão aqui apresentados.

Doravante a questão do paradoxo da privacidade é possível ver que esta é uma temática antiga que remeta-se a diversos estudos comportamentais das sociedades ao longo dos anos como os jogos de videogames, assim como a segurança da informação que no final do século XX e início do XXI tem sido alinhado mais a questões cibernéticas dentro das relações de consumo on-line que esta relação que será estudada aqui no modelo business-to-consumer de jogos para smartphones mostram sua importância para a questão do entretenimento das mais diversas classes sociais e das mais diferentes faixas etárias, todavia a partir que estamos no ambiente virtual todos estão sujeitos aos crimes cibernéticos.

**Quadro 1 - Referências temáticas**

<b>TEMAS</b>	<b>CONCEITOS</b>	<b>AUTORES</b>
Paradoxo da Privacidade	<i>“discrepância entre a atitude dos usuários em relação à privacidade e seu comportamento real”</i>	Barth; Jong; Junger; Hartelad; Roppelt (2019)
Segurança na informação	<i>“garantir a singularidade e imparcialidade dos resultados da avaliação”</i>	Hao Song (2020)
Videogames	<i>“desenvolver um ambiente de diversão e conectividade de jogos”</i>	Arruda Filho; Gammarano (2019)
Jogos para smartphone	<i>“os jogos continuaram evoluindo tanto nos jogos que são jogados quanto nas plataformas nas quais eles podem ser jogados”</i>	Balakrishnan; Griffiths (2019)

Fonte: Elaborado pelos autores

Quando é escrutada a questão analítica sobre como os gamers consomem jogos de base tecnológica ainda há muito a se estudar, uma vez que esta temática ainda é muito árida no mundo e quando realizamos um estudo de contexto específico e aplicado como o neste artigo é possível identificar uma série de conexões possíveis e ainda não devidamente realizadas.

## **Metodologia**

Este estudo foi esquadrihado em meio a um projeto de pesquisa quantitativa e assim realizada uma análise de dados primários, visando apresentar uma descrição do comportamento e da preservação da privacidade de seus dados e sua segurança on-line que os gamers de smartphones do Estado do Pará realizada durante o mês de março de 2020.

Ocorrendo de modo experimental de caso único, onde aplica-se em grupo específico visando identificar o comportamento deste grupo, além de coadjuvar para a compreensão dos acontecimentos organizacionais, através de uma descrição hodierna do método utilizado através desta apuração empírica para identificar os seguintes óbices o que, quem, quem, onde e como (Cooper e Schindler, 2003; Yin, 2003).

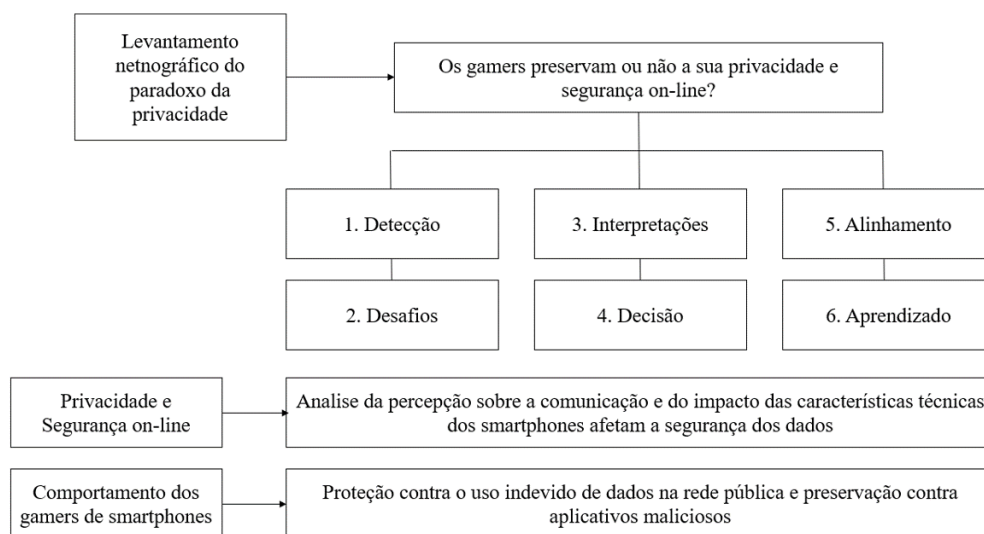
Sendo aplicado o questionário elaborado no programa Microsoft Forms buscando identificar duas situações que seriam norteadoras para a pesquisa, onde indicou-se como H1: Os gamers não preservam sua privacidade e segurança on-line e H2: Os gamers preservam sua privacidade e segurança on-line. Assim busca-se analisar não os jogos, mas sim, uma investigação das percepções em torno de um jogo para smartphone e o comportamento do gamer para a preservação de sua segurança.

## **Pesquisa Netnográfico com Usuários de Smartphones**

O método utilizado foi baseado em entrevistas estruturadas através do modelo

netnográfico para o envio dos convites onde as principais bases de convite foram Facebook, grupos de usuários de jogos de smartphones, grupos de WhatsApp, de usuários de jogos e grupos de interesses gerais, através do LinkedIn em grupos de usuários de jogos online e grupos de interesses gerais, onde foram aplicadas 18 questões identificando o perfil do usuário e seu comportamento na preservação de dados pessoais.

**Gráfico 1** - Elementos-chave do enquadramento estratégico



Fonte: Elaborado pelos autores

O referido questionário foi dividido em 03 etapas, a primeira na identificação do usuário (idade, sexo e grau de escolaridade), a segunda etapa se ocorre pela reconhecimento do equipamento que possui e seus cuidados quanto a segurança da informação e na terceira etapa utilizou-se uma questão de escala likert, para identificar a percepção do usuário sobre a preservação de seus dados cadastrais em seu smartphones.

Identificamos o perfil de jogadores casuais, que passam menos de 01 horas por dia jogando e de elevado desempenho, que passam mais de 03 horas jogando, neste momento a ideia não era de identificar o jogo ou jogos que estes usuários utilizam e sim o grau de segurança que estes jogadores possuem e utilizam em seus aplicativos e smartphones.

## Modelo Estatístico Utilizado

A escolha do teste estatístico apropriado requer conhecimentos sobre: Classificar o tipo de dado que está estudando (contínuo, categórico: ordinal ou nominal); como esses dados estão distribuídos após o término da sua coleta (Distribuição Normal ou Distribuição Anormal), e os tipos de amostras examinadas (Independentes ou Dependentes).

Para o artigo foi utilizado os tipos de dados contínuo, de forma de uma distribuição normal e as amostras examinadas Independentes, dessa forma foi utilizada um teste de hipóteses da média.

## Resultados

De acordo com a pesquisa a primeira etapa foi buscar uma identificação das pessoas que optaram em responder ao questionário. Podemos perceber que a maioria das pessoas que responderam o questionário são do sexo masculino, representando 80% do grupo e os 20% complementares são do sexo feminino. Vale ressaltar que o público feminino vem crescendo no ambiente de gamers, mas a predominância é masculina, branca e heterossexual conforme apontado por Job, Kurtz, Fortim (2019).

Quando analisamos a idade dos participantes que responderam ao questionário percebemos que a geração alpha possui a maior fatia do bolo, surpreendentemente 1 pessoa é da geração BB, mas o que nos chamou a atenção é que a grande maioria dos gamers estão concentrados nas gerações X, Y e Z, conforme demonstrado na tabela I.

**Tabela 1 – Faixa Etária**

<b>FAIXA ETÁRIA</b>	<b>RESPONDENTES</b>	<b>AV</b>
Abaixo de 18 - Geração ALPHA	8	27%
Entre 26 e 18 - Geração Z	7	23%
Entre 38 e 27 - Geração Y	7	23%
Entre 53 e 39 - Geração X	7	23%
Maior de 54 anos - Geração BB	1	3%

Fonte: Resultados da pesquisa

O fato que chama atenção, foi que a grande maioria (60%) dos respondentes possuem nível superior ou uma pós graduação, o que nos remete que são pessoas que possuem trabalho e família e ainda assim conseguem disponibilizar alguma hora do seu tempo para jogar no smartphones, a geração X tem como característica além da idade, pessoas que vivenciaram vários cenários econômicos, o empreendedorismo e qualificação técnica são marcantes nesta geração, que também trouxe um empoderamento feminino por reconhecimento social.

A geração Y é a mais suscetível aos jogos eletrônicos, pois também é conhecida como a geração da Internet. Essa geração, diferente da X, surge numa época, mas sofisticada, com grandes avanços tecnológicos e com um cenário econômico mais estável. A geração Z nasce na velocidade do conhecimento, pois a velocidade de informações que eles recebem e conseguem armazenar é muito mais rápida. De uma forma mais clara se compararmos a velocidade absolvidas pela geração Z em relação aos Baby Boomers (BB) é o mesmo que comparar uma Ferrari com uma carroça.

Na primeira etapa da pesquisa podemos constatar que a grande maioria são homens com nível escolar de pós-graduação dentro das gerações alpha e Z.

Na segunda etapa da pesquisa tentamos identificar quais equipamentos os gamers utilizam, bem como seus cuidados com a segurança da informação nesses aparelhos. Pela pesquisa 70% dos respondentes utilizam a plataforma do Android, o que é extremamente natural, já que o IOS é exclusivo da Apple e a plataforma Android é utilizada por diversas empresas de comunicação. Um detalhe importante das repostas é que 87% dos aparelhos tem mais de 1 ano de uso. Quando questionados sobre o tempo de uso do smartphones, apesar de 50% dos respondentes usarem por menos de 1 hora, o que nos chamou a atenção é que 30% joga por mais de 3 horas diárias.

Após conhecer os equipamentos, passamos a analisar as repostas sobre a gestão da segurança da informação e os resultados foram surpreendentes. Das repostas apresentadas 70% não utiliza qualquer aplicativo de antivírus no seu smartphones, 77% não utiliza

aplicativo de análise estática e 10% dos respondentes armazenam senhas no smartphone sem qualquer criptografia. Um vírus pode ser um programa malicioso cuja função é causar danos ao usuário (Caiçara, C. e Paris, W.S. p 165), diante do cenário 70% dos respondentes correm risco de algum dano, da mesma forma 10% correm risco por não usar uma criptografia.<sup>2</sup> A criptografia é o processo de tornar a mensagem indecifrável utilizando o princípio de chaves (Caiçara, C. e Paris, W.S. p 165), as chaves podem ser de 2 formas conforme quadro abaixo.

**Quadro 2 – Tipos De Chaves**

CATEGORIA	CARACTERÍSTICAS	OBSERVAÇÕES
Simétrica	Utiliza única senha ou chave. Chave pouco protegida.	Quem tiver acesso à chave, pode decifrar as mensagens
Assimétrica	Utiliza um par de chaves (uma pública e uma privada). Maior proteção	Mesmo tendo acesso à chave pública, não é possível decifrar as mensagens. Utilizada para assinatura digital.

FONTE: Caiçara, C. Paris, W.S.

Por fim 77% dos respondentes não utilizam aplicativos de análise de estática que nada mais é um teste para inspecionar código de programa e assim procurar possíveis falhas de codificação, back doors e códigos mal-intencionados.

Não conseguimos localizar pesquisas científicas que tratam sobre o uso de antivírus ou de análise estática nos smartphones, apenas no site da empresa ESET conseguimos localizar uma pesquisa utilizada pela empresa para entender os hábitos dos usuários de smartphone e nesta pesquisa constataram que 60% dos entrevistados não utilizam nenhum tipo de segurança nos seus aparelhos.

Com base nessa média podemos fazer um teste de hipóteses para a média, partindo da informação do último parágrafo podemos afirmar que 40% usam algum tipo de segurança em seu smartphone, aplicando esse percentual a nossa população podemos chegar a conclusão que 12 pessoas seria a média global. Para dar maior ênfase ao estudo, nós optamos por um teste de significância de 1%, de posse desses dados conseguimos montar a tabela 2.

**Tabela 2 – Teste De Hipótese**

DESCRIÇÃO	USO DE ANTIVIRUS	USO DE ANÁLISE DE ESTÁTICA
Média Populacional	12	12
Média Amostral	8	7
Amostra	30	30
Desvio Padrão	10	11
Significância	1%	1%
Erro Padrão	1,85292561	2,065591118
Teste Z	<b>(-2,16)</b>	<b>(-2,42)</b>

Fonte: Elaborado pelos autores

De acordo com a tabela 2 chegamos a resultados para ambos Z de forma negativa, ou seja, menor do que 1% de significância aceitando assim H0 nossos gamer sabem proteger seus smartphones. Dentro da média a nossa amostra possui o conhecimento da proteção dos seus aparelhos seja com o uso de antivírus, seja com o uso de análise de estática. Para

<sup>2</sup> Criptografia vem do grego Kryptos (oculto) e gráphein (escrever)

entendimento da tabela, a média amostral representa a quantidade de respondentes que usam alguma medida de proteção, a amostra refere-se aos 30 respondentes, o desvio padrão encontrado foi calculado em cima das respostas conforme apresentado na tabela 3.

**Tabela 3 – Perguntas Para Teste De Hipóteses**

<b>VOCE EXECUTA UM APLICATIVO ANTIVÍRUS NO SEU CELULAR?</b>		<b>%</b>
Sim	8	27%
Não	21	70%
Não sei	1	3%
<b>VOCE EXECUTA UM APLICATIVO DE ANÁLISE ESTÁTICA NO SEU CELULAR?</b>		<b>%</b>
Sim	7	23%
Não	23	77%
Não sei	0	0%

Fonte: Resultados da pesquisa

Ainda na nossa pesquisa outras respostas também chamaram a atenção como a metade dos respondentes já teve seu celular roubado pelo menos uma vez, apenas 43% nunca emprestou seu celular e 77% dos respondentes armazenam informações como fotos, vídeos e áudios no seu celular.

É importante ressaltar na questão da tabela 3 que na pergunta sobre o uso de aplicativos de análise estática no seu celular, a questão se referia ao monitoramento de padrões de códigos maliciosos sendo possível inspecionar o controle e revisão das permissões solicitadas entre aplicativos.

## Conclusões

Proteção de dados ou informação têm ostentado uma grande proporção de relevância no cenário atual de uma sociedade hiperconectada. Com a aceleração constante do crescimento tecnológico tornou a sociedade atual em acumuladores obrigatórios de dados, e o anteparo dessas informações, tanto contra invasão de informação mal-intencionada, quanto contra vazamentos acidentais de dados, constitui uma prioridade para manter o modo de vida proporcionado pela internet, o artigo abordou um estudo e análise de como usuários de aplicativos de jogos para smartphone cuidam de sua privacidade e segurança, que são os utilizadores de um período maior de tempo nas plataformas game para smartphone.

Foram relatados alguns aspectos de modo de uso e proteção dos dados utilizados, desde tecnologias de proteção utilizadas quanto responsabilidade dos usuários. Em pesquisa foi percebido que quantitativo elevado dos entrevistados estão concentradas as gerações X, Y e Z, onde disponibilizam de uma a três horas dos seus tempos diários e mesmo com todos as outras relações cotidianas jogam através do smartphone. Na análise feito por questionário foi constatado que a maior parcela desses usuários que chega a 70% que não utiliza nenhum tipo de sistema de proteção de informações e dados em suas plataformas, e ainda dentro de tal percentual um pequena parte foi reconhecida por armazenar dados e senhas em seu equipamento sem qualquer recurso de proteção criptográfica, neste ambiente aberto de dados e informações fica claro que a maioria dos pesquisados estão expostos a risco de apropriação indevida de dados ou danos por não utilizar sistema de análise estática ou até mesmo simples processo de criptografia. Apesar de um percentual pequeno dentro da análise hipotética proposta no trabalho, nos deparamos 30% dos usuários de plataformas de smartphone para games que tem conhecimento e utilizam sistemas de proteção de dados e informação em seus equipamentos.



Sendo assim uma efetiva proteção só ocorrerá através do conhecimento dos perigos e obrigações específicas de cada plataforma utilizada. A simples adaptação a normas e padrões de segurança usuais seja ela Android, IOS ou Windows, não os torna um sistema livre a ataques. É percebido que decifrar as ameaças e contramedidas de segurança de informação possibilita o usuário do sistema a atuar de forma a se precaver de possíveis ameaças. Ainda é compreendido como a melhor forma de proteção, por enquanto, e manter os acessos restritos, e assegurar de que todos aqueles a adentrar são conhecidos e confiáveis, seja no mundo físico, seja no ciberespaço, pois independente da metodologia de segurança utilizada no sistema, o elemento mais fraco relação será sempre o usuário e a melhor ferramenta de segurança é o conhecimento.

## Limitações e pesquisa futura

Este estudo apresenta algumas limitações. Primeiro, o estudo restringiu-se ao universo de 30 pessoas que se ofereceram espontaneamente a responder este questionário após receber o convite nas redes sociais que fazem parte, sendo uma opção de análise primária, neste momento não há como realizar comparações diretas com outros estudos internacionais.

Uma sugestão de pesquisa futura pode vir a ser o alargamento deste escopo com a inclusão de mais participantes, além de expandir para pessoas que não residam apenas no Estado do Pará, mas em outros Estado do Brasil e futuramente combinar com análises internacionais, visando obter assim um panorama mais amplo buscando assim identificar as lacunas e eventuais comparações de procedimentos e hábitos de preservação dos dados no Brasil e no mundo.

Outra questão é um mapeamento sobre a relação entre as plataformas com os tipos de games, uma vez que esta evolução dos aparelhos e dos jogos aparentemente esta ligada, contudo ainda cabe analisar qual gamer tem maior preocupação e qual realmente faz a preservação de seus dados e as informações contidas em seu aparelho de uso pessoal, os da plataforma IOS, Android ou outras.

## Referências

AHUVIA, A. C. (2005). **Beyond the extended self: Loved objects and consumers' identity narratives.** *Journal of Consumer Research*, 32(1), 171–184.

ALEDAVOOD, T., TOROUS, J., T. HOYOS, AM et al. **Smartphone-based sleep tracking in depression, anxiety and psychotic disorders.** *Curr Psychiatry Rep* 21, 49 (2019). <https://doi.org/10.1007/s11920-019-1043-y>

ARRUDA FILHO, E.J.M.; GAMMARANO, I.J.L.P. **Forevery-gameover-thereisa-playagain-: Analysis of user preferences regarding 7<sup>th</sup> and 8<sup>th</sup> generation videogames consoles.** *Journal of High Technology Management Research*, Volume 29, Issue 1, 2018, Pages 46-56.

ARRUDA FILHO, E. J. M.; GAMMARANO, I.J.L.P.; BARRETO, I. A. **Technology-driven consumption: digital natives and immigrants in the context of multifunctional convergence.** *Journal of Strategic Marketing*, v. 1, p. 1-25, 2019.

BARTH. S.; MENNO D.T.DE JONG; M. JUNGER; P.H., HARTELAD; J. C. ROPPELT. **Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources.** *Telematics and*

Informatics. Volume 41, August 2019, Pages 55-69

BALAKRISHNAN, J., GRIFFITHS, M.D. **Perceived Addictiveness of Smartphone Games: A Content Analysis of Game Reviews by Players.** Int J Ment Health Addiction 17, 922–934 (2019). <https://doi.org/10.1007/s11469-018-9897-5>

BILALIA, H.E.; ALLAHYARI, M.S. **Transition towards sustainability in agriculture and food systems:** Role of information and communication technologies. Information Processing in Agriculture. Volume 5, Issue 4, December 2018, Pages 456-464.

BUCK, C., HORBEL, C. KESSLER, T., GERMELMANN, C.C. **Mobile consumer apps:** Big data brother is watching you Market. Rev. St. Gallen (2014), pp. 26-34

CAICARA, C.J.; PARIS, W.S.: **Informática, Internet e Aplicativos**, ed. IBPEX. 2008

EGELE, M., KRUEGEL, C., KIRDA, E., VIGNA. G. **PiOS:** detecting privacy leaks in iOS applications San Diego, California Proceedings of the 18th Annual Network and Distributed System Security Symposium 2011 (2011), pp. 77-183

ENCK, W., GILBERT, P. CHUN, B.-G., COX, L.P., JUNG, J., MCDANIEL, P., SHETH TAIN, A.N. **Droid:** an information-flow tracking system for realtime privacy monitoring on smartphones 9th USENIX Symposium on Operating System Design and Implementation (2014), pp. 1-15

GAMMARANO, I.J.L.P. **Segunda Chance Só No Videogame:** Competição mercadológica e valores envolvidos no processo de consumo de videogames. CONTRIBUCIONES A LA ECONOMÍA, v. 1, p. 1-25, 2018.

HAO SONG, H. **Testing and Evaluation System for Cloud Computing Information Security Products.** Procedia Computer Science. Volume 166, 2020, Pages 84-87. <https://doi.org/10.1016/j.procs.2020.02.023>

HARRIS, J., & BLAIR, E. A. (2006). **Consumer preference for product bundles:** The role of reduced search costs. Journal of the Academy of Marketing Science, 34(4),506–513.

JOB, Aline; KURTZ, Gabriela; FORTIM, Ivelisse; CAETANO, Mayara; PIRRO, Roxane. **Videogame, Diversidade e Gênero:** Pesquisa Científica e Acadêmica, Volume I. Indaiatuba, SP: Oficina Lúdica, 2019.

KUNCHAMBOO, V., LEE, C. K., & BRACE-GOVAN, J. (2017). **Nature as extended-self:** Sacred nature relationship and implications for responsible consumption behavior. Journal of Business Research, 74, 126–132.

MOHR, H., WALTER, Z. **Formation of Consumers' Perceived Information Security:** Examining the Transfer of Trust in Online Retailers. Inf Syst Front 21, 1231–1250 (2019). <https://doi.org/10.1007/s10796-019-09961-7>

MOHAMMADIAN, M., & KARIMPOUR, Y. (2014). **Identifying the factors influencing the feeling of love toward a brand:** the Adidas case. Nationalpark–Forschung In Der Schweiz (Switzerland Research Park Journal), 103(1), 94–122.

STOECKLI, E., DREMEL, C. & UEBERNICKEL, F. **Exploring characteristics and transformational capabilities of InsurTech innovations to understand insurance value creation in a digital world.** Electron Markets 28, 287–305 (2018). <https://doi.org/10.1007/s12525-018-0304-7>