Revista GCTI
Gestão do Conhecimento e Tecnologia da Informação
GCTI 4(1):21-48, 2018
ISSN: 2526-8384

Utilização e compartilhamento de dados capturados por aplicativos de smartphones: uma revisão sistemática de literatura

Using and sharing of data captured by smartphones apps: a systematic literature review

Adriano Vieira da Silva[a], Paulo Victor Guimarães Rosa[b], Edilson Ferneda[c], Mário de Oliveira Braga Filho[d]

[a] adrianov1941@gmail.com

[b] paulovgr@gmail.com

[c] eferneda@gmail.com

[e] bragaucb@gmail.com

Resumo: As pesquisas sobre segurança de dados têm avançado nos últimos anos influenciadas pela expansão de aparelhos móveis, cada vez mais presentes na vida das pessoas. No mesmo sentido, também cresce a importância dada por nossa sociedade à privacidade e segurança dos dados gerados ou armazenados nesses dispositivos. Assim, pesquisadores se veem estimulados a compreender de que forma esses dados podem ser acessados por aplicativos e pelo próprio sistema operacional neles instalados. Esse é um tema de pesquisa relativamente novo, mas já com significativa quantidade de trabalhos publicados na última década. Dessa forma, é pertinente uma sistematização de conhecimento para um melhor direcionamento de pesquisas sobre o assunto. O objetivo deste trabalho é realizar uma revisão sistemática de literatura sobre a utilização de informações produzidas em *smartphones*.

Palavras chave: Segurança de dados; Privacidade; Computação móvel.

Abstract: The research on data security has recently advanced influenced by the expansion of mobile devices, increasingly present in people's lives. In the same sense, the importance given by our society for the privacy and security of the data generated or stored in these devices also grows. Thus, researchers are encouraged to understand how these data can be accessed by apps and the operating system installed on them. This is a relatively new research topic, but already with a large amount of works published in the last decade. Thus, a systematization of knowledge is pertinent for better driving research efforts on this subject. The aiming of this work is to carry out a systematic literature review on the use of information produced on smartphones.

Keywords: Data security; Privacity; Mobile computing.

1. Introdução

Diariamente, uma quantidade significativa de dados trafega pelo mundo por meio da rede mundial de computadores, a Internet. Esses dados são agrupados, armazenados e transformados em informação, disponibilizada para serem acessadas e manipuladas por algum interessado, seja um usuário numa conversa em rede social ou um aplicativo que irá utilizar os dados de alguma forma.

A excessiva exposição de dados nos *smartphones* e o desconhecimento por parte significativa dos usuários de que os dados contidos em seu dispositivo podem ser compartilhados sem seu conhecimento, podendo afetá-los em diversos aspectos. Embora isso pareça ser irrelevante, o compartilhamento de dados pessoais é capaz de levar a sérios prejuízos. Muitas empresas aproveitam da ignorância dos usuários quanto a isso para capturar e utilizar sem autorização seus dados. Por exemplo, muitos aplicativos que se servem de algoritmos de recomendação usam os dados pessoais para se adequarem ao estilo de vida e gostos do usuário,

como *streaming* de músicas e vídeos que indicam novos conteúdos baseados em acessos anteriores.

Este trabalho tem como objetivo abordar a coleta e a utilização de dados produzidos em dispositivos móveis por sistemas neles instalados na forma de uma revisão sistemática.

Sabe-se que dispositivos móveis contêm inúmeras funcionalidades que produzem dados que podem ser acessados remotamente por meio dos sistemas de software neles instalados. Nesse sentido, este trabalho busca responder as seguintes perguntas: *Quais dados podem ser acessados por terceiros a partir do sistema operacional e dos aplicativos instalados em dispositivos móveis? Quais as possíveis finalidade dessa captura de dados?*

Já é possível dizer que o *smartphone* tornou-se um grande companheiro das pessoas. O modo como o aparelho se integrou à vida de seus usuários resulta em uma extensa lista de vantagens, mas também em alguns pontos negativos. Pode-se dizer que esse aparelho possui dados a partir dos quais pode-se inferir aspectos da vida de seu dono que, talvez, poucas pessoas teriam conhecimento. Nele, compartilha-se senhas, fotos, informações bancárias, localização e outros dados que poderiam ser de grande interesse para empresas, corporações e outras entidades, mas, se mal utilizados, podem ser gerar sérios problemas para o usuário.

Em 2018, a grande mídia noticiou o caso da *Cambridge Analytica*, uma empresa britânica que, a partir de permissões concedidas pelos usuários, por meio do teste de personalidade *This Is Your Digital Life*, puderam ter acesso a dados não só do usuário, mas também de toda sua rede de contatos. O resultado disso foi aproximadamente 87 milhões de perfis analisados e, com isso, a criação de anúncios que visavam manipular a consulta popular sobre o *Brexit* no Reino Unido e os eleitores nas eleições presidenciais dos EUA de 2016 (Hinds, 2020).

E não é somente por meio das redes sociais e demais aplicativos que a privacidade dos usuários pode ser ameaçada, visto que as próprias funcionalidades do aparelho podem colaborar com isso (Jayakumar, 2019). Por exemplo, uma agência de viagem conseguiu identificar que a maioria dos seus acessos eram realizados à noite a partir dos dados gerados pelo acelerômetro e giroscópio instalados nos *smartphones* dos usuários de seus aplicativos, indicando quando esses usuários se deitavam.

Com a evolução da tecnologia dos dispositivos móveis, diversas ferramentas foram sendo incorporados a eles, como a câmera fotográfica. Essa funcionalidade é uma das mais utilizadas, e, com isso, muitos usuários acabam gerando e armazenando suas fotos pessoais nele, incluindo fotos íntimas. Em 2014, um *hacker* conseguiu invadir o iCloud, biblioteca de imagens da Apple, de diversas celebridades, vazando fotos de várias delas.

Assim, fica evidente a questão de como os dados presentes em aparelhos móveis podem mudar a vida de uma pessoa, como, por exemplo, a superexposição de suas fotos, ou até influenciar um conjunto de pessoas, como no caso da *Cambridge Analytica*. Devido às características dos *smartphones*, não é desprezível a possibilidade de difusão indesejada de dados pessoais.

Este trabalho ter por objetivo desenvolver uma revisão sistemática de literatura sobre o acesso e manipulação de dados por terceiros a partir de *smartphones*. Para alcançar o objetivo geral desta pesquisa, foram definidos os seguintes objetivos específicos: *(i)* Identificar os principais tipos de dados capturados por aplicativos; *(ii)* Compreender o que é segurança de dados no contexto de *smartphones*; *(iii)* Identificar a quais dados os aplicativos de *smartphones* têm acesso; *(iv)* Identificar como os dados acessíveis por aplicativos via *smartphones* vêm sendo utilizados por terceiros; *(v)* Analisar os problemas de segurança de dados em *smartphones* na perspectiva da LGPD.

2. Abordagem metodológica

Neste artigo, o processo metodológico está subdividido em duas aplicações principais. A primeira é a revisão da literatura acerca dos diversos temas que envolvem o papel da liderança na era digital, transformação digital e cultura digital, bem como uma visão do processo de adaptação das organizações e pessoas neste novo contexto de constantes e rápidas mudanças.

Para alcançar os objetivos deste trabalho, adotou-se a revisão sistemática de literatura (RS), que consiste em uma investigação científica para identificação, seleção, avaliação e sumarização de estudos disponíveis considerados relevantes para o assunto de interesse (Kitchenham, Dybå & Jørgensen, 2004; Biolchini et al.,

2005). Uma RS é conduzida por meio de um processo que envolve três fases (Biolchini et al., 2005; Brereton et al., 2007; Kitchenham, 2004; Mafra & Travassos, 2006): *(i)* planejamento, *(ii)* condução e *(iii)* publicação dos resultados. A fase de planejamento tem como objetivo identificar a finalidade da RS. É nesta fase que surge o protocolo de pesquisa, elemento essencial para a execução da RS. O protocolo visa minimizar vieses que possam vir a ser cometidos pelo pesquisador (Kitchenham & Charters, 2007; Brereton et al., 2007). Já na fase de condução, os estudos relacionados com o tema de pesquisa são coletados e analisados pelos pesquisadores, considerando-se critérios de inclusão e exclusão previamente definidos. A última fase do processo de RS está relacionada com a escrita dos resultados, que respondem às questões de pesquisa elaboradas.

2.1 Questões de pesquisa

Primeiramente, foram definidas as questões de pesquisa e a estratégia para respondê-las levou ao objetivo proposto neste estudo. Além disso, essas questões auxiliaram na produção da *string* de busca, tratada mais à frente. As seguintes questões de pesquisa foram propostas:

QP_1: Quais os principais tipos de dados coletados por aplicativos?

QP_2: O que é segurança de dados dentro do contexto de *smartphones*?

QP_3: Como os dados acessíveis por aplicativos via *smartphones* vêm sendo utilizados por terceiros?

2.2 Estratégia de busca

Inicialmente, optou-se por utilizar duas fontes de busca: as bases de dados *Scopus* e *Web of Science*, visto que ambas são abrangentes e incluem outros dados adicionais úteis aos pesquisadores deste trabalho, como a criação de gráficos e análises. Entretanto, devido ao grande número de trabalhos encontrados, optou-se por utilizar apenas a *Scopus*, visto que foi a que trouxe uma quantidade consideravelmente maior de resultados. Além disso, como o fenômeno da privacidade digital é considerado recente, foi de interesse dos pesquisadores selecionar apenas estudos recentes, com 2017 como limite mínimo de data de publicação.

Quanto aos métodos, por se tratar de uma busca automática, foi necessário se chegar a uma *string* de busca, elaborada com base nas questões de pesquisa. Para isso, foi utilizada a metodologia PICO (Akobeng, 2005; Flemming, 1999).

PICO pode ser utilizada para construir questões de pesquisa para diversos fins, possibilitando a definição correta das informações necessárias para a resolução do problema de pesquisa, além de maximizar a recuperação de evidências nas bases de dados. Por conseguinte, o PICO é utilizado numa RSL para auxiliar na formação e delimitação dos termos da *string* de busca. A metodologia foca no objetivo da pesquisa e evita buscas desnecessárias. PICO representa um acrônimo para: *(i)* **P**roduto, em que se estabelece o foco da pesquisa; *(ii)* **I**ntervenção, no qual se delimita o foco da pesquisa dentro de um escopo mais amplo; *(iii)* **C**omparação, aonde se identifica alternativas e se compara com a delimitação realizada na intervenção; e *(iv)* "**O***utcomes*" (desfecho), quando se apresenta o resultado esperado, ou seja, o que se pretende realizar, medir, melhorar ou afetar em relação ao problema).

A partir das questões de pesquisa e da metodologia PICO, desenvolveu-se a *string* de busca (Quadro 1). A Tabela 1 apresenta a quantidade de resultados obtidos. A *string* S_7, junção de todos os elementos, é a *string* final, utilizada para a pesquisa na base de dados. Como filtro foram utilizadas: *(i)* a data de publicação dos estudos selecionados, limitada ao intervalo 2017-2020; *(ii)* todas as categorias diferentes do tema de interesse foram excluídas, como, por exemplo, medicina e bioquímica; e *(iii)* restringiu-se a textos escritos em inglês ou português.

2.3 Critérios de inclusão e exclusão

Por fim, foram aplicados critérios de inclusão e exclusão nos estudos encontrados. Cada estudo precisava se enquadrar em pelo menos um desses critérios para ser aceito ou descartado.

- Critérios de inclusão: *(i)* Versar sobre a segurança de dados em *smartphones*; *(ii)* Tratar sobre compartilhamento, uso e vazamento de dados coletados a partir de *smartphones*; *(iii)* Apresentar uma pesquisa prática sobre a captura de dados; *(iv)* Analisar entidades envolvidas na captura de dados e suas consequências; *(v)* Discutir sobre a comunidade dos desenvolvedores e suas ligações com questões de privacidade; *(vi)* Abordar aspectos de motivação para a captura de dados a partir de *smartphones*; *(vii)* Examinar barreiras e dificuldades em manter a privacidade

Quadro 1. Definição dos elementos PICO.

	Descrição	Palavras-Chave	Termos de Busca
P	Publicações relacionadas ao acesso por terceiros de informações presentes em *smartphones*.	*Smartphone*, dados, Segurança, Usuário, Aplicativo, Técnicas de proteção de dados;	*Smartphone*; Data; Security; User; App.
I	Identificação dos mecanismos de captura e tratamento não autorizado de dados armazenados em *smartphones*.	Manipulação de dados, Compartilhamento de dados, Análise de dados.	Data manipulation; Data sharing; Data analysis; Data access.
C	***Não se aplica***	–	–
O	Identificação das vulnerabilidades de dados em *smartphone*s e os mecanismos presentes em aplicativos e nos sistemas operacionais que viabilizam o compartilhamento involuntário desses dados.	Visão geral dos estudos propostos na literatura que reportam quais e como os dados são manipulados com o uso do *smartphone*, e seus meios de mitigação.	Data destination; Data use; Data security; Main types of data used in apps.

Fonte: Autores

Tabela 1. Definição dos termos de busca.

ID	Termos de Busca/*Strings*	Quantidade	
		S/filtro	C/filtro
S_1	"portable devices" OR mobile* OR Cellular* OR "cell phone" OR android* OR ios OR iphone* OR *smartphone** OR social media* OR twitter OR instagram OR facebook OR IoE OR IoT OR "Internet of Things" OR "Internet of everything"	2.351.004	326.070
S_2	data and ("data manipulat*" OR "data shar*" OR "data analy*" OR "user's security" OR "securing data" OR "data leakage" OR "Collection of data" OR organisation* OR strategic OR leakage OR "theft of data" OR "privacy leakage" OR "data collect*" OR GDPR OR CCPA OR sharing OR "security policies" OR "data accountability" OR "data subjects" OR "private information" OR "anonymity and protection of private information" OR "consumer behavior" OR "personal privacy protection" OR owner OR "General Data Protection Regulation" OR "policy guidelines" OR "consent to personal data use" OR "personal data" OR "data leaks" OR "publication of data" OR anonym* OR "collected information" OR "sensitive data" OR "data privacy violation*" OR "social psychology" OR ethi" OR regulation OR restrictions OR "strategic value of personal data")	2.560.083	325.637
S_3	privacy OR security OR leaks OR theft OR collect* OR exposed OR "target advertisement" OR advertisement OR marketing OR consent OR "data breach" OR "tick box" OR protection OR disclosure OR policies OR "data publication"	283.711	48.899
S_4	S_1 AND S_2	174.423	42.208
S_5	S_1 AND S_3	22.663	6.854
S_6	S_2 AND S_3	48.657	12.448
S_7	S_1 AND S_2 AND S_3	6.690	**2.722**

Fonte: Autores

de dados em aplicativos móveis.

- Critérios de exclusão: *(i)* Não apresentar resumo ou apresentar texto incompleto; *(ii)* Apresentar apenas a metodologia de um projeto, sem expor os resultados e/ou análises relevantes; *(iii)* Não disponível de forma gratuita; *(iv)* Estudo repetido.

3. Resultados da revisão da literatura

Foram aplicados critérios de inclusão e exclusão nos estudos encontrados. O Quadro 2 apresenta os trabalhos selecionados enquadrados em pelo menos um dos critérios de inclusão. A partir dessas referências, outras por elas citadas foram também consideradas.

Quadro 2. Descrição e uso dos estudos na revisão de literatura.

Referência	Descrição	Tipos de dados	Segurança de dados	Uso de dados por terceiros	LGPD/GPDR
Hinds, Williams e Joinson (2020)	Procura compreender o quão preocupadas as pessoas se sentem sobre sua privacidade *online*.		X	X	
Jayakumar et al. (2019)	É feita uma revisão da importância dos *smartphones* na vida do ser humano atualmente e fala sobre os métodos usados para coletar e explorar os dados dos usuários.	X		X	
Presthus e Vatne (2019)	Investiga como os usuários do Facebook percebem a privacidade das informações em relação aos benefícios de ser um membro.	X	X	X	
Yu et al. (2020)	Apresenta os problemas de proteção de privacidade que a plataforma Android enfrenta.		X		
Breitinger, Tully-Doyle e Hassenfeldt (2019)	Explora as escolhas do usuário, consciência e educação no que diz respeito à cibersegurança.		X		
Schomakers, Lidynia e Ziefle (2020)	Analisa as preferências dos usuários da Internet quanto à privacidade de dados compartilhados.		X		
Gubernatorov et al. (2020)	Analisa o uso de dispositivos móveis, apresenta estatísticas de crescimento do vazamento de dados em todas as esferas da sociedade, descreve os problemas de segurança de dispositivos móveis.		X		
Polykalas e Prezerakos (2019)	Examina a extensão do acesso a dados pessoais, exigidos pelos aplicativos móveis mais populares disponíveis na *Google Play Store*.	X			
Shozi e Mtsweni (2017)	Destaca o papel que o *Big Data* desempenha nas redes sociais mídia mostrando as várias invasões de privacidade que ocorreram nas redes sociais devido à grande quantidade de informações disponíveis.	X	X	X	
Chen et al. (2019)	Visa ajudar os usuários de aplicativos a entender a privacidade e problemas de vazamento e lembrá-los de prestar mais atenção à sua privacidade ao usar aplicativos.		X		
Brückner et al. (2018)	Esclarece quais tipos de informações pessoais são exibidas em formato digital nos jogos para celular.	X			
Adams (2020)	Analisa das políticas de privacidade de aplicativos famosos	X		X	
Osho et al. (2019)	Conduz uma investigação de doze aplicativos populares para avaliar alguns tópicos de segurança.		X		
Baalous e Poet (2018)	Analisa as políticas de privacidade de aplicativos Android.	X			
Atkinson et al. (2018)	Analisa como informações de *smartphones* podem ser obtidas de forma externa. Através de tecnologia de transmissão sem fio.	X			
Baalous, Poet e Storer (2018)	Analisa questões de privacidade nas políticas de aplicativos.	X		X	
Binns et al. (2018)	Fornece uma visão de alto nível da extensão do rastreamento de terceiros no ecossistema móvel.			X	

Referência	Descrição	Tipos de dados	Segurança de dados	Uso de dados por terceiros	LGPD/GPDR
Brandtzaeg, Pultier e Moen (2019)	Analisa de fluxos de dados pessoais em aplicativos e análise de conteúdo das políticas de privacidade.			X	
Story, Zimmeck e Sadeh (2018)	Analisa políticas de privacidade de aplicativos móveis.		X		
Elahi, Wang e Chen (2020)	Investiga os problemas de privacidade, segurança e confiança dos aplicativos *bloatware*.	X	X		
Dai et al. (2017)	Apresenta comportamentos de coleta de dados e ilustra as motivações e razões atrás deles.	X		X	
He, Hu e Han (2018)	Estuda os comportamentos de vazamento de privacidade de bibliotecas de terceiros dentro de aplicativos Android.	X			
Greene e Shilton (2018)	Revela as interações cotidianas entre desenvolvedores e a plataforma, e descreve as maneiras como as decisões dos desenvolvedores são moldadas pela plataforma em que trabalham.	X	X		
Kandil et al. (2018)	Analisar a políticas de privacidade de aplicativos móveis.	X		X	
Jensen et al. (2019)	Prova que os aplicativos executados em sistemas operacionais móveis atuais são vulneráveis à coleta de dados por desenvolvedores de aplicativos maliciosos.	X			
Liu et al. (2019)	Estuda quais informações são coletadas pelas bibliotecas analíticas integradas em aplicativos Android populares. Também demonstra quais informações privadas podem ser vazadas pelos aplicativos. Além disso, analisa as políticas de privacidade dos aplicativos.	X		X	
Fong (2017)	Detalha os problemas de privacidade de dados associados aos aplicativos. Em seguida, examina a função das lojas de aplicativos nessa questão.			X	X
Tramontana e Verga (2019)	Mostra os mecanismos que um aplicativo pode usar para obter dados confidenciais, violando a privacidade do usuário.	X			
Kusyanti e Catherina (2018)	Tem como objetivo determinar os fatores que afetam os usuários em ler permissões de aplicativos que foram fornecidas por um aplicativo antes de instalar o aplicativo.		X		
Singh, Saini e Bathla (2019).	Fornece uma estrutura que pode ajudar os consumidores e as organizações a evitar preocupações relacionadas a vazamento de dados em *smartphones* e a funcionar sem problemas.			X	X
Pal e Crowcroft (2019)	Fornece argumentos para a necessidade virtualmente inevitável de coleta, compartilhamento e comercialização de dados obtidos a partir do *smartphone*.	X	X	X	
Lai e Flensburg (2020)	Explora as possíveis implicações de privacidade de por meio da investigação de permissões móveis.	X		X	
Kul, Upadhyaya e Chandola (2018)	Foca em mostrar as vulnerabilidades recentes relatadas que pode permitir que invasores roubem informações confidenciais do banco de dados dos aplicativos.	X			

Fonte: Dados da pesquisa

Os *smartphones* atuais são equipados com processadores comparáveis aos de computadores. Neles, há vários sensores para proporcionar ao usuário uma melhor experiência de uso, dos quais se servem também os aplicativos. Entretanto, não só para as funções estritamente necessárias para suas funcionalidades os aplicativos se servem desses sensores. A Google, por exemplo, já chegou a remover de sua loja aplicativos que abusavam do uso desses recursos (Baraniuk, 2018).

"Os dados são o novo petróleo e já temos a tecnologia para refiná-los", afirmou Maurício Ruiz, presidente da Intel no Brasil, ao ser perguntado sobre as inovações da empresa (Ruiz, 2018). Os dados têm importância cada vez maior para diversos segmentos. Nesta seção será apresentado como isso pode se dar, e como informações inseridas pelo usuário em seus *smartphones*, ou inferidas a partir de sensores neles disponíveis, podem abastecer bancos de dados de várias empresas.

3.1 Motivos para captura de dados dos *smartphones*

Muitos aplicativos têm a capacidade de se adaptar ao perfil de seu usuário. Para prestar serviços de acordo com as preferências do usuário, esses aplicativos precisam capturar dados. Quando, a partir desses dados, for possível identificar indivíduos, esses dados podem ser considerados dados pessoais (Parlamento Europeu, 2016).

A quantidade de dados pessoais que estão sendo coletados de sites e aplicativos vem aumentando (Corones & Davis, 2017). Várias empresas, inclusive, têm nos dados pessoais sua principal fonte de renda (Lang, Wiesche, & Krcmar, 2018), tendo como clientes, por exemplo, agências de publicidade (Lipman, 2016) que coletam tais informações para propaganda e outras finalidades. (Federal Trade Commission, 2014).

Outra grande razão pela qual aplicativos capturam dados dos usuários tem a ver com a cada vez maior facilidade de se utilizar ferramentas de inteligência artificial, notadamente o aprendizado de máquina, para a extração de informações úteis para as organizações (Horvitz & Mulligan, 2015). Essas informações incluem a forma com que os usuários utilizam o aplicativo, quais as funções mais requisitadas, hábitos de navegação na Internet. Quase todo aplicativo popular contém funções de captura e análise de dados (Liu et al., 2019).

3.2 Smartphones Vs. computadores pessoais

A ameaça de privacidade se mostrou maior no âmbito de aplicativos móveis se comparado com a navegação em computadores. Dentre os motivos, cabe citar que os *cookies*, principal meio de autenticação na Internet, são fáceis de serem excluídos pelos usuários para fins de preservação de sua privacidade. Entretanto, o ID, forma de autenticação nos *smartphones*, é difícil de ser alterado. Além disso, mais de uma pessoa pode usar o mesmo computador, por outro lado, os celulares geralmente são de uso individual. Logo, dados capturados em um dispositivo geralmente vêm de um mesmo usuário.

Aplicativos móveis, incluindo suas bibliotecas de rotinas, ou APIs (Application Programming Interface), também podem acessar muitos outros recursos no dispositivo. Por fim, no computador, os usuários têm o costume de abrir muitas páginas ao mesmo tempo, logo, os sistemas de análise de navegação têm dificuldade de saber quais páginas estão sendo visualizadas naquele momento. Já o aplicativo móvel em execução geralmente é de fato aquele que está sendo visualizado pelo usuário (Dykes, 2013).

3.3 Políticas de privacidade dos aplicativos

Em se tratando do uso de dados por aplicativos, é essencial analisar suas políticas de privacidade. Dessa forma, é possível compreender quais tipos de dados são importantes para as empresas, quais são compartilhados com terceiros e se eles realmente são utilizados para a função que o aplicativo se propôs cumprir. Para a *Federal Trade Commission* (2014), as políticas de privacidade expõem as formas como as empresas manipulam os dados de seus usuários. No entanto, Polykalas e Prezerakos (2019) avaliaram milhares de aplicativos móveis da *Google Play Store* com foco nas políticas de privacidade e constataram que 71% dos aplicativos avaliados manipulam e compartilham dados pessoais de seus usuários, mesmo sem ter políticas de privacidade. Tal análise corrobora Brandtzaeg, Pultier e Moen (2018), que concluíram que muitos aplicativos também solicitam e compartilham informações detalhadas dos usuários sem uma justificativa para isso.

Story, Zimmeck e Sadeh (2018), a partir de uma análise de mais de um milhão de aplicativos da *Google Play Store* dos EUA, descobriram que apenas 45% deles possuem *links* para as políticas de privacidade adotadas. A análise também mostrou que é mais comum os aplicativos publicados recentemente terem alguma política de privacidade em comparação com aplicativos mais antigos, embora em número ainda baixo para ambas as categorias. Os autores consideram que a ausência dessas políticas não significa falta de conhecimento sobre a legislação, mas descompromisso.

Baalous e Poet (2018) analisaram as políticas de privacidade dos 100 mais populares aplicativos Android disponíveis no *Google Play Store*. O resultado é detalhado na Tabela 2.

Tabela 2. Frequência de termos presentes nos textos referentes à política de privacidade dos principais aplicativos disponíveis na *Google Play Store*.

Terminologia da política de privacidade	Frequência
Informações pessoais	74%
Números de telefone	34%
Localização	30%
Informação de localização	29%
Fotos	27%
Informação de contato	26%
Dado pessoal	23%
Números de telefone	22%
Dado de localização	16%
Endereços	15%

Fonte: Baalous, Poet e Storer (2018)

Baalous, Poet e Storer (2018) analisaram as políticas de privacidade de 15 aplicativos Android. Os resultados (Tabela 3) mostraram que, em geral, elas tratam de áreas importantes sobre a captura de dados. Entretanto, em alguns aspectos, verificou-se escassez de informações detalhadas como, por exemplo, sobre o período de retenção de dados.

Segundo esses autores, muitas políticas de privacidade esclarecem os tipos de informações que podem ser coletadas pelos aplicativos. As empresas pedem essas informações alegando necessidade para fornecer um melhor do serviço, prover maior segurança (prevenção de fraudes, atividades ilegais ou má conduta), para cumprir a lei (ordens judiciais e mandados de busca e apreensão) ou para atividades de marketing. O *Google Analytics* é utilizado por alguns aplicativos, sendo que a maioria deles deixa claro que as informações coletadas são enviadas e armazenadas em um servidor da Google nos EUA. Essas políticas também informam que o usuário pode negar aprovação a essa coleta de informações pelo *Google Analytics*.

Em relação às formas de controle, foi identificado que vários direitos foram dados aos usuários, como a opção de não receber anúncios e propagandas, capacidade de desativar ou recusar *cookies*, editar e excluir seus dados pessoais, e conhecimento sobre mudanças na política de privacidade. Entretanto, apenas uma pequena parcela afirmou que notificam o usuário se as empresas estiverem prestes a serem vendidas ou incorporadas por outras entidades, fato que pode ocasionar um risco à privacidade dos dados. Em muitas políticas de privacidade, não houve clareza sobre terceiros e parceiros de negócios com quem os dados seriam compartilhados. Os resultados também revelaram que, embora a maioria dos aplicativos analisados forneçam um *link* para a política de privacidade, alguns forneceram *links* inativos. (Baalous, Poet, & Storer, 2018)

Segundo Brandtzaeg, Pultier e Moen (2018), alguns aplicativos declararam que terceiros não tinham permissão para usar dados pessoais fora do objetivo do aplicativo. No entanto, foram identificadas violações desse tipo. Constataram também que muitos dos termos eram complicados ou ambíguos. Para os autores, algumas políticas de privacidade, apesar de transparentes, são problemáticas. O aplicativo de relacionamento Tinder, por exemplo, deixa claro que seus usuários podem perder o controle de seus dados para sempre.

Após análise de 20 políticas de privacidade de aplicativos famosos, Kandil et al. (2018) constataram que os provedores examinados declaram as informações que coletam e seu uso, mas falta clareza sobre, por exemplo, o local onde os dados são armazenados, etapas para remoção da conta e o que acontece com os dados depois disso. Os resultados mostraram que aplicativos coletam uma grande quantidade de dados, usados principalmente para personalizar anúncios, melhorar o software, desempenhar suas funções e identificar novos usuários em potencial para o aplicativo.

A Figura 1 apresenta alguns resultados importantes da pesquisa realizada.

Tabela 3. Resultados obtidos a partir da análise das políticas de privacidade.

Categorias de conteúdo da política de privacidade	Subcategorias de conteúdo da política de privacidade	Número de aplicativos
Tipo de informação coletada	Informação pessoal	15
	Dados de uso ou registro	15
	Metadados de arquivos	3
Mecanismos de coleta	Cookies	15
	Armazenamento local HTML5	1
	Web beacons	3
	Google Analytics	3
Objetivo da coleta	Finalidades funcionais	15
	Melhorar e desenvolver objetivos	14
	Para fins de contato e comunicação	9
	Propósitos de marketing	11
	Finalidades estatísticas ou analíticas	9
	Fins de segurança	3
Compartilhamento de informações	Para atender aos pedidos dos usuários, entregar e aprimorar os serviços	15
	Para cumprir a aplicação da lei ou responder a processos legais	13
	Para usá-lo para marketing e anúncios	5
	Para proteger os direitos, propriedade ou segurança do provedor de nuvem, terceiros ou membros do público	8
	Para parar atividades ilegais	6
	Em conexão com uma venda, fusão, aquisição ou falência	8
Controles e direitos do usuário	Pode optar por não receber materiais de marketing	10
	Informado sobre seu direito de desativar cookies ou remover objetos de armazenamento local HTML5	13
	Pode editar e / ou excluir informações pessoais	11
	Pode solicitar acesso a informações pessoais mantidas pelo provedor de armazenamento em nuvem	7

Fonte: Baalous, Poet e Storer (2018)

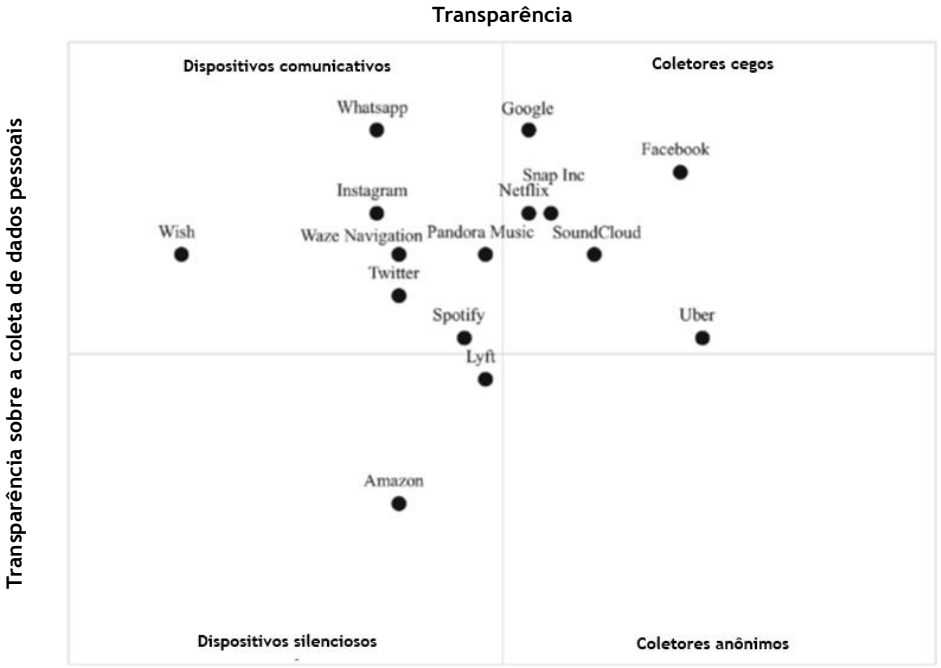
O primeiro quadrante (dispositivos comunicativos) se refere aos aplicativos que armazenam poucos dados e comunicam isso explicitamente. O segundo quadrante (coletores cegos) contém aplicativos que coletam grande quantidade de dados e não notificam isso em suas políticas. O terceiro quadrante (dispositivos silenciosos) contém os aplicativos que não armazenam grandes quantidades de dados, mas não têm políticas claras privacidade. Nessa pesquisa, os autores não encontraram nenhum aplicativo condizente com o quarto quadrante (coletores disfarçados), mas comentam que empresas que capturam secretamente dados de seus usuários provavelmente possuem baixa transparência. (Kandil et al., 2018)

3.4 Permissões

Para desfrutar dos serviços oferecidos por aplicativos, é necessário conceder algumas permissões de captura de dados, alguns deles pessoais. Após a permissão do usuário, o aplicativo poderá manipular esses dados ou mesmo enviá-los pela rede.

No sistema operacional, as permissões servem para restringir o acesso de aplicativos a dados privados do usuário e a recursos do dispositivo. Certos tipos de permissões trazem riscos à privacidade, pois alguns aplicativos capturam mais do que seria necessário para executar suas funções. Captura abusiva de dados são mais difíceis de serem detectados do que um vírus (Dai et al., 2017).

Figura 1. Comparação de políticas de privacidade no ecossistema de aplicativos móveis.



Fonte: Kandil et al. (2018)

Uma das principais razões para a captura abusiva de dados deve-se a falhas dos sistemas operacionais atuais, como na autorização de permissão de baixa complexidade, ou seja, que possibilita apenas dois tipos de permissões: tudo ou nada. Significa que quando um aplicativo obtém permissão para acessar algum tipo de dado de um usuário, por exemplo, uma foto, ele poderá acessar todos dados do mesmo tipo. Além disso, quando é aceita a primeira solicitação de um aplicativo para acessar o álbum, o aplicativo poderá acessá-lo indefinidamente até que o usuário negue manualmente essa permissão. (Dai et al., 2017)

Dentre os níveis de permissão definidos pelo Android, há o normal e o perigoso. Permissões normais regulam o acesso aos dados considerados inofensivos para a privacidade, diferentemente das permissões perigosas, que manipulam dados confidenciais do usuário e recursos críticos do dispositivo. As permissões normais são concedidas automaticamente a um aplicativo ao instalá-lo, mas, para as perigosas, são solicitadas permissões explícitas ao usuário (Tramontana & Verga, 2019). É a combinação desses dois tipos de permissões que leva a um risco de privacidade dos dados. Por exemplo, uma permissão perigosa que permite que o aplicativo acesse materiais confidenciais combinada com uma permissão normal para acessar a Internet permite que um aplicativo envie esses dados pela rede. Nos Quadros 3 e 4 são apresentados exemplos de permissões normais e perigosas, respectivamente.

Os níveis de permissão, em geral, não analisam fluxos de dados dos aplicativos. Por exemplo, um aplicativo, tendo pedido permissão para capturar dados sonoros, como o som do microfone, pode fazê-lo continuamente durante sua execução, mesmo em segundo plano, sem que o usuário saiba disso (Sarma et al., 2012). Uma possibilidade de evitar problemas desse tipo seriam permissões para acesso apenas a dados estritamente necessários para o bom desempenho do aplicativo, e nada além disso (Sanders et al., 2015).

Lai e Flensburg (2020) mostraram que certas permissões são fundamentais para o funcionamento de alguns aplicativos (Tabela 4), enquanto outras são solicitadas unicamente para o comércio de dados. As permissões primordiais para o bom desempenho de um aplicativo podem também fornecer dados que seriam de interesse de anunciantes. As permissões mais comuns são para que os aplicativos acessem os dados em armazenamento externo, como o cartão de memória. Entretanto, há aqueles que permitem que outros aplicativos vinculem sua utilização ao login de outros aplicativos, como *Gmail*, *Instagram* ou *Facebook*.

A categoria “pesquisa” é a que exige o maior número de permissões, seguido por aplicativos

Quadro 3. Exemplos de permissões normais.

Permissão	Descrições
Acesso ao status da rede	Para acessar informações da rede
Acesso ao Wi-Fi da rede	Para acessar informações do Wi-Fi da rede
Bluetooth	Para se conectar a dispositivos *bluetooth* emparelhados
Administrador de Bluetooth	Para descobrir e parear dispositivos *bluetooth*
Alterar o status da rede	Para alterar o status de conectividade da rede
Alterar o Wi-Fi da rede	Para alterar o status de conectividade Wi-Fi
Desativar proteção de teclado	Para desativar a proteção do teclado se não for segura
Serviço de primeiro plano	Para usar serviço em primeiro plano
Internet	Para abrir sockets de rede
Receber *boot* concluída	Para receber a intenção transmitida logo após o *booting*
Uso da biometria	Para usar as modalidades biométricas suportadas pelo dispositivo
Vibração	Para acessar a vibração
Manter o dispositivo com a tela ligada	Para evitar que o processador hiberne ou a tela escureça

Fonte: Tramontana e Verga (2019)

Quadro 4. Exemplos de permissões perigosas.

Grupo de permissão	Permissões
Calendário	Consulta dados do calendário, inserir dados no calendário
Registro de chamadas	Ler dados de registro de chamadas, inserir dados registros no calendário e processar chamadas feitas
Câmera	Acesso a câmera
Contatos	Consulta dados nos contatos, inserir dados nos contatos e obter contatos
Localização	Acessar localização precisa, acessar localização aproximada
Microfone	Gravar áudio
Telefone	Ler status do telefone, ler números de telefone, ligar, atender chamadas e correio de voz
Sensores	Sensores corporais, enviar, receber, ler e receber *sms*
Armazenamento	Ler armazenamento externo, inserir dados em armazenamento externo

Fonte: Tramontana e Verga (2019)

de “comunicação”, como mostra a Tabela 5. Já as categorias “reprodutores de vídeos”, "editores", "sociais”, "educação” e “jogos" têm o maior número de serviços de terceiros. (Lai & Flensburg, 2020)

Aplicativos de comunicação normalmente requerem muitas permissões relacionadas a bibliotecas ou ao rastreamento de terceiros, o que torna essa categoria extremamente intrusiva. Como mostrado na Tabela 6, Facebook é o aplicativo de comunicação que solicita o maior número de permissões e coopera com uma grande quantidade de bibliotecas de terceiros em comparação com os outros aplicativos da categoria (Lai & Flensburg, 2020).

Kusyanti e Catherina (2018) buscaram determinar os fatores que levam os usuários a ler ou não as permissões solicitadas por aplicativos. Concluíram que os motivos da indisposição dos usuários em ler o conteúdo dessas permissões são: *(i)* preguiça, visto que normalmente elas são complexas ou longas; *(ii)* não as considerarem importantes; *(iii)* terem a sensação de desperdício de tempo; *(iv)* presunção de que não há riscos em dá-las.

Um aspecto que dificulta a leitura e compreensão das políticas de privacidade é o tamanho de tela limitado dos dispositivos móveis. Isso foi confirmado por Singh, Sumeeth e Miller (2011), que examinou o quão legível são os documentos de política de privacidade em ambientes móveis.

Vários outros estudos têm mostrado que usuários, em geral, não se atentam às solicitações

Tabela 4. Visão geral de permissões importantes e os acessos específicos que exigem.

Permissão	Permite ao aplicativo...	%
Acesso total à rede	Enviar pedidos e obtenha respostas através da rede (Wi-Fi ou dados móveis)	97%
Recepção de dados da internet	Receber mensagens *push* da Internet	81%
Leitura o conteúdo de um armazenamento USB	Acessra conteúdo armazenado no cartão SD do telefone	78%
Modificação ou deleção o conteúdo de um armazenamento USB	Mudar ou apagar armazenados no cartão SD do telefone	79%
Ver conexões Wi-Fi	Visualizar informações sobre Wi-Fi, redes (nome, status, etc)	60%
Localização precisa (GPS e com base na rede)	Recuperar a localização precisa usando o sistema de posicionamento global (GPS) ou torres de celular e Wi-Fi	53%
Execução na inicialização	Começar assim que o telefone for ligado	53%
Tirar fotos e grave vídeos	Acessar a câmera a qualquer momento e tire fotos e vídeos com ela	49%
Encontrar contas no dispositivo	Obter a lista de contas conhecidas pelo telefone Também existem contas criadas por outros aplicativos	33%
Leitura do status e da identidade do telefone	Acessar os recursos do telefone e determina o número do telefone e IDs do dispositivo, se uma chamada está ativa e o número conectado	29%

Fonte: Lai e Flensburg (2020)

de permissão e possuem baixa compreensão dessas permissões. Pesquisas relataram que menos de 20% dos usuários prestam atenção a permissões durante a instalação de aplicativos, e apenas 3% se lembram do seu conteúdo (Felt et al., 2012; Kelley et al., 2012).

3.5 Sistemas operacionais

Devido ao ambiente de desenvolvimento aberto do Android, não é trivial restringir ou impedir que os desenvolvedores escondam os códigos de captura de dados inseridos em seus aplicativos. Enck et al. (2011) estudou cerca de mil aplicativos Android, e descobriu que metade deles expôs informações de localização dos usuários para publicidade sem ter tido consentimento para isso. Críticos apontaram para a loja Android como "um mar de problemas de privacidade" (Zang et al., 2015).

Outra dificuldade encontrada no sistema operacional Android é que há muitos problemas de atualização ocasionados pelas fabricantes. Estima-se que 68% dos aparelhos Android não recebem atualizações que, provavelmente, resolveriam problemas de segurança de dados (Gubernatorov et al., 2020). O fato de que alguns *smartphones* são desatualizados ou incompatíveis com as novas versões do sistema operacional, deixa a tarefa de preservar a privacidade nas mãos dos desenvolvedores, tendo eles que empregar seus próprios mecanismos de defesa (Kul, Upadhyaya, & Chandola, 2018).

A Apple tem a privacidade do usuário como prioritário. Seus produtos são considerados difíceis de hackear e de serem alterados, e possuem atualizações frequentes para corrigir problemas relacionados à privacidade. Além disso, nem mesmo a Apple pode visualizar os dados que são transmitidos, devido ao tipo de criptografia utilizada (Singh, Saini, & Bathla, 2019).

Embora as empresas mencionadas permitam que os usuários excluam suas contas das plataformas, é difícil afirmar o que de fato acontece com os dados dessas contas excluídas (Noor et al., 2016).

3.6 *Bloatwares*

Bloatware é o termo usado para descrever aplicativos pré-instalados fornecidos com os *smartphones* novos. Não existem meios oficiais para a remoção desses aplicativos, apesar de existirem formas alternativas para isso, que podem, no entanto, gerar vulnerabilidades de segurança, instabilidade no sistema e perda da garantia. Devido à dificuldade de exclusão, a violação de privacidade pode ser sustentada por um longo período de tempo (Spensky, 2016).

O uso massivo de permissões perigosas por *bloatwares* concede a eles um maior poder em

Tabela 5. Média de permissões solicitadas e de bibliotecas de terceiros para cada categoria de aplicativos.

Categorias	Número de aplicativos analisados	Média de permissões	Média de bibliotecas de terceiros	Exemplos de aplicativos
Pesquisa	1	72	2	Google
Comunicação	9	34	5	Viber, WhatsApp
Reprodução de vídeos e editores	1	16	20	Imgur
Social	8	30	5	Facebook, Instagram
Relacionamento	1	18	12	Tinder
Música e áudio	6	19	8	Spotify, Shazam
Educação	2	13	12	Forældreintra, Duolingo
Viagem e navegação	25	17	6	Airbnb, Google Maps
Fotografia	12	14	8	Airbrush, CoCrop
Produtividade	8	19	3	Outlook, Google Docs
Jogos	12	10	12	Angry Birds, SongPop 2
Saúde e *fitness*	11	15	6	Clue, Endomondo
Religião	3	12	9	Holy Bible, Joyce Meyer
Compras	9	13	8	H&M, Asos
Entretenimento	6	13	7	Kino, IMDB
Ferramentas	4	17	2	QR Reader, Google Translate
Negócios	4	17	2	PlanDay, My Business
Esporte	6	11	7	US Open, Forza Football
Privacidade	3	14	3	AdBlock, AdBlocker Plus
Comidas e bebidas	4	11	6	5:2 Recipes, Wolt
Streaming	5	12	5	Netflix, Viaplay
Tempo / Clima	3	12	4	YR, DMI Vejr
Finanças	11	13	2	MobilePay, Mobilbank
Estilo de vida	3	10	5	Dalle Valle, Opskrifter
Eventos	3	9	6	Vega, Royal Arena
Jornais e Revistas	9	8	6	BT, NYTimes
Livros e referências	2	6	2	Biblioteket, Sproghjælp
Veículos	1	4	3	My Mazda

Fonte: Lai e Flensburg (2020)

comparação com os aplicativos instalados através das lojas (Wei et al., 2012). Além disso, aplicativos *bloatware* têm sido metodicamente utilizados por empresas como o Google, ao forçar fabricantes a pré-instalar o Google Chrome em seus *smartphones*, gera uma receita considerável de lucro com dados capturados (European Commission, 2018).

Elahi, Wang e Chen (2020), com base no conjunto de 17.179 aplicativos Android, revelaram que a maioria dos aplicativos de *bloatware* podem acessar dados confidenciais. Afirmam que esses aplicativos possuem altos níveis de privilégio em comparação com aplicativos instalados pelas lojas. Eles são uma grande ameaça à privacidade dos usuários.

Há um grande número de aplicativos em um único *smartphone* que capturam e processam esses dados. A quantidade de *Bloatwares* que podem gravar áudio, obter informações sobre serviços de telefonia, manipular mensagens SMS e acessar o status da rede é bastante alta. Em relação ao armazenamento externo, um grande número de *bloatwares* solicitam permissões para acesso de leitura e gravação, extraviando-se, muitas vezes, de suas funções típicas (Elahi, Wang, & Chen, 2020). Por fim, os resultados mostram que vários *bloatwares* não preservam

Tabela 6. Média de permissões solicitadas e de bibliotecas de terceiros por aplicativos de comunicação.

Aplicativos	Empresa	Permissões	Bibliotecas ou rastreadores de terceiros
Messenger	Facebook	46	10
WhatsApp	Facebook	43	1
Gmail	Alphabet	39	1
Viber	Rakuten	44	11
Skype	Microsoft	40	5
Signal	Signal	44	0
Slack	Slack	19	4
Mobilporto	Post Nord	17	4
Popularsticker	Ghostwording	12	Sem dados

Fonte: Lai e Flensburg (2020)

a segurança e desrespeitam princípios de privacidade, capturam dados confidenciais e acessam recursos críticos do dispositivo.

3.7 Desenvolvedores e seus conhecimentos sobre privacidade

Desenvolvedores de aplicativos móveis variam de amadores a extremamente capacitados (Stack Overflow, 2020). Seus aplicativos possuem capacidade de capturar uma ampla variedade de dados pessoais. Os desenvolvedores têm permissão para implementar quase qualquer tipo de função em seus aplicativos. Alguns costumam utilizar bibliotecas de código aberto, nas quais existem comandos que implementam funções de obtenção e captura de dados. (Dai et al., 2017).

Em muitos casos, os desenvolvedores são indivíduos ou uma pequena equipe com pouco conhecimento sobre privacidade e sobre como as legislações concernentes devem ser incorporadas a seus aplicativos. Esse tipo de desenvolvedor pode criar riscos significativos à vida privada dos usuários de *smartphones* (Wong & Zhu, 2016). Concomitantemente, serviços de terceiros, como publicidade, estão se desenvolvendo rapidamente e, se utilizados por desenvolvedores sem devido cuidado, podem divulgar dados pessoais de seus usuários.

Greene e Shilton (2018) verificaram que a privacidade é frequentemente debatida entre desenvolvedores iOS e Android. Mas eles definem e abordam a privacidade de maneiras diferentes nessas plataformas. A subjetividade dos desenvolvedores e as normas da plataforma são os principais fatores que auxiliam na definição de conceitos de privacidade. A plataforma, por meio de restrições e políticas, desencoraja ou proíbe os desenvolvedores de tomar certas decisões e os incentiva a seguirem suas regras. As plataformas exercem um enorme benefício: introduzir conceitos de privacidade aos desenvolvedores (Gillespie, 2015).

Os diferentes significados de privacidade nos ecossistemas Android e iOS produzem resultados diferentes para os usuários. Os desenvolvedores iOS, por exemplo, parecem estar mais preocupados com os conceitos de privacidade definidos pela Apple do que na exploração de conceitualizações de outras fontes. Há tempos existem críticas quanto a essa postura da Apple (Martin, 2013).

A Apple requer um processo de aceitação para todos os aplicativos em sua loja. Para isso, os desenvolvedores devem cumprir suas políticas de conteúdo, privacidade e segurança (Spencer, 2016). Em contraste, o Android é uma plataforma de código aberto em que desenvolvedores têm maior liberdade. Ainda assim, a inserção de aplicativos na *Google Play Store* exige que os desenvolvedores concordem com o contrato de distribuição do desenvolvedor do Google, que inclui instruções básicas de privacidade. Logo, em ambas as plataformas, os desenvolvedores devem obedecer a um conjunto de regras (Holzer & Ondrus, 2011; Gillespie, 2015).

Por conseguinte, plataformas móveis não são apenas intermediárias de suporte a outras tecnologias. Elas possuem uma importância fundamental na promoção de normas específicas de privacidade e de treinamento de programadores, além do poder de puni-los com base em seus desempenhos. Logo, as plataformas têm

um papel fundamental de educar desenvolvedores sobre questões de privacidade (Greene & Shilton, 2018)

As diferenças entre as várias legislações no mundo também se tornaram um problema aos desenvolvedores, visto que a captura de dados pessoais geralmente faz com que fiquem sujeitos às leis locais de privacidade de dados. Eles muitas vezes não têm conhecimento prévio da legislação de privacidade de dados dos países onde seus aplicativos são distribuídos. Uma situação que se tornou comum é a de uma empresa responder às reclamações de privacidade de usuários estrangeiros com a declaração de que não se responsabilizarão pelo fato de que não são regidas pela legislação estrangeira (Fong, 2017).

3.8 Plataformas de aplicativos

Lojas de aplicativos são a principal forma dos usuários baixarem os programas em seus *smartphones*. Essas lojas são um mercado *online* no qual os desenvolvedores de aplicativos podem disponibilizá-los e os usuários podem baixá-los para consumo. São as entidades intermediárias entre desenvolvedores e usuários de aplicativos.

Como foi visto anteriormente, embora as plataformas não decidam diretamente sobre o controle dos dados coletados, elas têm um papel importante em garantir que a privacidade dos dados seja protegida.

Em 2014, autoridades da privacidade globais, como a *Global Privacy Enforcement Network*, enviaram uma carta aberta a vários mercados de aplicativos, reconhecendo a importância de suas lojas no que diz respeito à privacidade. A carta incentiva as lojas a assumirem a responsabilidade na proteção da privacidade de dados, garantindo que cada aplicativo tenha sua política de privacidade, que contenha informações sobre a utilização dos dados coletados e capturados e sobre como irá proteger a confidencialidade dos usuários, e para colocar em prática mecanismos que fazem cumprir esta responsabilidade. Esta carta é um reconhecimento internacional do importante papel que as lojas de aplicativos desempenham na proteção de privacidade de dados dos usuários (Office of the Privacy Commissioner of Canada, 2014).

Cada loja tem seus próprios requisitos para que os aplicativos possam ser aceitos, e requisitos para que eles não sejam removidos (Fong, 2017):

- ***Apple Store***. Para que um aplicativo seja distribuído por meio da *App Store*, os desenvolvedores devem concordar com o "Contrato de Licença de Desenvolvedor Apple". Antes de serem aceitos na loja, os aplicativos devem ser enviados à Apple para avaliação. O contrato inclui o cumprimento de requisitos sobre coleta e captura de dados, legislações, entre outras informações sobre privacidade.
- ***Google Play Store***. Para ser disponibilizado na *Play Store*, o aplicativo deve assinar o "Contrato de distribuição do desenvolvedor" do *Google Play*. Nele, há uma cláusula em que os desenvolvedores devem concordar em proteger a privacidade dos usuários.

Em 2015, o Google anunciou que os aplicativos seriam analisados usando ferramentas automatizadas com supervisão humana (Welch, 2015). Ter uma política de privacidade de dados é um requisito utilizado por ambas as lojas de aplicativos. Por exemplo, o *Apple Developer Agreement* afirma que é preciso da autorização do usuário antes da coleta de dados e tais dados devem ser usados apenas para fins previamente especificados (Fong, 2017). Da mesma forma, o *Google Developer Agreement* estabelece que os aplicativos devem seguir conforme suas políticas de privacidade e a captura de dados precisa ser limitada a somente aos casos permitidos pelo usuário (Fong, 2017).

Em outubro de 2015, foi relatado que a Apple havia removido 250 aplicativos de suas lojas por ter sido descoberto que eles transmitiam informações pessoais[1]. Em setembro de 2016, a Apple analisou 2 milhões de aplicativos em sua plataforma, removendo aqueles desatualizados e os que não estavam em conformidade com as suas políticas (Goel, 2016; Hern, 2015).

Entretanto, dificilmente as lojas de aplicativos determinarão a finalidade e os meios de processamento de dados. Elas também não controlam a utilização dos dados. Logo, lojas de aplicativos são incapazes de determinar modos e motivos para a coleta e utilização de dados (Fong, 2017).

Outra área que é importante na discussão da regulamentação dos intermediários de aplicativos é a possibilidade de responsabilidade das

[1] https://www.virtualdcs.co.uk/blog/apple-pulls-250-privacy-infringing-applications-from-its-app-store

plataformas. Se as lojas de aplicativos forem responsáveis pela conduta dos aplicativos, eles seriam indiretamente regulados por meio da responsabilidade assumida pela plataforma[2].

Singh, Saini e Bathla (2019) apresentam uma possível solução que as plataformas poderiam adotar quanto à privacidade de seus usuários: na loja, a página de *download* de cada aplicativo deveria listar os dados acessados pelo aplicativo com a explicação do motivo do acesso daquele dado. Depois que o usuário instala um aplicativo, ele não deve apresentar todas as permissões de uma vez, mas sim aos poucos, quando julgar necessário. As plataformas devem ter uma página que apresenta a quantidade e o momento em que dados estão sendo usados por cada produto. As lojas devem facilitar a alteração de preferências para permitir ou negar acesso a um aplicativo.

3.9 Publicidade e empresas terceirizadas

Ao analisar o comportamento dos usuários, uma empresa pode obter com precisão e rapidez o cenário das tendências de mercado, principalmente para marketing e publicidade (Baalous, Poet, & Storer, 2018). Algumas empresas, frequentemente, contratam terceiros para fornecer-lhes certos serviços úteis. Isso implica que os dados pessoais dos usuários serão compartilhados com essas entidades, que podem até mesmo ter uma própria política de privacidade diferente da do aplicativo (Baalous, Poet, & Storer, 2018).

Estudos afirmam que cerca de 70% dos aplicativos compartilham os dados coletados com empresas como o *Google Analytics* (Vallina-Rodriguez, 2018). Essas empresas podem obter dados de vários aplicativos com o objetivo de lucro, criando anúncios direcionados. Anúncios direcionados, que têm como base os interesses do usuário, já existiam com o uso de *desktops* e *laptops*, mas a captura de dados no âmbito de *smartphones* tem um nível maior de detalhamento (Jayakumar, 2019). Alguns dos dados mais utilizados por essas empresas são os históricos de pesquisa e de navegação, localização, postagens visualizadas, interações nas redes sociais, nacionalidade, idade, fotos e vídeos assistidos e gênero (Polykalas & Prezerako, 2019), e até algumas palavras-chave baseadas na atividade do teclado.

Pesquisadores preocupam-se porque esse tipo de publicidade pode gerar vazamento de dados e muitos desses aplicativos não solicitam permissões para acesso desses dados. Com a localização disponibilizada pelo aparelho, é possível verificar quais lugares os usuários mais frequentam ou que já foram frequentados, dando abertura para anúncios relacionados a viagens ou serviços próximos a esses locais (Jayakumar, 2019).

Alguns exemplos podem ser citados sobre esse assunto (Presthus, 2019;). Houve casos em que os preços de hotéis variavam de acordo com os locais frequentados pelo usuário, ou alguém que, ao mudar o status de relacionamento no Facebook de solteiro para noivado, começou a receber anúncios de anéis de noivados. A criação de perfis tem potencial até mesmo para prejudicar grupos minoritários, vulneráveis ou com dificuldades financeiras, envolvendo, por exemplo, oferta de preços diferenciados ou privando certos grupos. Um caso conhecido foi o da empresa de marketing DoubleClick, cujos rastreadores direcionaram anúncios de empregos de melhor remuneração para homens em uma frequência superior se comparado às mulheres (Binns et al., 2018).

3.10 Captura de dados

A seguir são destacados os principais alvos de captura de dados.

Fotos e vídeos

Os aplicativos com foco em imagens muitas vezes contêm informações privadas e confidenciais do usuário, como informações de cartão de crédito capturadas nos arredores de uma foto. O fato de normalmente haver um único pedido de permissão para acesso à câmera, resulta no problema de captura de informações mesmo quando o aplicativo está em segundo plano, além da capacidade de transferir informações dela pela rede (Jensen et al., 2019).

Devido às tecnologias avançadas de visualização de imagem, informações extras podem ser obtidas a partir das fotos tiradas por *smartphones*, como, por exemplo, localização e horário. Como resultado, é possível obter não somente informações do conteúdo visual da foto, mas também outras informações privadas. Algumas fotos têm significativo valor comercial em organizações terceirizadas. Um rascunho do design

[2]https://www.economist.com/business/2016/03/10/things-are-looking-app

de um produto de uma empresa, por exemplo, poderia ser de extremo interesse para outra concorrente (Dai et al., 2017).

Devido a fragilidade e limitação do sistema de permissões dos *smartphones*, assim que um usuário autoriza a permissão de um aplicativo para acessar uma foto, este aplicativo utiliza essa permissão para todo o álbum e por tempo indefinido (Dai et al., 2017).

Contatos

A partir do relatório de *Appthority*, 26% dos principais aplicativos iOS gratuitos e 8% dos pagos acessam os catálogos de endereços dos usuários. Também 30% dos principais aplicativos para Android gratuitos e 14% dos pagos acessam esse catálogo. O acesso a todos os contatos é mais vantajoso para os aplicativos, porque é de interesse dos desenvolvedores verificar não somente o status do usuário, mas também de seus contatos sobre o uso de algum aplicativo. Quando o usuário autoriza que um aplicativo acesse sua lista de contatos, ele pode continuar obtendo seus dados indefinidamente, a menos que o usuário desative manualmente a permissão (Dai et al., 2017).

Status do telefone e informações sobre os serviços de telefonia

Dados sobre serviços de telefonia incluem número SIM (*Subscriber Identity Module*), detalhes da operadora e status da chamada. Essas permissões possibilitam que os aplicativos façam e processem chamadas, além de ler, escrever e receber mensagens SMS e MMS (Dai et al., 2017).

Em relação ao status do telefone, a análise dessas informações revela detalhes, como o número de telefone, informações atuais da rede, o status de chamadas em andamento, contas de telefone registradas no dispositivo e número de telefone de uma chamada, os detalhes da operadora, detalhes do SIM e detalhes do provedor de serviços (Dai et al., 2017). Como foi dito, tal função foi confirmada na análise dos aplicativos *bloatware* por Elahi, Wang e Chen (2020).

O IMEI (International Mobile Equipment Identity) e UDiD (*Unique Identifier*) constituem o identificador único de um telefone celular e podem ser usados para identificar dispositivos. Ambos são utilizados para criar perfis de usuários, fator considerado como um grande risco à privacidade (Elahi, Wang, & Chen, 2020).

Bancos de dados de outros aplicativos

Geralmente, o banco de dados de cada aplicativo é privado e não permite o acesso de outros aplicativos. Entretanto, existe a possibilidade de permitir que outros aplicativos consultem o banco de dados através da configuração do provedor de conteúdo. Kul, Upadhyaya e Chandola (2018) afirmam que, além da ampla quantidade de casos de vulnerabilidades à privacidade no banco de dados dos aplicativos, existem outras com semelhantes consequências que ainda não foram descobertas.

Localização

A localização é algo que, atualmente, é básico nos *smartphones*. Com ela os usuários recebem informações de trânsito, clima, locais, entre outros e, com isso, ela se torna uma ferramenta valiosa para os desenvolvedores de aplicativos de saúde, navegação, redes sociais e jogos. Há relatos de que em aparelhos com o sistema operacional Android, mesmo que ele esteja desligado, sem cartão SIM, sem acesso à Internet e com nenhum aplicativo necessitando do serviço da posição do usuário, ainda assim os dados de localização são coletados e enviados ao Google no momento que se conecta a internet (Baraniuk, 2018).

Para desempenhar sua função, muitos aplicativos necessitam obter a localização do usuário para poder operar, como é o caso de aplicativos de namoro, que podem transmitir continuamente a localização do usuário em tempo real para encontrar correspondentes potenciais próximos (Farnden, Martini, & Choo, 2015). Zang et al. (2015), com base em uma amostra de 110 aplicativos populares, relatou que 47% dos aplicativos iOS compartilham coordenadas geográficas e outros dados de localização com terceiros.

O sistema iOS oferece um serviço de sistema sobre local, denominado Locais Frequentes, utilizado para registrar os lugares visitados pelos usuários. O usuário pode até desativar esse serviço, mas os dados continuarão sendo capturados pelo sistema operacional, ficando apenas invisível ao usuário (Dai et al., 2017).

Dados obtidos por certas categorias de aplicativos

De acordo com Atkinson et al. (2016), apesar da importância da captura de dados pessoais para sua inserção no banco de dados do aplicativo, também é possível obter informações dos

usuários de forma externa, sem utilizar um aplicativo hospedeiro ou o sistema operacional. Uma série de informações podem ser inferidas a partir de dados funcionais de outros aplicativos, a saber:

- Aplicativos de notícias podem resultar na descoberta do idioma ou nacionalidade e os vieses políticos do usuário;
- Aplicativos de compras auxiliam na inferência da renda de um usuário;
- Aplicativos de relacionamentos podem identificar o estado civil e a faixa etária do usuário;
- Alguns aplicativos são exclusivos de algumas regiões e podem fornecer informações de nacionalidade;
- A presença de certos aplicativos pode servir para inferir hobbies ou até mesmo vícios, como, por exemplo, aplicativos de loteria, que indicam disposição para o jogo;
- Aplicativos imobiliários fornecem informações sobre a renda de um usuário;
- Aplicativos de saúde podem fornecer informações como grau de ansiedade, se for um aplicativo de controle de ansiedade;
- Aplicativos de gravidez e menstruação denotam informações de saúde, sexo e idade dos usuários.

3.11 Rastreamento e bibliotecas de terceiros

O rastreamento de terceiros é uma tecnologia que os desenvolvedores inserem em seus aplicativos principalmente para fins de marketing e publicidade. Permite que se identifique usuários e rastreie seus comportamentos. A partir dos dados coletados por esses rastreadores, e com auxílio de bibliotecas analíticas, empresas de análise fornecem estatísticas aos desenvolvedores (Liu et al., 2019).

Binns et al. (2018) analisaram o uso de rastreadores de terceiros em 959.000 aplicativos das lojas *Google Play* dos EUA e Reino Unido, e constataram que a maioria deles contém tais rastreadores. A construção de perfis detalhados por meio destes rastreadores foi usada para uma variedade de fins, desde publicidade direcionada até mensagens de campanha políticas.

Muitos aplicativos têm um alto número de rastreadores que não servem de auxílio para as suas funções, mas sim para fins de publicidade e análises. Pouco mais de 90% de todos os aplicativos analisados continham pelo menos um rastreador. Em média, cada aplicativo continha rastreadores de 5 empresas, sendo 17% com mais de dez empresas.

A sede da maioria dessas empresas se encontra nos Estados Unidos, China, Noruega, Rússia, Alemanha, Cingapura e Reino Unido. O rastreamento também se mostrou um fenômeno multinacional: muitos aplicativos analisados enviam dados para rastreadores localizados em mais de um país (Binns et al., 2018).

Embora ferramentas de terceiros para anúncios estejam cada vez mais populares, foi confirmado que os próprios desenvolvedores desconhecem quais e como os dados são coletados por essas ferramentas (Balebako et al., 2014). Eles, muitas vezes, não têm ciência dos riscos envolvidos por essas bibliotecas que, em geral, possuem interesses diferentes dos desenvolvedores (He, Hu, & Han, 2019).

Muitos dos aplicativos analisados por Brandtzaeg, Pultier e Moen (2018), apesar de compartilharem informações com terceiros, não informam quais as empresas com quem os dados são compartilhados. O estudo também concluiu que o rastreamento era contínuo, visto que alguns aplicativos rastrearam os usuários mesmo quando o aplicativo não está sendo utilizado.

De acordo com He, Hu e Han (2019), as bibliotecas de terceiros obtêm dados do próprio sistema do *smartphone*, IMEI e MAC (*Media Access Control*), por exemplo. Leem informações relacionadas à localização e se conectam com a rede, o que pode levar ao vazamento de dados e violações de privacidade. Inclusive, essas são as informações que vazam com mais frequência. A rede Wi-Fi é o principal meio para o vazamento dessas informações.

A maioria dos dados coletados são transferidos para os Estados Unidos, dando às empresas de tecnologia norte-americanas enorme vantagem se comparados a empresas de outros países. Outro problema é que cada país tem uma diferente legislação sobre privacidade de dados (Brandtzaeg, Pultier, & Moen, 2018).

Para Brandtzaeg, Pultier e Moen (2018), o fato de que alguns aplicativos não utilizarem rastreamento ou bibliotecas de terceiros não significa necessariamente que esses serviços oferecem maiores níveis de privacidade. O Facebook, por exemplo, é uma grande empresa que não possui necessidade de enviar dados para outros, mas já se envolveu em escândalos de privacidade de dados.

Muitas fontes de anúncios, apesar de capturarem informações confidenciais, não especificam isso em sua documentação (Stevens et al., 2012). Tal comportamento está se tornando cada vez mais comum (Book, Pridgen, & Dan, 2013).

Embora haja um enriquecimento de informações a respeito das bibliotecas de publicidade, as analíticas ainda sofrem com uma grande falta de informação e possuem poucas pesquisas e trabalhos sobre o tema. Diferentemente das bibliotecas de publicidade, os desenvolvedores precisam definir previamente quais dados serão manipulados ou utilizados por bibliotecas analíticas. Depois da captura, elas os enviam para as empresas que analisam e apresentam os resultados aos desenvolvedores (Liu et al., 2019).

Liu et al. (2019) mostram que bibliotecas analíticas podem ser exploradas por desenvolvedores mal intencionados para coletar informações pessoais dos usuários. Foi confirmado também que alguns aplicativos realmente vazam informações pessoais dos usuários para empresas de análise, embora muitas vezes nem os desenvolvedores saibam disso. Os autores concluem que os programadores raramente informam os dados pessoais disponíveis acessados por seus aplicativos. Cabe citar que empresas de análise podem causar significativo dano à privacidade, pois elas podem vincular os dados coletados de vários aplicativos. Quanto mais popular a biblioteca analítica, mais perigosa ela é, visto que mais informações ela pode obter.

3.12 Vazamento de dados através de Wi-Fi

De acordo com um relatório publicado pelo *World Advertising Research Center* (WARC), quase 75% do mundo usarão apenas seus *smartphones* para acessar a Internet até 2025. Hoje, devido a sua vulnerabilidade, conexões sem fio para o vazamento de dados é bastante utilizada para captura de dados.

Um famoso caso, conhecido como *"London's tracking bins"* (caixas de rastreamento de Londres), é um exemplo da vulnerabilidade de dados de *smartphones* por meio da tecnologia Wi-Fi (Beaumont, 2013), em que uma empresa inglesa estava aplicando tecnologia de rastreamento nas ruas de Londres. O caso envolveu lixeiras tecnológicas que apresentavam notícias e publicidade aos pedestres. A empresa foi obrigada a retirar as lixeiras após a queixa de que os dispositivos estavam coletando dados dos *smartphones* dos pedestres com o Wi-Fi habilitado, para a criação de perfis e para fins de marketing.

Aplicativos de dispositivos móveis são capazes de transmitir informações pessoais por meio do Wi-Fi, apesar do uso de criptografia. Atkinson et al. (2016) mostrou que, a partir da utilização do Wi-Fi, é possível inferir informações privadas do usuário sem a necessidade de um aplicativo hospedeiro. Logo, a análise se dá por meio de uma perspectiva externa. Neste estudo foram selecionados alguns dos principais aplicativos da *Google Play Store* com o objetivo de detectá-los remotamente. Os dados que podem ser inferidos apenas usando o rastreamento externo através do Wi-Fi são (Atkinson et al., 2016): gênero; religião; faixa etária; raça/etnia; idade aproximada; saúde psicológica e mental; estado civil; visão política; nacionalidade e opção sexual.

Outra descoberta interessante foi que mesmo aqueles aplicativos que não necessitavam de Internet para executar suas funções, se comunicavam na rede quando tinham oportunidade. Com as comunicações sem fio se tornando mais preponderantes, as empresas mostram uma maior disposição em rastrear e analisar a transmissão sem fio para captura de dados.

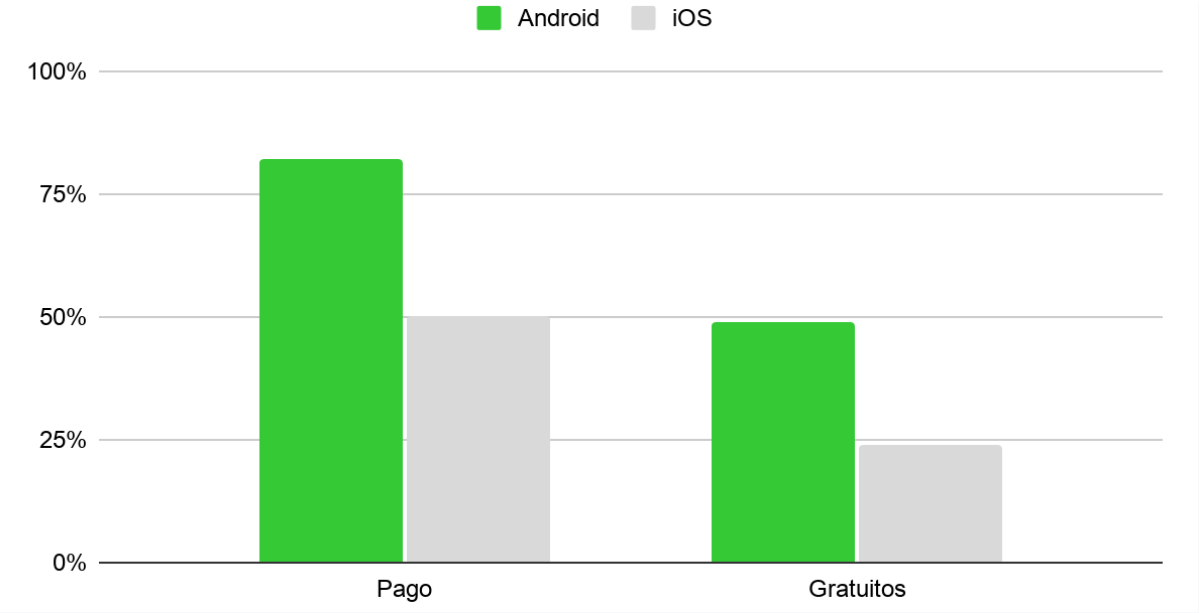
3.13 Aplicativos gratuitos Vs. pagos

Atualmente, aplicativos gratuitos são considerados apenas *aqueles* que não cobram nada para sua aquisição. Entretanto, muitos desenvolvedores consideram os dados capturados uma fonte mais rentável do que o próprio valor de desenvolvimento e manutenção do aplicativo. Por exemplo, ferramentas gratuitas como o Google Analytics não são gratuitas em sentido estrito, pois os dados que os aplicativos e sites enviam ao Google Analytics fundamentam seus outros empreendimentos e geram receita ao próprio Google.

É uma tendência servir-se do argumento de que os aplicativos gratuitos têm direito de lucrar servindo-se de formas alternativas, como a captura de dados. No entanto, isso deveria haver maior transparência a respeito disso e mais debates a respeito. Dados são altamente lucrativos. (Lai & Flensburg, 2020).

Outro argumento comum é que se os aplicativos fossem pagos, esse problema não existiria. No entanto, as estatísticas provam que os consumidores estão cada vez menos dispostos a pagar por um aplicativo (Pal & Crowcroft, 2019).

Figura 2. Relação entre aplicativos iOS e Android, pagos e gratuitos, com rastreamento de localização.



Fonte: Dai et al. (2017)

Aplicativos móveis gratuitos solicitam acesso a dados em maior quantidade em relação aos pagos, o que indica que os dados pessoais dos usuários são a fonte de renda de vários desses tipos de aplicativo. O relatório da *Authority* constatou que 50% dos principais aplicativos gratuitos para iOS e 82% dos gratuitos para Android rastreiam a localização do usuário (Figura 2). Em contrapartida, o número é consideravelmente menor para aplicativos pagos: 24% para iOS e 49% para Android (Dai et al., 2017).

3.14 Defesa ao compartilhamento de dados

Pal e Crowcroft (2019) defendem que o uso e compartilhamento de dados é inevitável, apesar das barreiras existentes para prevenir sua comercialização. As tentativas de proibir a captura, compartilhamento e comercialização de dados aumentam as chances de levar empresas a empregarem meios ilegais para alcançar esses fins, ou tirá-las do mercado. Além disso, os *Data Brokers*, corretores de dados, empresas que capturam informações pessoais de consumidores e as revendem ou compartilham com outros, possivelmente encontrariam maneiras alternativas de continuar essas práticas mesmo com as barreiras impostas. Logo, é provável que haveria uma violação inevitável de informações pessoais dos usuários para a sobrevivência dos sistemas de anúncios e publicidades digitais atuais (Barnes, 2006).

Cabe citar também que, diferente das grandes empresas que possuem soluções alternativas de lucros, as pequenas e médias empresas, altamente dependentes da publicidade comportamental, teriam dificuldades de encontrar outra fonte de lucro e de se manter no mercado. (Pal & Crowcroft, 2019)

Uma solução comercial seria aquela em que todos ganham: desenvolvedores e profissionais de marketing poderiam se beneficiar do compartilhamento de dados, mas teriam a obrigação de preservar a privacidade dos usuários. Já os usuários estariam dispostos a disponibilizar não seus dados pessoais, mas sim os dados mais genéricos, como a quantidade de horas de sono, em troca de ter acesso aos serviços oferecidos (Patrick, 2017).

3.15 Paradoxo da privacidade

Muitos dos usuários aceitam perder a privacidade, pois há um desejo de ter acesso ao que os *smartphones* podem proporcionar. Além disso, existe uma sensação de ser dominado e de perda de controle, isso é chamado de paradoxo da privacidade. É comprovado que, embora haja uma preocupação com os dados pessoais, ainda há o compartilhamento voluntário deles sem hesitação (Schomakers, 2020; Gerber

et al., 2018)[3]. Poucos usuários optam por negar as permissões, mesmo tendo ciência de que aplicativos acessam seus dados privados (DAI et al., 2017).

3.16 Problemas e soluções

Mesmo com o quadro de apresentado sobre a privacidade de dados pessoais em dispositivos móveis, há algumas ações que podem aumentar a segurança dos usuários. Eles devem, por exemplo, atentar para as solicitações de permissões. Uma das atitudes que pode ser tomada é desativar o acesso à localização de aplicativos que não precisam dela, e é recomendado deixar a permissão para acessar esse serviço apenas durante o uso do aplicativo, bloqueando o seu uso em segundo plano.

Outro método importante é sempre baixar e instalar aplicativos das lojas oficiais do sistema operacional, *App Store* para iOS e *Google Play Store* para Android, evitando fontes não-confiáveis (Chen et al., 2019). Deve-se também tomar cuidado sobre dados confidenciais em *backups* que são realizados pelos sistemas operacionais. Essa é uma prática não recomendada (Osho, 2019). O Quadro 5 resume algumas ações preventivas para se evitar o vazamento de dados pessoais.

4. Lei geral de proteção de dados pessoais

A presença de legislação sobre a proteção de dados pessoais é hoje realidade em 126 países. Essas leis visam a regulamentação do acesso e do tratamento de dados pessoais mantidos por empresas. No Brasil, tem-se a Lei 13.709 (Brasil, 2018), a Lei Geral de proteção de dados pessoais (LGPD). Por ela, é necessário o consentimento do titular dos dados pessoais para a sua utilização. Ele pode ainda determinar o nível de proteção e garantir a sua extensão. Logo, ele deve ser questionado, de forma explícita, se autoriza que seus dados sejam usados por alguma empresa, sendo o produto e serviço gratuito ou não.

O dono dos dados tem direito a obter a confirmação se seus dados estão sendo usados, e de ter acesso a eles, corrigi-los e eliminá-los, caso desejado. Ademais, o proprietário das informações pode solicitar a portabilidade de seus dados para outro serviço ou produto, saber se eles foram compartilhados e proibir seu uso,

Quadro 5. Cenário atual e proposta de ações preventivas.

Cenário atual	Proposta
As plataformas e os aplicativos não informam aos consumidores quais aplicativos e serviços eles devem usar e quais aplicativos coletam dados	Quando os usuários virem todas as informações sobre os dados coletados, eles prestarão mais atenção ao problema.
A maioria dos aplicativos solicitam acesso a dados que não estão relacionados ao funcionamento de seus aplicativos.	Os desenvolvedores devem apenas solicitar os dados que são necessários para o funcionamento de seu aplicativo
Se um usuário deseja excluir sua conta de seu aplicativo ou serviço, os desenvolvedores ainda podem manter seus dados em seus servidores e o usuário não terá como saber disso.	Os usuários devem ter controle sobre seus dados e mais ninguém. Os desenvolvedores não terão mais o controle sobre os dados de seus consumidores.
Os usuários não veem uma lista de recursos que um aplicativo acessa em seu *smartphone* antes de baixar o aplicativo. Além disso, existem apenas duas opções quando um aplicativo pede permissão para usar um recurso do usuário, que são "Permitir" e "Negar". Isso força alguns usuários a permitir o uso de um determinado recurso em todos os momentos, mesmo que pretendam usar esse recurso apenas uma vez.	Antes de baixar um aplicativo, o usuário analisa os recursos que um aplicativo deseja acessar. Além disso, a adição de outra opção "Permitir uma vez" em cada solicitação de permissão.

Fonte: Singh, Saini e Bathla (2019)

[3] Existem, hoje, reflexões sobre a conexão entre a servidão consentida, conceito proposto por La Boétie (1987) no século 16, e as novas tecnologias da informação e comunicação (Karnal, 2016). Ou seja, mesmo com perda de privacidade, muitos usuários não abrem mão dos serviços prestados por certos aplicativos.

segundo o art. 18 da LGPD. No art. 8 consta que "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas". Ao clicar em "permitir", há a autorização do que foi solicitado e, no pedido da permissão, o consentimento deverá ser em escrito ou por outra alternativa que transmita a intenção do aplicativo.

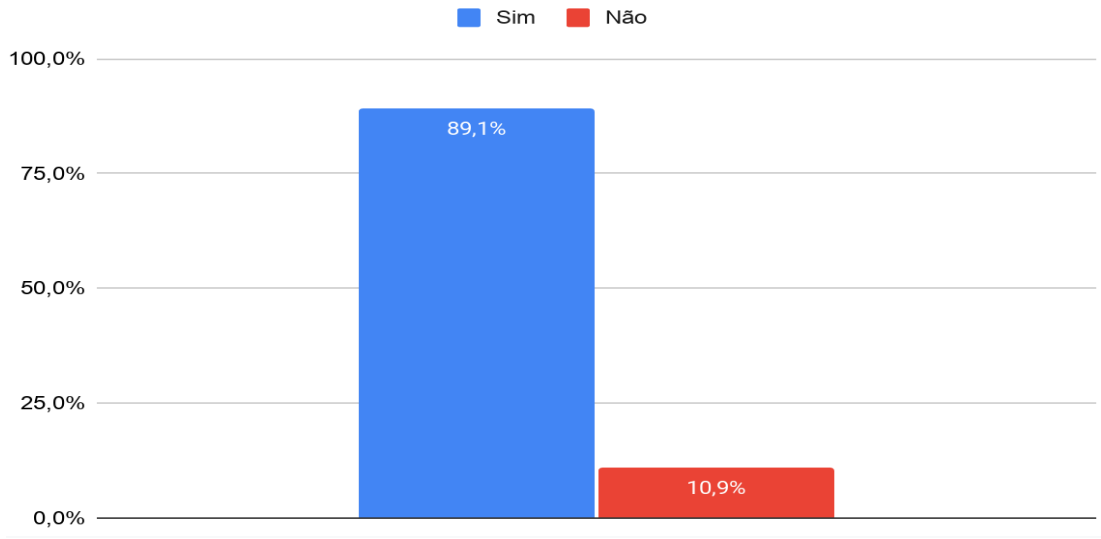
5. Pesquisa sobre privacidade, dados e segurança

Foi elaborado um questionário para levantar informações sobre a utilização do *smartphone* e como seus usuários lidam com a privacidade de seus dados. A pesquisa envolveu 92 respondentes.

Ao serem perguntados a respeito da preocupação com a privacidade de seus dados, a grande maioria (89,1%) respondeu afirmativamente (Figura 3), mas quando perguntados se pagariam para ter mais privacidade (Figura 4), apenas 12% aceitaria, e um pouco mais da metade (56,5%) condicionou a resposta positiva ao preço do serviço. O restante (31,5%) respondeu negativamente.

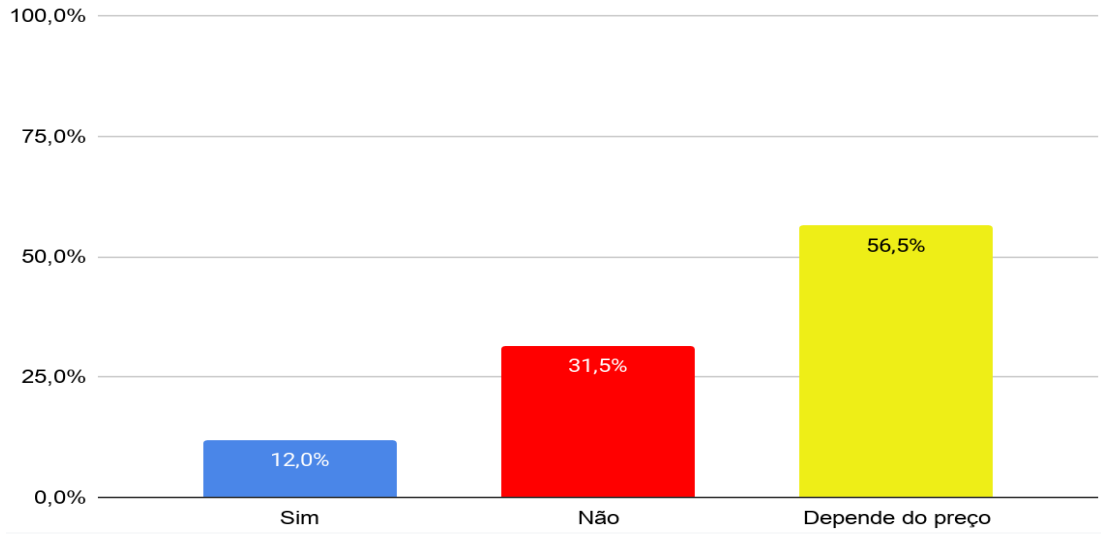
A maioria dos participantes armazenam fotos pessoais em seus *smartphones*, como mostrado na Figura 5. Assim como vídeos, elas são os dados mais solicitados por aplicativos, daí a necessidade de atenção à solicitação de permissão

Figura 3. Resultados da pergunta "Você se preocupa com a privacidade dos seus dados?".



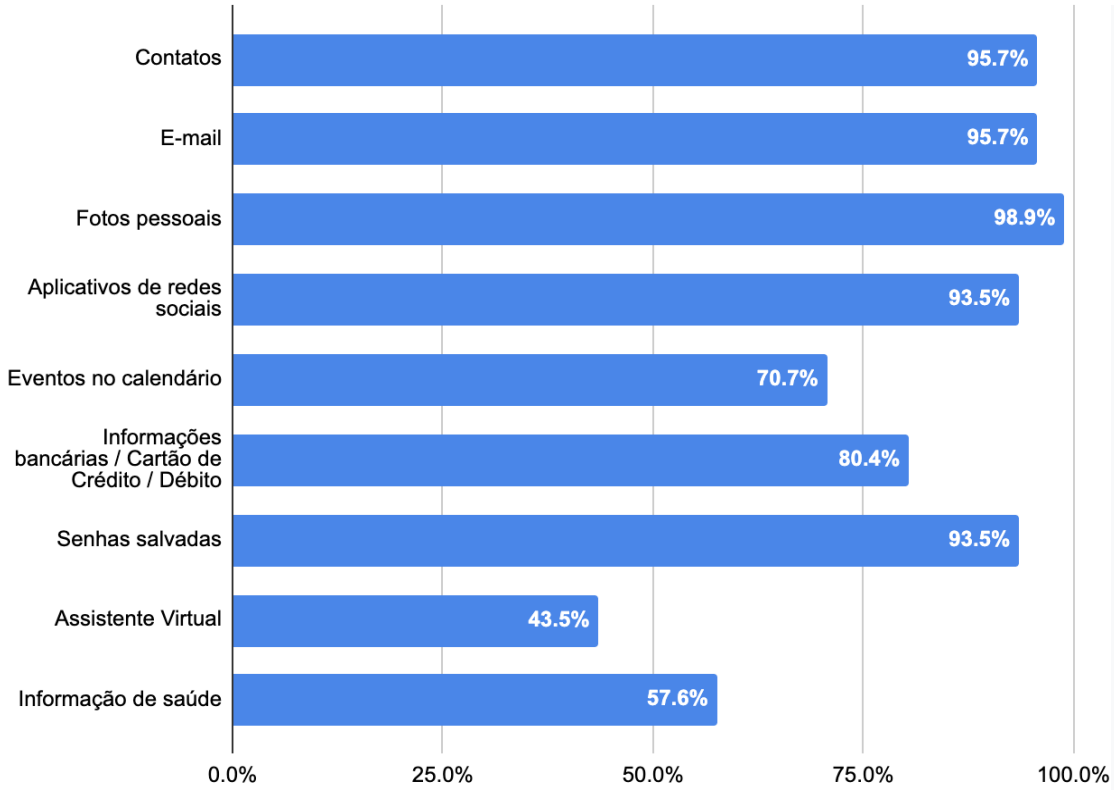
Fonte: Resultado da pesquisa

Figura 4. Resultados da pergunta "Você pagaria para ter mais privacidade?".



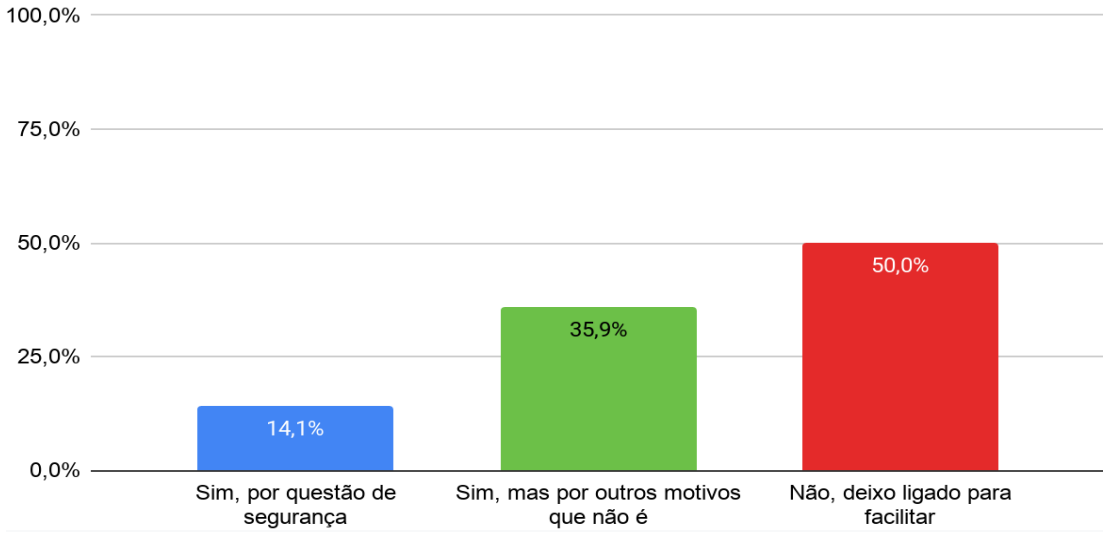
Fonte: Resultado da pesquisa

Figura 5. Resultados da pergunta "Quais informações você armazena no seu *smartphone*?".



Fonte: Resultado da pesquisa

Figura 6. Resultados da pergunta "Você costuma desligar elementos como Wi-Fi, Bluetooth e GPS?".



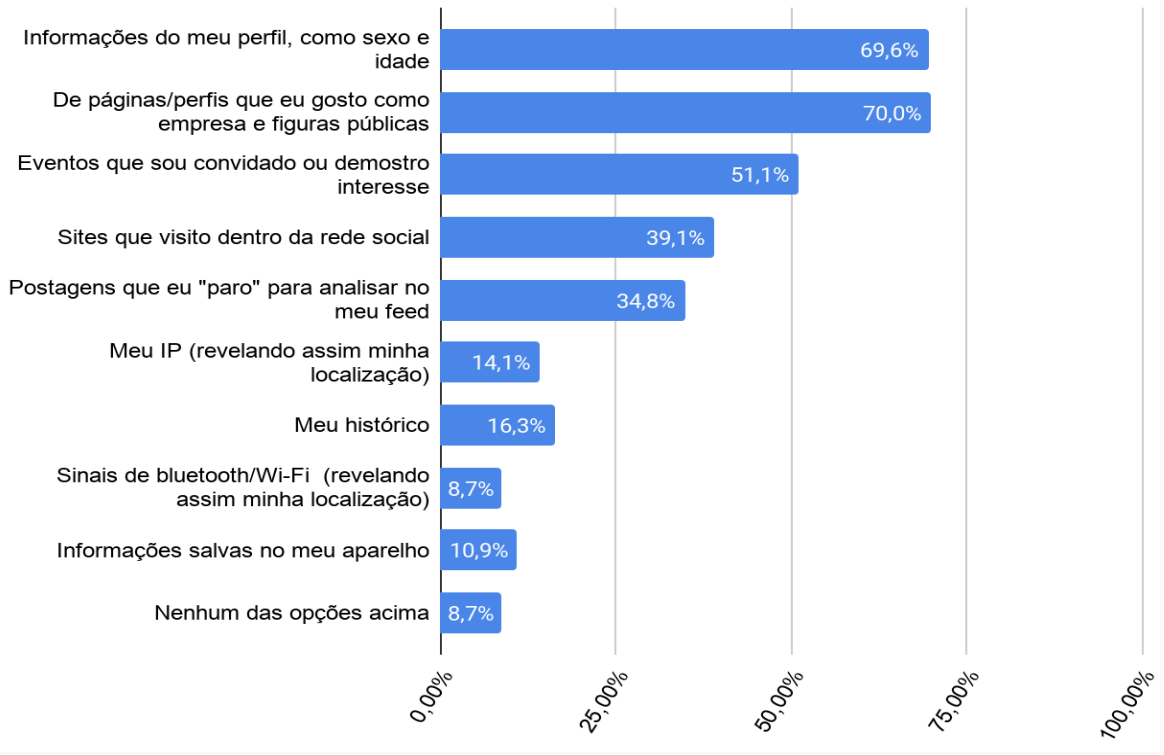
Fonte: Resultado da pesquisa

para as mídias.

Sobre as conexões e localizações dos aparelhos (Figura 6), metade dos entrevistados os deixam ligadas, abrindo assim a guarda para que outros aplicativos captem facilmente esses dados dos usuários, por exemplo, rastreando os lugares que eles mais frequentam e oferecendo produtos nas cercanias de onde ele costuma frequentar.

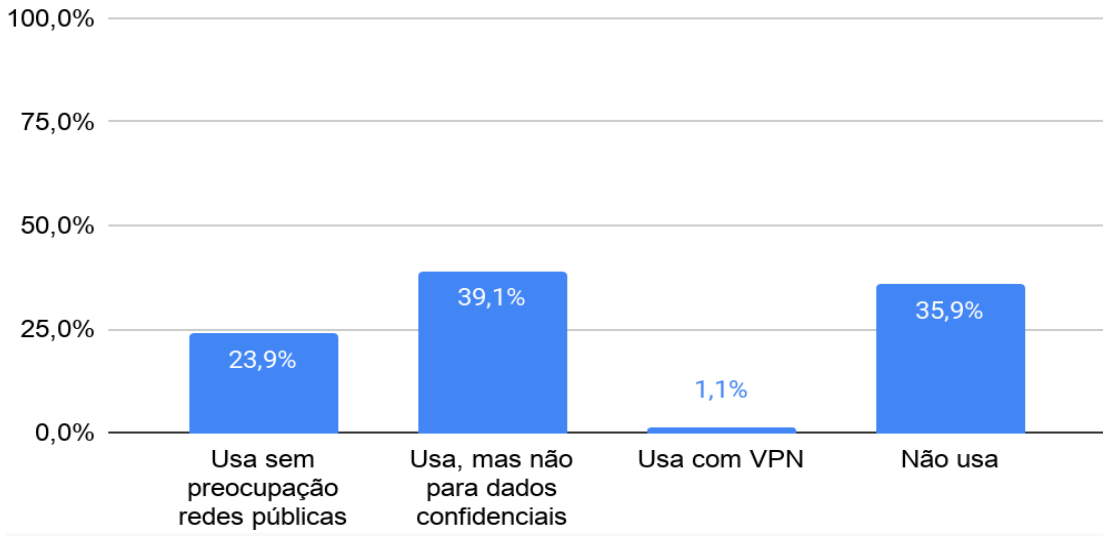
Ao serem questionados sobre quais dados acham viáveis para uma empresa comercializar (Figura 7), as duas alternativas mais votadas foram "Informações do meu perfil, como sexo e idade" (69,6%) e "De páginas/perfis que eu gosto como empresas e figuras públicas" (70%), tópicos estes com considerável possibilidade para análise algorítmica de gostos e hábitos do usuário, direcionado conteúdos relacionados a seu

Figura 7. Resultados da pergunta "Sobre redes sociais, quais dos dados pessoais você acha que é aceitável para a empresa usar para lucrar?".



Fonte: Resultado da pesquisa

Figura 8. Resultados das ações dos usuários sobre o uso de Wi-Fi pública.



Fonte: Resultado da pesquisa

perfil.

Finalmente, questionou-se sobre o uso de Wi-Fi público, visto que esse recurso deixa os dados contidos no aparelho em estado de vulnerabilidade. Pode-se conferir o resultado na Figura 8.

6. Conclusão

Os achados do trabalho sugerem um alto grau de importância aos dados coletados e capturados a partir dos *smartphones* e que a falta de conhecimento e a indiferença dos usuários em relação a seus dados é uma grande vantagem para quem lucra com eles. Foram apresentados os principais dados acessíveis a partir dos *smartphones*, e como terceiros os utilizam. Discutiu-se sobre a segurança no âmbito *mobile*, sendo citados diversos exemplos de dados produzidos

pelos *smartphones* e o destino que cada um deles pode ter.

Muitos se sentem incapazes e acham que nada pode ser feito para evitar essa situação de captura massiva de dados, entretanto, a avaliação de uma permissão ou um cuidado com redes Wi-Fi públicas são atitudes simples que podem evitar problemas de vazamento de dados a partir dos *smartphones*.

Mostrou-se ainda que as atuais políticas de privacidade adotadas pelos desenvolvedores de aplicativos não são tão claras como deveriam ser e, principalmente, não são sinceras quanto aos dados que capturam e compartilham. Por outro lado, os usuários não se sentem dispostos a se inteirarem de tais políticas, e o fato de não existir uma legislação mundialmente unificada causa prejuízo aos desenvolvedores, que, pelo menos na teoria, tinham que conhecer a legislação concernente de todas as nações as quais seus aplicativos são distribuídos, e também causa problemas aos usuários, devido a extrema dificuldade de recorrer à justiça contra uma empresa regida por leis diferentes das suas.

É surpreendente a variedade de tipos de dados que podem ser capturados, desde dados pessoais até dados do hardware do aparelho. Dados sobre os aplicativos instalados no *smartphone* também podem falar muito sobre o usuário daquele aparelho. Com isso, entende-se que usuários de *smartphones* são constantemente ameaçados com violações de privacidade.

Plataformas, sistemas operacionais e as próprias fabricantes de *smartphones* desempenham papel fundamental para a preservação da privacidade e no desenvolvimento de normas e regras para a captura de dados. Estudos sobre os dois sistemas operacionais mais conhecidos, Android e IOS, e suas respectivas empresas, Google e Apple, constataram que a segunda, no geral, se preocupa mais com a privacidade de seus usuários, sendo mais rígida, controladora e punitiva em relação à captura e manipulação de dados. Já Google mostra-se menos dispostas em relação a essa questão, embora também tenham políticas versando sobre privacidade. Essas empresas possuem uma forte influência no comportamento dos aplicativos e podem auxiliar consideravelmente na preservação da privacidade dos usuários.

Mostrou-se também que um certo grau de mercantilização dos dados é inevitável, visto que eles são uma fonte promissora de lucro para muitas empresas que teriam dificuldades de se manter no mercado de outra forma. Além do que a análise de dados ajuda a melhorar cada vez mais o serviço dos aplicativos, tão úteis à sociedade. Logo, seria preciso encontrar um meio termo, onde a captura não seja ofensiva à privacidade, mas que alguns dados possam ser divulgados para tais empresas.

Em relação a pesquisas futuras, recomenda-se análises com um maior grau de detalhes das consequências dessa captura excessiva de dados, seja no cenário individual, numa perspectiva do usuário, ou no cenário coletivo, com consequências para empresas e até mesmo países. Além disso, ainda é cedo para que se consiga mensurar as consequências da LGPD sobre a difusão involuntária de dados pessoais pela utilização de *smartphones*.

Finalmente, cabe citar as limitações para o desenvolvimento deste trabalho. A base de dados Scopus foi a única utilizada, devido à significativa quantidade de artigos encontrados sobre o tema, o que também limitou a pesquisa ao período entre 2017 e 2020.

Referências

Adams, P. (2020). Agreeing to surveillance: digital news privacy policies. *Journalism, & Mass Communication Quarterly*, 97(4), 868-889.

Atkinson, J. S., Rio, M., Mitchell, J. E., & Matich, G., (2018). Your Wi-Fi is leaking: what do your mobile apps gossip about you? *Future Generation Computer Systems*, 80, 546-557.

Baalous, R. Poet, R., & Storer, T. (2018). Analyzing Privacy Policies of Zero Knowledge Cloud Storage Applications on Mobile Devices. In *IC2E: IEEE International Conference on Cloud Engineering*, pp. 218-224.

Baalous, R., Poet, R. (2018). How Dangerous Permissions are Described in Android Apps' Privacy Policies? *SIN 18 - 11th International Conference on Security of Information and Networks*, pp. 1-2.

Balebako, R., Marsh, A., Lin, J., Hong, J. I., & Cranor, L. F. (2014). The privacy and security behaviors of smartphone app developers. *USEC: Workshop on Usable Security*. DOI: 10.14722/usec.2014.23006

Baraniuk, C.: Phone sensors can save lives by revealing what floor you are on (2018). *New Scientist*. https://www.newscientist.com/article/2152366-phone-sensors-can-save-lives-byrevealing-what-floor-you-are-on

Barnes. S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*. DOI:

https://doi.org/10.5210/fm.v11i9.1394

Beaumont, R. (2013). City of London Smartphone Tracking Bins. CookieLaw Blog. https://www.cookielaw.org/blog/city-of-london-*smartphone*-tracking-bins

Binns, R., Lyngs, U., Kleek, M. V., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. *10th ACM Conference on Web Science*.

Biolchini, J., Mian, P. G., Natali, A. C., & Travassos, G. H. (2005). *Systematic review in software engineering*. Technical Report – ES 679/05. System Engineering and Computer Science Department COPPE/UFRJ. Rio de Janeiro: COPPE/UFRJ.

Book, T., Pridgen, A., & Dan, S.W. (2013). Longitudinal analysis of android ad library permissions. *MoST: Mobile Security Technologies*. https://arxiv.org/pdf/1303.0857.pdf

Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2018). Losing control to data-hungry apps: a mixed-methods approach to mobile app privacy. *Social Science Computer Review*, 37(4), 466-488.

Brasil (2018). Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2019). A survey on smartphone user's security choices, awareness and education. *Computers, & Security*, 88(101647).

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, 80(4), 571-583.

Brückner, S., Sato, Y., Kurabayashi, S., & Waragai, I. (2018). The Handling of Personal Information in Mobile Games. In: Cheok, A., Inami, M., & Romão T. (eds) *Advances in Computer Entertainment Technology*. ACE 2017. LNCS, v. 10714. Springer,

Chen, S., Zhao, S., Han, B., & Wang, X. (2019). Investigating and revealing privacy leaks in mobile application traffic. *WD: IFIP Wireless Days*. DOI: 10.1109/WD.2019.8734246

Corones, S. & Davis, J. (2017). Protecting consumer privacy and data security: regulatory challenges and potential future directions. *Federal Law Review*, 45(1), 65-95.

Dai, W., Qiu, M., Qiu, L, Chen, L., & Wu, A. (2017). Who moved my data? Privacy protection in smartphones. *IEEE Communications Magazine*, 55(1), 20-25.

Dykes, B. (2013). Web analytics vs. mobile analytics: What's the difference? *Analytics Hero*. http://www.analyticshero.com/2013/07/24/web-analytics-vs-mobile-analytics-whats-the-difference

Elahi, H., Wang, G., & Chen, J. (2020). Pleasure or pain? An evaluation of the costs and utilities of bloatware applications in Android smartphones. *Journal of Network and Computer Applications*, 157.

Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S. (2011). A study of Android application security, *SEC'11: 20th USENIX Conference Security*.

European Commission (2018). *Antitrust: commission fines google Euros 4.34 billion for illegal practices regarding android mobile devices to strengthen dominance of google's search engine*. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581

Farnden, J., Martini, B., & Choo, K.-K. R. (2015). Privacy Risks in Mobile Dating Apps. *21st Americas Conference on Information Systems*. https://arxiv.org/ftp/arxiv/papers/1505/1505.02906.pdf

Federal Trade Commission (2014). *Data brokers: a call for transparency and accountability*, EUA: FTC. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: user attention, comprehension, and behavior. *SOUPS: ACM Symposium on Usable Privacy and Security*.

Fong, A. (2017). The role of app intermediaries in protecting data privacy. *International Journal of Law and Information Technology*. 25(2), 85-114.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226-261. DOI: 10.1016/j.cose.2018.04.002.

Gillespie, T. (2015). Platforms intervene. *Social Media+Society*. DOI: 10.1177/2056305115580479.

Goel, V. (2016). Beware, iPhone users: fake retail apps are surging before holidays. *New York Times* http://www.nytimes.com/2016/11/07/technology/more-iphone-fake-retailapps-before-holidays.html?_r.0

Greene, D. & Shilton, K. (2018). Platform privacies: governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media, & Society*, 20(4), 1640-1657.

Gubernatorov, A. M., Teslenko, I. B., Muravyova, N. V., Vinogradov, D. V., & Subbotina, N. O. (2020). Information security of mobile systems. *Lecture Notes in Networks and Systems*, 73, 677-686.

He, Y., Hu, B., & Han, Z. (2018). Dynamic privacy leakage analysis of android third-party libraries, *ICDIS: 1st International Conference on Data Intelligence and Security*. DOI: 10.1109/ICDIS.2018.00051

Hern, A. (2015). Apple pulls 250 privacy-infringing from App Store. *The Guardian*. https://www.theguardian.com/technology/2015/oct/20/apple-pulls-250-privacy-infringing-apps-from-store

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human Computer Studies*, 143(102498).

Holzer, A. & Ondrus, J. (2011). Mobile application market: a developer's perspective. *Telematics and Informatics*, 28(1): 22-

31.

Horvitz E. & Mulligan, D. (2015). Data, privacy, and the greater good, *Science*, 349, 253-255. DOI: 10.1126/science.aac4520.

Jayakumar, P., Lawrence, L., Chean, R. L. W., & Brohi, S. N. (2019). A review and survey on *Smartphones*: the closest enemy to privacy. *Lecture Notes of the Institute for Computer Sciences, social-Informatics and Telecommunications Engineering*, LNICST, v. 285, pp. 106-118.

Jensen, J., Hu, J., Rahmati, A., & Likamwa, R. (2019). Protecting visual information in augmented reality from malicious application developers. *WearSys '19: The 5th ACM Workshop on Wearable Systems and Applications*, pp. 23-28.

Kandil, S., Akker, M., van Baarsen, K., Jansen, S., & Vulpen, P. (2018). Benchmarking privacy policies in the mobile application ecosystem. *ICSOB: 9th International Conferenceon Software Business*, pp. 43-55. Lecture Notes in Business Information Processing, v. 336.

Karnal, L. (2016). A servidão voluntária. Video. https://www.youtube.com/watch?v=shUKfvyo4NE&list=PLyvMMekyJGJa7REFbVMd3RbYhzaOrdHzG&index=28

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. In: *Financial Cryptography and Data Security*, LNCS 7398, pp. 68-79.

Kitchenham, B. A., Dybå, T., Jørgensen, M. (2004). Evidence-based software engineering. *ICSE: 26th International Conference on Software Engineering*, p. 273-281.

Kitchenham, B. A. & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering – version 2.3*. EBSE Technical Report EBSE-2007-01. Software Engineering Group School of Computer Science and Mathematics (Keele University) / Department of Computer Science (University of Durham), Reino Unido.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Technical Report TR/SE-0401, 33, 1-26.

Kul, G., Upadhyaya, S., & Chandola, V. (2018). Detecting data leakage from databases on Android apps with Concept Drift. *TrustCom/BigDataSE: 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Big Data Science and Engineering*, pp. 905-913.

Kusyanti, A. & Catherina, H. P. A. (2018). An empirical study of app permissions: a user protection motivation behaviour. *International Journal of Advanced Computer Science and Applications*. 9(11), 106-111.

La Boétie, E. de (1987). *Discurso da servidão voluntária*, São Paulo, Escuta.

Lai, S. S. & Flensburg, S. (2020). A proxy for privacy uncovering the surveillance ecology of mobile apps. *Big Data, & Society*, 7(2).

Lang, M., Wiesche, M., & Krcmar, H. (2018). Perceived control and privacy in a professional cloud environment, *Hawaii International Conference on System Sciences*. DOI: 10.24251/HICSS.2018.464

Lipman, R. (2016). Online Privacy and the Invisible Market for our Data. *120 Penn State Law Review* 777.

Liu, X., Liu, J., Zhu, S., Wang, W., & Zhang, X. (2019). Privacy risk analysis and mitigation of analytics libraries in the Android ecosystem. *IEEE Transactions on Mobile Computing*. 19(5), 1184-1199.

Mafra, S. N.; Travassos, G. H. (2006). *Estudos primários e secundários apoiando a busca por evidência em engenharia de software*. Relatório Técnico - ES 687/06, Universidade Federal do Rio de Janeiro (COPPE/UFRJ).

Martin, K. E. (2013). Transaction costs, privacy, and trust: the laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*, 18(12). http://firstmonday.org/ojs/index.php/fm/article/view/4838

Noor, T., Sheng, Q., Yao, L., Dustdar, S., & Ngu, A. (2016). CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services, *IEEE Transactions on Parallel and Distributed Systems*, 27(2), 367-380.

Office of the Privacy Commissioner of Canada (2014). *Privacy Enforcement Network Joint Open Letter to App Marketplaces*. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/let_141210

Osho, O., Mohammed, U. L., Nimzing, N. N., Uduimoh, A. A., & Misra, S. (2019). Forensic analysis of mobile banking apps. In: *ICCSA 2019: Computational Science and Its Applications*. LNCS, v. 11623, pp. 613-626.

Pal, R. & Crowcroft, J. (2019). Privacy trading in the surveillance capitalism age viewpoints on 'privacy-preserving' societal value creation. *Computer Communication Review*. 49(3), 26-31.

Parlamento Europeu (2016). *Regulamento Geral sobre a Proteção de Dados*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

Patrick Wendy L. (2017). The open book: what your reading choices say about you. *Psychology Today*. https://www.psychologytoday.com/us/blog/why-bad-looks-good/201712/the-open-book-what-your-reading-choices-say-about-you

Polykalas, S. E. & Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance*, 21(2), 89-101.

Presthus, W. & Vatne, D. M. (2019). A survey on Facebook users and information privacy. *Procedia Computer Science*, 164, pp. 39-47.

Ruiz, M. (2018). Os dados são o novo petróleo. [Entrevista concedida a] Rodrigo Loureiro. *Isto É*, n. 1060, 9 mar. 2018.

Sanders, C., Shah, A., Zhang, S., 2015. Comprehensive analysis of the android Google play's auto-update policy. *ISPEC 2015: Information Security Practice and Experience*, Lecture Notes in Computer Science, 9065. Springer-Verlag, pp. 365-377.

Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2012). Android permissions: a perspective combining risks and benefits. *Symposium on Access Control Models and Technologies*, pp. 13-22.

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2020). All of me? Users' preferences for privacy-preserving data markets and

the importance of anonymity. *Electronic Markets*, 30(6221). DOI: 10.1007/s12525-020-00404-9

Shozi, N. A., Mtsweni, J. (2017). Big data privacy in social media sites. *IST-Africa Week Conference*.

Singh, I., Saini, S., & Bathla, R. (2019). Consumer privacy concerns over free cloud services. *ISCON: 4th International Conference on Information Systems and Computer Networks*, pp. 46-50.

Singh, R., Sumeeth, M., & Miller, J. (2011). Evaluating the Readability of Privacy Policies in Mobile Environments, *International Journal of Mobile Human Computer Interaction*, 3(1), 55-78.

Spencer G (2016) Developers: apple's app review needs big improvements. *MacStories*. https://www.macstories.net/stories/developers-apples-app-review-needs-big-improvements

Spensky, C., Stewart, J., Yerukhimovich, A., Shay, R., Trachtenberg, A., Housley, R., Cunningham, R. K., SoK: Privacy on mobile devices - It's complicated. *Privacy Enhancing Technologies* 2016(2), 96-116,

Stack Overflow (2020). 2020 Developer Survey. https://insights.stackoverflow.com/survey/2020

Stevens, R., Gibler. C., & Crussell, J., Erickson, J., & Chen, H. (2012). Investigating user privacy in android ad libraries. *MoST: Mobile Security Technologies*. https://web.cs.ucdavis.edu/~hchen/paper/most2012ad.pdf

Story, P., Zimmeck, S., & Sadeh, N. (2018). Which apps have privacy policies? An analysis of over one million google play store apps. In: *APF 2018: Privacy Technologies and Policy*, pp. 3-23.

Tramontana, E. & Verga, G. (2019). Mitigating privacy-related risks for Android users. *WETICE: IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 243-248.

Vallina-Rodriguez, N. (2018). 7 in 10 smartphone apps share your data with third-party services. Scientific American. https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services

Wei, X., Gomez, L., Neamtiu, I., Faloutsos, M., (2012). Permission evolution in the Android ecosystem. *ACSAC: 28th Annual Computer Security Applications Conference*, pp. 31-40.

Welch, C. Android apps are now reviewed by google before you can download Them .*The Verge*http://www.theverge.com/2015/3/17/8231125/android-apps-now-reviewedby-google

Wong, S. & Zhu, G. (2016). *Personal data (privacy) law in Hong Kong: a practical guide on compliance*, Office of the Privacy Commissioner for Personal Data / THE Cicy University of Hong Kong Press.

Yu, F., Xuming, L., Xiao, G., Lin, L., & Jingzhao, L. (2020). A survey on key technologies of privacy leakage detection for Android platform. *ISBDAS - 2nd International Symposium on Big Data and Applied Statistics*, Dalian, China. DOI: 10.1088/1742-6596/1437/1/012006

Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*. https://techscience.org/a/2015103001

Sobre os autores

Adriano Vieira da Silva
Bacharel em Ciência da Computação pela Universidade Católica de Brasília (2020).

Paulo Victor Guimarães Rosa
Bacharel em Ciência da Computação pela Universidade Católica de Brasília (2020).

Edilson Ferneda
Graduado em Tecnologia de Computação pelo Instituto Tecnológica de Aeronáutica (1979), Mestre em Sistemas e Computação pela Universidade Federal da Paraíba (1988) e Doutor em Ciência da Computação pelo *Laboratoire d'Informatique, Robotique et de Microélectronique de Montpellier* – LIRMM/CNRS, França (1992). Entre 1986 e 2000, foi professor do Departamento de Sistemas e Computação da UFPB (atual Universidade Federal de Campina Grande - UFCG), tendo atuado nos cursos de Bacharelado em Ciência da Computação, Mestrado em Informática e Doutorado em Engenharia Elétrica. Desde 2001 é professor titular da Universidade Católica de Brasília, onde atua nos Cursos de Bacharelado em Ciência da Computação e em Administração e no Mestrado em Gestão, Tecnologia e Inovação (antigo Mestrado em Gestão do Conhecimento e Tecnologia da Informação). Seus interesses incluem Inteligência Artificial e Gestão do Conhecimento.

Mário de Oliveira Braga Filho
Graduado em Tecnologia da Construção Civil pela Universidade para o Desenvolvimento do Estado e Região do Pantanal (1990), Especialista em Análise de Sistemas na Universidade Federal de Mato Grosso do Sul (1994) e Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília (2008), desde 2003 é professor da Universidade Católica de Brasília, atuando no curso de Bacharelado em Ciência da Computação.