UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

Catálogo de critérios para avaliação de políticas de privacidade

---

Trabalho de Graduação

Aluno: Augusto Henriques Terra

Orientadora: Jéssyka Flavyanne Ferreira Vilela

Co-orientadora: Mariana Maia Peixoto

Recife
2021

Universidade Federal de Pernambuco

Centro de Informática

Augusto Henriques Terra

Catálogo de critérios para avaliação de políticas de privacidade

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Orientadora: Jéssyka Flavyanne Ferreira Vilela

Recife
2021

RESUMO

Contexto: Notícias constantes de vazamentos de dados pessoais têm levantado o questionamento em usuários de aplicativos e websites sobre quão seguras suas informações estão sob o domínio das empresas responsáveis. Nesse contexto, o cenário é tão preocupante ao ponto de vários governos ao redor do mundo adotarem medidas para que empresas e organizações aumentem o investimento em ações que protejam as informações dos usuários. Dessa forma, diversas leis de proteção de dados pessoais têm surgido em várias regiões a fim de proteger, regulamentar e garantir a privacidade dos cidadãos, como a Regulamentação Geral de Proteção de Dados (do inglês, *General Data Protection Regulation* - GDPR) em países pertencentes à União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. Políticas de Privacidade são os documentos que as empresas e companhias elaboram com o intuito de alertar os usuários das plataformas sobre uma série de informações a respeito de como tratam seus dados pessoais. Entretanto, pesquisas anteriores mostraram que as Políticas de Privacidade são documentos longos, difíceis de serem lidos e nem sempre estão de acordo com a lei vigente ou mesmo refletem a real prática de coleta e manutenção de dados da organização. Isto é um problema pois a Política de Privacidade da organização é a principal fonte do usuário para saber como a empresa trata seus dados pessoais, além disso, a penalização que o governo impõe para empresas que violem a lei de proteção de dados pode chegar a multas milionárias. Sendo assim, é válido estudar e analisar políticas de privacidade para que se tenha uma base sólida sobre quais métricas elas devem ser avaliadas. Objetivo: Este trabalho propõe um catálogo de critérios para avaliação de Políticas de Privacidade. Método: Para atingir esse objetivo, foi realizada uma revisão sistemática da literatura, aplicando a técnica de bola de neve (do inglês, *snowballing*) para encontrar artigos relevantes da área, que fazem avaliação de políticas de privacidade e que expõem os critérios utilizados para fazer a análise. O estudo contempla resultados coletados a partir de 48 artigos diferentes que se relacionam diretamente com o tema. Baseado nos critérios de avaliação que esses artigos adotam e nos resultados encontrados pelos autores, foi elaborado o catálogo. Resultados: O catálogo proposto possui 29 critérios diferentes agrupados em 5 categorias que dizem respeito a: Acessibilidade da Política de Privacidade, Conteúdo do documento, Participação do usuário, Alterações no documento e Consentimento e Permissão do usuário. Conclusões: O catálogo desenvolvido pode ser utilizado como um guia para redatores de Políticas de Privacidade para escrever documentos mais completos e corretos, além de auxiliar analistas e responsáveis pela aplicação, deixando mais claro quais informações devem ser devidamente documentas sobre a prática de coleta de dados.

Palavras-chave: Privacidade, Políticas de privacidade, LGPD, GDPR, Dados pessoais, Catálogo, Proteção de dados, Critérios de avaliação.

ABSTRACT

Context: News of personal data leaks has raised questions in many app's and website's users about how secure the information is under the domain of those responsible companies.This scenario is so worrying that the government around the world takes measures for companies and organizations to increase incestment in actions that protect user's personal information. Thus, various personal data protection laws have emerged in various regions in order to protect, regulate and ensure the privacy of citizens, such as the General Data Protection Regulation (GDPR) in member countries of the European Union and the General Data Protection Law (from portuguese, Lei Geral de Proteção de Dados - LGPD) in Brazil. Privacy Policies are documents that companies prepare with the aim of alerting platform users to a series of information about how they treat their sensitive data. However, previous research has shown that the privacy policies are long documents, difficult to be read and do not Always comply with the current law or even reflect the actual data collection and maintenance practice of the organization.This is a problem because the organization's privacy policy is the user's main source to know how the company treats their personal data, in addition, the penalty that the fovernment imposes on companies that violate the data protection law can reach fines millionaires.Therefore, it is Worth studying and analyzing privacy policies so that you have a solid basis on which metrics they should be evaluated. Objective: This work proposes a catalog of criteria for evaluating privacy policies. Method: To achieve this objective, a systematic literature review was carried out, applying the snowballing technique to find relevant articles in the area, which assess privacy policies and expose the criteria used to carry out the analysis. The study considered 48 different articles that relate directly to the topic. Based on the evaluation criteria adopted by these articles and on the results found by the authors, the catalog was created. Results: The proposed catalog has 29 different criteria grouped into 5 categories that relate to: Accessibility of the Privacy Policy, Document content, User participation, Document changes and User consent and permission. Conclusions: The catalog carried out guides Privacy Policy writers to write more complete and correct documents, in addition to helping analysts and those responsible for the application, making it clearer which information must be properly documented about the practice of data collection.

Keywords: Privacy, Privacy Policy, LGPD, GDPR, Personal Data, Catalog, Data protection, Rating Criteria.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 Introdução

1.1 Contexto

A privacidade de dados pessoais dos usuários de aplicativos e websites tornou-se um ponto debatido e considerado importante após diversas notícias de vazamento de dados [1]. Por exemplo, em 2016, um vazamento de dados pessoais que ocorreu com o Uber[1], uma das maiores empresas de mobilidade urbana do planeta, expôs informações de mais de 50 milhões de usuários. Dentre as informações vazadas, encontram-se expostos endereços de e-mail, números de celular, dados de carteira de habilitação de motoristas e até endereços domésticos de seus usuários e colaboradores [7].

Outro acontecimento que tomou proporções nacionais, foi em janeiro de 2021, um mega vazamento de dados de cerca de 223 milhões de brasileiros [48]. Este número é maior do que a população do Brasil pois incluía também dados de pessoas falecidas. As informações que foram expostas incluem CPF, nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs. Os *hackers* responsáveis colocaram à venda na internet todas essas informações.

Grande parte dos sites e aplicações web coletam dados automaticamente à medida que as pessoas o utilizam [49]. Além disso, fazem uso de ferramentas de fácil acesso e implantação como o Google Analytics[2] e o Hotjar[3], permitindo monitorar a atividade de forma completa, gerando até mesmo gráficos comparativos por tipo de usuário e mapas de calor sobre qual funcionalidade da aplicação vem sendo mais utilizada [2].

O Marketing por Dados é uma tendência que vem ganhando cada dia mais força no mercado [3]. De acordo com este conceito, é possível tomar decisões mais concretas e assertivas a respeito de qual público-alvo deve ser atingido para determinado produto ou serviço a partir das informações armazenadas na base de dados. Grandes corporações, como a Amazon[4], investem fortemente nessa estratégia [50] de coletar, armazenar, processar e analisar as informações sobre clientes que navegam pelo site e redes sociais da empresa. Com essa enorme quantidade de dados a companhia busca aumentar a satisfação do cliente, antecipando produtos que tem grandes chances de serem comprados já deixando-os prontos na distribuidora, o que reduz o tempo de entrega. Outra estratégia adotada pela empresa é alterar os preços de seus produtos em um curto período de tempo, à medida que são coletados dados sobre a concorrência, demanda e disponibilidade de produtos, por exemplo [4].

Uma pesquisa conduzida pela CBS News[5] (CBS) e The New York[6] Times [5], mostrou que cerca de 82% dos entrevistados acreditam que o direito à privacidade está sob séria ameaça ou já está perdido. Além disso, os usuários da internet estão cada vez mais preocupados com empresas que coletam suas

[1] Uber: https://www.uber.com/
[2] Google Analytics: https://analytics.google.com
[3] Hotjar: https://www.hotjar.com/
[4] Amazon: https://www.**amazon**.com.br
[5] CBS News: https://www.cbsnews.com
[6] The New York Times: https://www.nytimes.com

informações pessoais e com os riscos dessas informações serem compartilhadas de forma inadequada [6].

Por conta dos diversos casos de vazamento de dados pessoais, usuários têm buscado compreender algumas questões antes de realmente começarem a utilizar certo produto ou serviço [8]:

- Como e onde as informações coletadas dos usuários são utilizadas?
- O que acontece com a informação coletada?
- As informações são compartilhadas com outros websites ou empresas?
- O website instala algum software no sistema do usuário?

Diante desses questionamentos e da necessidade de manter a privacidade dos usuários, surgiram algumas leis com o intuito de regulamentar a problemática do tratamento e proteção de informações pessoais. A Lei Geral de Proteção de Dados Pessoais nº 13.709/2018 (LGPD), sancionada em agosto de 2018 e que entrou em vigor em agosto de 2021, possui um conjunto de direitos e obrigações que tem como foco proteger a privacidade e a autonomia dos titulares de dados pessoais dos cidadãos brasileiros [51]. A LGPD regulamenta como as empresas devem lidar com o processamento de dados de seus clientes, atividades de coleta, armazenamento e eliminação de informações pessoais, determinando as bases legais de processamento de dados, o consentimento e a anonimização dos dados, entre outras atividades.

Entretanto, muitas empresas não estão prontas para tratar das novas diretivas determinadas pela LGPD [52], várias estão precisando reformular seus processos de extração de dados e regras de negócio para garantir a conformidade com a lei. Dessa forma, elas vão precisar explicitar o motivo para a coleta e o armazenamento de tais dados, quem possui acesso a eles e quando e onde esses dados serão utilizados. A punição para companhias que descumprirem a LGPD pode variar levando em conta a gravidade da infração. As multas podem chegar a 2% do faturamento total, além disso, as empresas podem ter suas atividades suspensas, parcial ou totalmente [17].

Organizações já vêm sendo multadas por descumprimento a leis de privacidade. Na França, a agência reguladora para a internet multou o Google em 100 milhões de euros [53] por não deixar claro como coleta dados de usuários para exibir propagandas personalizadas. A Comissão Nacional de Informática e Liberdades da França afirmou que o valor da multa foi um recorde, devido a gravidade das infrações e o impacto dos sites na população francesa. No Brasil, empresas também já estão sendo multadas por violação a LGPD. A Cyrela é uma companhia brasileira construtora e incorporadora de imóveis. Em novembro de 2018, a empresa foi punida por compartilhamento indevido de dados pessoais de clientes com parceiros comerciais [54], o que é ilegal segundo a LGPD. A Cyrela foi multada em uma indenização de R$10 mil aos clientes que tiveram seus dados partilhados e foi condenada a não repassar mais os dados pessoais ou financeiros de clientes, sob pena de multa de R$300,00 a cada contrato mal utilizado.

Portanto, a transparência no tratamento dos dados pessoais é fundamental para a conformidade com as leis de privacidade. A LGPD determina que o usuário tem direito a facilmente acessar as informações sobre como seus dados pessoais são tratados. Esses processos precisam estar disponíveis de

forma clara, direta e acessível, atendendo ao princípio do livre acesso. Essas informações devem ser descritas nas políticas de privacidade das empresas. Sendo assim, faz-se necessário investigar como essas políticas vêm sendo construídas e apresentadas aos usuários.

1.2 Motivação e justificativa

Uma política de privacidade pode ser definida como uma descrição abrangente das práticas de coleta de um site ou aplicativo [9]. A política deve descrever quais informações são coletadas, a finalidade dessa coleta e como os dados obtidos serão manipulados, armazenados e usados. Além disso, deve contemplar informações sobre se os clientes têm permissão para acessar as informações coletadas e para resolver disputas relacionadas à privacidade com o site.

Infelizmente, as políticas de privacidade atuais publicadas em sites e aplicativos são geralmente longas, complexas e difíceis para os usuários finais lerem e compreenderem [10]. Uma pesquisa realizada por Miller [11] mostrou que muitas políticas carecem de clareza e requerem uma habilidade de leitura consideravelmente maior do que o nível médio de alfabetização da população que diariamente utiliza a internet.

As políticas de privacidade têm um histórico de serem consideradas difíceis de serem compreendidas [12]. São documentos que abordam as obrigações legais de uma organização e divulgam suas práticas de privacidade e procedimentos no que se refere às interações dos usuários ao utilizar o site da organização. As obrigações legais da organização, ao invés da legibilidade do documento, tendem a ser a principal força motriz na construção do documento, o que, muitas vezes, resulta em documentos extremamente longos, confusos e que contêm uma sofisticação de termos e linguagem de orientação jurídica [35].

Para as políticas de privacidade serem realmente úteis, elas precisam ser compreendidas pelos usuários que visitam e utilizam a aplicação. Isso significa que o aviso de privacidade precisa ser escrito em um nível apropriado e deve ser fácil de navegar até a informação. Portanto, é necessário melhorar as políticas atuais para ajudar os usuários dos produtos e serviços a lerem, entenderem e assim aumentar a conscientização sobre a privacidade de seus dados [13].

A Organização para Cooperação e Desenvolvimento Econômico (OCDE) fornece um Gerador de Políticas de Privacidade como uma tentativa de ajudar organizações a produzir documentos de fácil compreensão. Entretanto, essas políticas geradas são muito superficiais e, muitas vezes, não explicitam o propósito e as informações relativas ao tratamento de dados.

De acordo com McDonald e Cranor [14], o tamanho médio de uma política de privacidade em um website popular é de 2514 palavras, resultando em uma leitura longa e entediante, o que faz com que muitos usuários simplesmente ignorem esse aviso [15] [16].

O site The New York Times publicou uma pesquisa [55] avaliando a política de privacidade de aproximadamente 150 websites e aplicativos populares. A política de privacidade do Facebook, por exemplo, levou cerca de 18 minutos para ser lida por completo. A pesquisa também avaliou quão difícil é

ler cada política utilizando a plataforma de avaliação de textos Lexile[7], mensurando a complexidade baseada em fatores como tamanho da sentença e dificuldade do vocabulário e atribuindo um score para cada documento, quanto mais alto, mais difícil de se ler. Para se formar na faculdade as pessoas precisam entender textos com um score de 1300, profissionais como médicos e advogados precisam entender materiais com um score de 1440. A pesquisa mostrou que muitas políticas de privacidade possuem um score acima dessa média.

Nesse contexto, é importante definir métricas a respeito das políticas de privacidade para avaliar as diversas dimensões envolvidas nesse documento legal. Assim, será possível auxiliar o trabalho tanto de projetistas de sistemas ao desenvolverem a aplicação, quanto o trabalho dos responsáveis por escrever a política, além de melhorar a experiência do usuário ao ler o documento.

1.3 Objetivos

Dado que a recente Lei Geral de Proteção de Dados Pessoais ocasionou grandes mudanças no cenário brasileiro de proteção de dados que, muitas vezes, é ignorado em várias empresas, esse trabalho busca investigar a avaliação de políticas de privacidade e a elaboração de políticas corretas e completas. Para atingir esse objetivo principal, é importante pontuar os seguintes objetivos específicos:

1. Investigar e estudar conceitos relacionados a privacidade, leis de privacidade, políticas de privacidade e métodos de avaliação de políticas de privacidade;
2. Realizar uma revisão sistemática da literatura a fim de encontrar artigos que avaliam políticas de privacidade;
3. Elaborar um catálogo com um conjunto de critérios de avaliação de políticas de privacidade.

1.4 Trabalhos Relacionados

Este trabalho tem como objetivo a elaboração de um catálogo com um conjunto de critérios para avaliação de políticas de privacidade. Dado a natureza deste trabalho, não foram encontrados trabalhos com o mesmo propósito, sendo assim, nesta seção discute-se (i) trabalhos relacionados a avaliação de políticas de privacidade; e, (ii) trabalhos que propõem catálogos nas mais diversas áreas.

1.4.1 Avaliação de políticas de privacidade

Políticas de privacidade têm sido o foco de muitas pesquisas nos últimos anos [18, 19, 20, 21]. Alguns estudos têm como foco analisar políticas de privacidade de vários sites diferentes de uma forma abrangente e outros focam em aspectos como: de que forma os dados são coletados, como os dados são

[7] Lexile: https://lexile.com

armazenados, como esses dados são utilizados pela aplicação, se há o compartilhamento das informações entre aplicações externas e como ocorre essa interação.

Inicialmente, Graber [18] em 2002 verificou que muitos indivíduos gostariam de manter sua privacidade em questões relacionadas à saúde e informações médicas na internet. Foi investigado que alguns sites coletam e armazenam dados dos usuários. As informações rastreadas incluíam termos digitados em motores de busca, bens ou serviços comprados online e participação em fóruns, chats e listas de e-mail. Essa informação pode ser vendida para anunciantes para fazer propaganda daquilo que o usuário busca. Por exemplo, um indivíduo que visita um site dedicado ao tratamento de diabetes mellitus irá receber publicidade sobre novos medicamentos recomendados para quem tem diabetes. Entretanto, essas informações médicas podem e estão sendo utilizadas de outras maneiras [57], como um candidato a uma vaga que não é contratado pois a empresa identificou que ele sofre de uma doença terminal, por exemplo. Graber [18] então conduziu uma pesquisa que avaliou 80 sites e aplicações de língua inglesa relacionados à saúde, incluindo os 25 sites mais bem avaliados nesse tema na época. Foi comparado o nível de legibilidade dessas políticas de privacidade utilizando alguns métodos conhecidos no meio acadêmico, incluindo o método de Flesch, de Fry e SMOG. Os resultados obtidos mostraram que dos 80 sites avaliados, 30% não tinham nenhuma política de privacidade exposta. A média de legibilidade das políticas dos sites restantes requeria ao menos dois anos de estudo superior para serem compreendidos e nenhum site tinha uma política de privacidade que fosse compreendida pela maioria dos falantes da língua inglesa.

Lewis [19] no ano de 2008 realizou uma pesquisa semelhante, mas focou a análise em sites que se relacionavam com a indústria financeira, estudando as políticas de privacidade de cerca de 75 companhias online diferentes. Os documentos selecionados para serem analisados pertenciam a empresas que possuíam um porte parecido, com um número semelhante de bancos, de empresas de aconselhamento de crédito e de empresas de desconto de cheques. O objetivo de Lewis foi analisar a legibilidade das políticas de privacidade utilizando o método de Flesch. A conclusão desse estudo mostrou que as políticas de privacidade desse grupo não eram facilmente compreendidas pela maioria dos usuários que utilizavam a plataforma e não eram consideradas boas medidas para informar aos usuários sobre os direitos de privacidade.

Krumay [20] em 2020 analisou políticas de privacidade das 15 maiores empresas listadas na revista Forbes. Foi realizado primeiramente um estudo qualitativo, aplicando métodos para mensurar a legibilidade de cada política. Foram escolhidas sete escalas diferentes: *Dale-Chall Index*, *Automated Readability Index Gunning Fog Index, SMOG, Fry Graph Readability Formula, Flesch-Kincaid Grade Level* e *Coleman-Liau Index*. Em seguida, foi conduzido um estudo quantitativo medindo a quantidade de palavras, quantidade de sentenças, média do tamanho de cada sentença, média de sílabas por palavra e média de caracteres por palavras. Por último, foram expostas essas políticas de privacidade para quinze pessoas de diferentes níveis de ensino. Krumay mostrou nos resultados que as abordagens para medir legibilidade podem ser aplicadas a políticas de privacidade, uma vez que coincidiu o texto que fez a maior pontuação na análise qualitativa e quantitativa (o mais difícil de ler) com o

que as pessoas consideraram mais desafiador para ser lido. Entretanto, são necessárias regras adicionais, visto que os resultados dos níveis de legibilidade não mostram explicitamente o que deve ser mudado.

Zeadally e Winkler [21] também fazem uma análise da legibilidade de políticas de privacidade em 2016, porém focando seu estudo em plataformas de mídias sociais. Foram comparadas as políticas dos gigantes da tecnologia: Facebook[8], Twitter[9], Google[10] e Linkedin[11]. Verificou-se que todas essas plataformas estudadas coletam dados do usuário incluindo localização, endereço de IP, e-mail, nome, data de nascimento, modelo do dispositivo que está sendo usado e o sistema operacional. Zeadally e Winkler identificaram que a plataforma que capta a maior quantidade de dados é o Facebook, inclusive toda informação que o usuário publique ou acesse no site, informações de pagamentos, como cartões de créditos do usuário cadastrado e se entende para coletar informações sobre o uso geral da internet. Para avaliar a qualidade das políticas de privacidade foi utilizado o nível de legibilidade de Flesch-Kincaid que mensura a dificuldade de compreensão durante a leitura de um texto em inglês acadêmico contemporâneo. Os resultados dos níveis de legibilidade foram: 12.8 para o Twitter, 11.9 para o Facebook, 11.3 para o Linkedin e 13.5 para o Google. Esses níveis correspondem aos níveis da série escolar. Quanto maior o resultado, mais difícil de se compreender o texto. Para que a maioria dos usuários dessas redes sociais pudessem compreender os documentos de privacidade, esse valor deveria ser no máximo 8, visto que atualmente, nos Estados Unidos, 50% das pessoas não conseguem entender literaturas de nível de oitava série. Isso é ainda mais grave uma vez que essas redes sociais permitem a criação de contas de crianças a partir dos 13 anos.

Na Tabela 1, é apresentada uma comparação entre os estudos mencionados.

Tabela 1 – Comparação entre os trabalhos relacionados.

Critério:	**Graber, 2002**	**Lewis, 2008**	**Krumay, 2020**	**Zeadally e Winkler, 2016**
Quantidade de políticas avaliadas	80	75	15	4
Domínio dos sites	Sites e aplicativos relacionados a saúde e estilo de vida fitness.	Sites de companhias relacionadas à indústria financeira. As políticas de privacidade selecionadas eram compostas por um número	Sites das maiores empresas listadas na Revista Forbes. Todos os sites foram avaliados na primavera de 2019.	As plataformas web populares na época.

[8] Facebook: https://facebook.com
[9] Twitter: www.twitter.com.br
[10] Google: https://www.google.com.br
[11] Linkedin: https://br.linkedin.com

		igual de bancos, empresas de aconselhamento de crédito e empresas de desconto de cheques.		
Sites avaliados	Os 25 principais sites do domínio escolhido.60% eram sites comerciais (.com), 17,5% eram organizações (.org), 8,8% eram do Reino Unido (.uk), 3,8% eram governamentais dos Estados Unidos (.gov) e 2,5% eam educacionais (.edu)	Não mencionado	Allianz, Axa Group, Banco Santander, BMW Group, BNP Paribas, Daimler, Gazprom, HSBC Holding, ING Group, Nestle, Sberbank, Shell, Siemens, Total, Volkswagen	Google, LinkedIn, Twitter e Facebook.
Porte das empresas avaliadas	Grandes	Pequenas, médias e grandes	Grandes	Grandes
Lei de privacidade vigente	Não é mencionado.	Não é mencionado.	GDPR	Depende do país e região que o usuário que utiliza a plataforma pertence.
País que a política se refere	Reino Unido e Estados Unidos	Estados Unidos	Países membros da União Europeia	Estados Unidos
Ano do trabalho	2002	2008	2020	2016
Critérios principais para avaliação	Níveis de legibilidade de Flesch, de Fry e SMOG.	Níveis de legibilidade de Flesch-Kincaid. Medindo a média de palavras por frase e média de sílabas por palavra.	Foram utilizados sete critérios de análise de texto diferentes: Dale-Chall Index, Automated Readability Index Gunning Fog Index Readability Formula, SMOG Grading, Fry Graph	Foi utilizado o nível de legibilidade de Flesch-Kincaid, porém a comparação de políticas de privacidade é mais focada em quais informações estão incluídas ou excluídas e

			Readability Formula, Flesch-Kincaid Grade Level, Coleman-Liau Index. Foram também realizadas pesquisas qualitativas e comparadas com o resultado das análises de textos.	as seções que as plataformas oferecem, ao invés de focar puramente no usuário
Resultados	Dos 80 sites que foram analisados, 30% (incluindo 23% dos sites comerciais) não tinham nenhuma política de privacidade exposta. A média do nível de legibilidade dos sites restantes exigia 2 anos de educação de nível universitário para serem compreendidos. Nenhum site tinha uma política de privacidade que fosse abrangente e acessível o suficiente para maioria dos indivíduos que falam inglês nos Estados Unidos.	As políticas de privacidade desses grupos não eram facilmente compreendidas pela maioria dos usuários e não puderam ser consideradas uma boa medida para informar o usuário sobre seus direitos de privacidade.	A maioria das políticas avaliadas não atendeu ao limite mínimo que as técnicas de análise de texto propuseram. Parâmetros como organização de parágrafos, prevenção de disseminação de informações redundantes no texto, bem como destacar informações importantes foram encontrados na maioria dos documentos. O mesmo se aplica à estrutura e design.	As políticas de privacidade do Facebook, Google, Linkedin e Twitter foram classificadas como tendo um nível de leitura acima do oitavo grau. Os níveis de leitura resultantes de cada política de privacidade depois de usar o método de Flesch-Kincaid foram: 12.8 para o Twitter, 11.9 para o Facebook, 11.3 para o Linkedin e 13.5 para o Google. Esses níveis correspondem com o nível escolar. Quanto maior o número, mais difícil é para o indivíduo compreender. Para que a maioria dos usuários compreenda, essas notas deveriam ser de 8 ou menos.

A partir da comparação dos trabalhos relacionados da Tabela 1, concluiu-se que existe na literatura uma série de artigos que realizaram avaliações de políticas de privacidade. Alguns focam em análise quantitativa [18], medindo o

número de palavras, de sentenças, quantidade média de sílabas que o documento possui e obtém suas conclusões a partir desses dados.

Outros trabalhos [19, 21] utilizam métodos já conhecidos no meio acadêmico para quantificar o nível de legibilidade das políticas avaliadas e comparar se estão de acordo com o nível de leitura que os usuários que utilizam a plataforma conseguem compreender. Existem ainda pesquisas [20] que fazem uma abordagem mais subjetiva, entrevistando usuários e pedindo que classifiquem as políticas de privacidade da mais fácil a mais difícil e comparando com os resultados dos níveis de legibilidade. Um ponto importante de se observar é que a maioria dos artigos escolhe um subconjunto particular de sites para avaliar a política que abordem temas parecidos e pertençam a mesma área. Por fim, é válido destacar que grande parte das políticas de privacidade analisadas nesses estudos, independentemente do método de análise empregado, não apresentavam uma boa legibilidade e não eram uma boa referência para os usuários conhecerem seus direitos relacionados à privacidade de seus dados pessoais.

1.4.2 Construção de catálogos

Um catálogo é definido como uma coleção organizada ou classificada de objeto ou informação que possa ser agrupada [58]. Os catálogos são importantes, pois por meio deles é possível apresentar com clareza, fidelidade e objetividade os pontos a serem defendidos [59]. Por conta disso, o catálogo é frequentemente utilizado na metodologia científica, para apresentar de forma sucinta e direta os resultados de uma pesquisa. Vários trabalhos anteriores [60, 61, 62, 85] tiveram como proposta a construção de catálogos nas mais diversas áreas como, por exemplo, privacidade, aplicações de blockchain, métricas de manutenção de software orientado a objetos e correlações de requisitos não-funcionais (do inglês, *Non-Functional Requirements* - NFRs).

Peixoto, Silva e Maia [60] apresentaram em seu estudo um catálogo de conceitos relacionados à privacidade. Os autores trouxeram a discussão de que a comunidade de Engenharia de Requisitos tem reconhecido a necessidade de abordar questões a respeito da privacidade dos usuários desde as primeiras fases do processo de desenvolvimento do software. Entretanto, ainda é obscuro para os desenvolvedores quais aspectos relacionados à privacidade eles devem considerar no momento de construção da aplicação. Sendo assim, os autores realizaram uma revisão sistemática da literatura para construir um catálogo de conceitos relacionados à privacidade. Primeiramente, foi extraído dos documentos conceitos específicos que se relacionam com a privacidade. Em seguida os conceitos correlacionados foram agrupados em categorias mais gerais. Depois, foi observado quais são as relações entre as categorias e então foi criada a relação entre categorias. O catálogo consiste em uma tabela com duas colunas. A primeira coluna contém os conceitos de privacidade agrupados por categorias gerais e a segunda coluna apresenta as definições destes conceitos.

Outros autores que desenvolveram trabalhos que fizeram a construção de catálogos foram Precht, Wunderlich e Gómez [61]. Dado o crescimento do mercado mundial de blockchain e o surgimento de novas aplicações com diferentes funcionalidades e algoritmos internos diversos, ficou cada vez mais

difícil identificar o sistema blockchain correto para determinada aplicação. Sendo assim, os autores desenvolveram um catálogo com um conjunto de critérios para avaliar aplicações de blockchain. Para isso, eles usaram os conceitos de Qualidade de Software para atender aos critérios específicos para blockchain. Inicialmente, foi apresentado um sumário com cada critério escolhido e uma breve descrição explicando como avaliar este critério. O sumário foi escrito em texto, dividido em parágrafos, em que cada parágrafo corresponde a um critério diferente. Em seguida, foi elaborada uma tabela aplicando o catálogo de critérios em 3 aplicações blockchain extremamente conhecidas no mercado: *Bitcoin*, *Hyperledger* e *Ethereum*.

Saraiva, Soares e Castor [62] desenvolveram um catálogo de métricas de manutenção de software orientado a objetos. Os autores identificaram que existia um grande número de métricas para medir a Manutenção de Software Orientado a Objetos (do inglês, *Object-Oriented Software Maintainability* - OOSM). Este foi um trabalho pioneiro na área uma vez que não existia até então um catálogo abrangente e útil para descrever quais métricas são as mais adequadas para serem adotadas na avaliação dos OOSM. A metodologia adotada consistiu em um estudo de mapeamento sistemático para identificar métricas de sustentabilidade realizado em um trabalho anterior. A partir disso, foram extraídas 570 métricas relacionadas à OOSM. Após a identificação das métricas, foi feita uma classificação e agrupamento em 15 categorias diferentes de domínio para auxiliar a construção do catálogo. Essas categorias gerais foram a base dos critérios de inclusão ou exclusão para selecionar o que compôs ou não o catálogo. Neste trabalho foi discutido uma série de opções de categorização de métricas de OOSM, tornando esse processo preciso e confiável. O catálogo proposto, portanto, consistiu em uma estrutura de texto na qual cada parágrafo corresponde a uma métrica distinta, seguido por uma explicação porque essa métrica foi escolhida para compor o catálogo e a fonte de onde foi extraída a métrica.

Carvalho, Andrade e de Oliveira [85] estudaram correlações de NFRs em Computação Ubíqua (do inglês, *Ubiquitous Computing* - UbiComp) e Internet das Coisas (do inglês, *Internet of Things* - IoT). Invisibilidade é um termo bastante utilizado no contexto de IoT e se refere à fusão da tecnologia no ambiente do usuário. Essa pesquisa visou capturar correlações de invisibilidade com NFRs para sistemas UbiComp e IoT e definir um catálogo com essas informações. Para realizar esse catálogo os autores realizaram um estudo sistemático por meio dos seguintes métodos de pesquisa: Entrevista, Análise de Conteúdo Técnico e Questionário. O catálogo proposto possui mais de 100 correlações positivas e negativas com 9 NFRs. A estrutura do catálogo criado consiste em uma tabela com 3 colunas em que a primeira coluna é a estratégia adotada, a segunda diz respeito se o impacto foi positivo ou negativo e a terceira é o NFR relacionado. Os autores avaliaram o catálogo realizando um experimento controlado para verificar se ele ajuda os desenvolvedores na tomada de decisões sobre NFRs em sistemas UbiComp e IoT e os resultados indicaram que o catálogo melhorou as decisões dos participantes

Após analisar trabalhos que constroem catálogos, é possível perceber que eles estão presentes em diversas áreas da computação. Como visto em [60, 85] na área de Engenharia de Requisitos, em [61] na área de Banco de Dados e blockchain e em [62] na área de Engenharia de Software e Manutenção de software.

Os catálogos desenvolvidos nos trabalhos mencionados também mostraram ser uma forma robusta e direta de expor os dados de uma pesquisa. Este corpo de conhecimento é utilizado por terceiros para acumular experiências anteriores e acrescentar novas [86]. Assim, é útil para apoiar os interessados na seleção de estratégias adequadas que satisfaça o que é proposto.

Também é importante pontuar que para realizar a construção dos catálogos, os trabalhos acima utilizaram como metodologia a realização de um estudo prévio do tema abordado e em seguida fizeram um estudo sistemático para coletar amostragens suficientes para a construção do catálogo. A partir dos insumos e dos estudos anteriores, os autores escolheram critérios de inclusão e exclusão para selecionar as informações a serem incluídas no catálogo.

2. Referencial Teórico

Neste capítulo são discutidos os principais conceitos relacionados a este trabalho: privacidade, leis de privacidade e políticas de privacidade.

2.1 Privacidade

Privacidade é um termo antigo que vem sendo definido de acordo com a realidade de cada época e no contexto histórico associado.

Por ser um conceito bem antigo, a mitologia grega já abordava esse tema. A história afirma que a deusa Diana puniu o filho do rei Cadmo, chamado Acteón, por ter espionado ela nua, enquanto tomava banho (violando assim sua privacidade). A deusa então transformou o príncipe em um cervo e, dessa forma, ele não conseguia se comunicar com ninguém para contar que havia visto a deusa sem roupa [22].

Ainda na Grécia antiga, os filósofos Platão e Aristóteles tratavam da concepção de esfera pública e privada. Platão defendia não haver diferença entre o que é particular e o coletivo. Aristóteles, por outro lado, afirmava que a distinção entre uma esfera de vida privada e uma esfera de vida pública corresponde à existência da família e da política como entidades diferentes e separadas. No pensamento Aristotélico, a esfera privada é inferior à esfera pública, precedendo-a no tempo e no espaço. O privado é constituído pela família, ambiente responsável por desenvolver em seus membros uma ética individual, necessária nas relações interativas no público [23].

O conceito de privacidade foi então se desenvolvendo e ganhando cada vez mais destaque. Já no final da idade Moderna, uma das muitas influências com as quais a Revolução Francesa teve no mundo, foi a inserção nas Constituições da dignidade do ser humano como direito fundamental. Os direitos ligados à pessoa se tornam inerentes, impossíveis de serem desvinculados do ser, garantindo a ele constitucionalmente vida privada e direito à intimidade [24].

Em 1890, os advogados Samuel Warren e Louis Brandeis escreveram e publicaram um dos artigos mais famosos da história do direito americano, denominado: “O Direito à Privacidade" (do inglês, “*The Right to Privacy*”), articulando esse direito principalmente como um “*direito de ser deixado sozinho*” [26].

O 12º artigo da Declaração Universal dos Direitos Humanos de 1948 [63] deixa claro que ninguém deve ser submetido à adversas interferências com a sua privacidade, família, casa ou correspondência, nem a ataques sobre sua honra e reputação. Todos têm direito à proteção da lei contra essas arbitrárias e indesejadas influências externas.

Thomas Scanlon é um famoso filósofo contemporâneo americano que estudou conceitos de privacidade [64], de acordo com ele, o primeiro elemento a se pensar em uma teoria da privacidade deve ser uma caracterização do interesse especial que temos em ser capaz de ficar livres de certos tipos de intrusões.

A evolução da tecnologia, em especial o uso dos smartphones nas diferentes classes sociais e a difusão estrondosa de aplicativos com diversas

funcionalidades têm mostrado que o conceito de privado da era passada não se aplica mais aos dias de hoje [65]. Inclusive, há pesquisas que afirmam que a privacidade não existe mais [25]. Existem mais de um bilhão de sites na internet que são acessados por quase metade da população de todo o planeta [72]. Como resultado disso, uma quantidade muito grande de dados é coletada e processada por serviços terceiros. Sendo assim, é importante que a computação que trata diretamente com o controle, obtenção, armazenamento e uso desses dados, também aborda as questões de privacidade.

Cranor [15], em seu estudo, discutiu requisitos de privacidade com base em dados históricos e perspectivas contemporâneas sobre privacidade. Ele afirmou que todo sistema de informação executa um ou mais das seguintes funções: transferência, armazenamento e processamento de dados. Cada uma dessas atividades pode levar a vulnerabilidades relacionadas à privacidade.

Na Engenharia de Software, a privacidade também se tornou um ponto importante e debatido em muitos estudos. A Dra. Ann Cavoukian [70] argumenta que o futuro da privacidade não pode ser garantido apenas pela conformidade com marcos regulatórios, ao contrário disso, a garantia de privacidade deve se tornar o modo de operação padrão de uma organização.

Sendo assim, os desenvolvedores devem, desde o princípio do processo de desenvolvimento, se preocupar com questões relacionadas à privacidade [70]. Essa visão também é compartilhada por outros autores como Peixoto, Silva e Maia [60]. Esse novo paradigma é recente e possui impacto significativo nas organizações, pois pesquisas revelam que não é comum que os desenvolvedores abordem a privacidade dos dados dos usuários no processo de desenvolvimento [71]. Para que a privacidade se torne o *modus operandi* de uma empresa, a Dra. Cavoukian destacou 7 princípios de Privacidade por Design (do inglês, *Privacy by Design - Pbd*) que devem ser seguidos pelas organizações para garantir uma melhor proteção dos dados de seus usuários [70]:

1. **Proatividade:** Antecipar e evitar eventos invasivos a privacidade antes mesmo que aconteçam.
2. **Padrão (*Default*):** Garantir que os dados pessoais sejam protegidos automaticamente em qualquer sistema de tecnologia da informação (TI) ou prática de negócios.
3. **Embutido:** O Pbd deve estar embutido no design e arquitetura de sistema de TI e práticas de negócios. Não como um complemento, a privacidade deve ser parte integrante do sistema.
4. **Funcionalidade total:** O Pbd busca acomodar todos os interesses e objetivos da organização em uma forma de soma positiva, isto é, as funcionalidades da aplicação devem ser garantidas por completo, em conjunto com a privacidade.
5. **Segurança de ponta a ponta:** O Pbd ter sido incorporado no sistema antes da primeira informação ser coletada estende a segurança dos dados por todo o ciclo de vida dos dados envolvidos.
6. **Visibilidade e transparência:** Procurar sempre assegurar que todas as partes interessadas estão operando de acordo com as práticas declaradas, sujeitas a verificação.
7. **Respeito a privacidade do usuário:** O Pbd requer arquitetos de software que busquem manter os interesses dos usuários,

oferecendo medidas de privacidade fortes, avisos apropriados e amigáveis.

Nesse contexto, o conceito de privacidade mudou bastante ao longo dos anos, principalmente com a chegada da internet e a facilidade de acesso às redes através do avanço da tecnologia. Dessa forma, é importante também compreender as formas de regulamentar e proteger os usuários de possíveis ameaças relacionadas à privacidade e proteção de dados.

2.2 Leis de privacidade

Ao redor do mundo, vários países já se atentam a proteger seus habitantes de possíveis ameaças à invasão de seus dados pessoais. Existem diversas leis que visam regulamentar e fortalecer as práticas de segurança e privacidade de dados. Algumas dessas leis abrangem um conjunto de países específicos, como a Lei de Proteção de Dados da União Europeia [73], outras são de nível nacional, focando em um país específico, como é o caso da Lei de Proteção de Dados Pessoais brasileira [74] e ainda existem aquelas a nível estadual como é o caso do Ato de Privacidade do Consumidor da Califórnia [75]. Trata-se, afinal, de uma preocupação crescente tanto por parte dos órgãos reguladores quanto por parte das empresas e dos próprios cidadãos.

A Regulamentação Geral de Proteção de Dados (do inglês, *General Data Protection Regulation* - GDPR) foi aplicada em todos os Estados-membros da União Europeia em 25 de maio de 2018 e foi um marco na evolução da estrutura da privacidade europeia. A lei europeia foi impulsionada por uma filosofia de abordagem à proteção de dados, com base no conceito de privacidade como um direito humano fundamental (conforme determinado na Carta dos Direitos da UE [76]), o Regulamento teve um amplo impacto global. A lei abrange os dados pessoais dos residentes da União Europeia independentemente da localização do processamento. Dados pessoais são informações que, diretamente ou indiretamente, podem identificar um indivíduo, e inclui especificamente identificadores online, como endereços IP (do inglês, *Internet Protocol* - IP), cookies, impressão digital e localização de dados que podem identificar indivíduos. Isso é muito mais amplo do que o conceito de informações de identificação pessoal sob a lei de privacidade dos Estados Unidos [75].

A GDPR tem seis princípios gerais de proteção de dados: (1) justiça e legalidade, (2) limitação de propósito, (3) minimização de dados, (4) precisão, (5) limitação de armazenamento e (6) integridade e confidencialidade. A proteção de dados por padrão (*privacy by default*) é a essência da GDPR. É suportado de um lado pela transparência, garantido que todas as informações sejam fornecidas para indivíduos em um estilo acessível e, do outro lado, por prestação de contas, garantindo que todas as organizações assumam responsabilidades comprovadas pelo uso de dados pessoais.

Os Estados Unidos não possuem apenas uma lei de proteção de dados que regulamenta todo o território americano. Na realidade, o país possui diversas legislações específicas dependendo do contexto a que a privacidade afeta. Existem atualmente cerca de 20 leis voltadas à proteção de dados dos norte-americanos, além de outras 100 legislações estaduais de privacidade [77]. A mais antiga e a principal dessas leis é o Ato de Privacidade do Consumidor da Califórnia (do inglês, *California Consumer Privacy Act* - CCPA), que garante aos

consumidores da Califórnia quatro direitos básicos sobre seus dados pessoais:

1. O direito de serem notificados caso seus dados pessoais estejam sendo analisados ou processados em alguma plataforma;
2. O direito de terem acesso aos dados que foram coletados ou estão sendo utilizados para extrair alguma informação;
3. O direito de poderem optar (ou não) por uma coleta de dados;
4. O direito de terem acesso igualitário a serviços;

O CCPA se aplica a empresas que atendam a uma ou mais das seguintes:

1. Têm uma receita anual bruta de mais de US$ 25 milhões;
2. Derivam mais de 50% da receita anual da venda de informações pessoais do consumidor da Califórnia;
3. Compram, vendem ou compartilham as informações pessoais de mais de 50.000 consumidores da Califórnia anualmente.

É válido pontuar que as empresas que coletam e/ou tratam dados dos cidadãos californianos precisam seguir o CCPA, e não apenas aquelas com sede no estado. As empresas regulamentadas pelo CCPA têm várias obrigações com seus consumidores, incluindo divulgações sobre os direitos de usuário, um "*opt-out*" para determinadas transferências de dados e um requisito de "aceitação" para menores.

Neste contexto, a regulamentação da CCPA tem sido uma conjuntura crítica onde diversas partes se envolvem na definição legal do que a privacidade de dados deve implicar na Califórnia. A Califórnia foi o primeiro estado que aplicou uma lei de privacidade nos Estados Unidos. Além disso, esse estado é um símbolo que abriga muitas empresas de tecnologia no Vale do Silício, incluindo sedes de grandes corporações como Facebook, Google e Twitter. Portanto, o CCPA foi considerado uma referência para uma lei federal ou um gatilho para uma colcha de retalhos de leis estaduais [32].

No Brasil, em agosto de 2018, foi criada a Lei nº 13.709 a Lei Geral de Proteção de Dados Pessoais (LGPD), que visa medidas preventivas e proativas na manutenção e privacidade dos dados de terceiros. A Lei parte do princípio de que todo dado pessoal tem importância e valor. Por essa razão, o conceito amplo de dado pessoal foi adotado, assim como estabelecido no Regulamento Europeu (GDPR), sendo ele definido como informação relacionada à pessoa natural identificada ou identificável. Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela.

A lei exige que toda captação, armazenamento e processamento que envolva dados pessoais dos usuários precisa ter uma base legal, isto é, uma autorização prevista na LGPD para que o tratamento daqueles dados seja realizado. A LGPD enumera dez diferentes possibilidades de bases legais, mas duas delas são consideradas as mais importantes: o consentimento e o legítimo interesse.

O artigo 5º, inciso XII da LGPD diz que o consentimento significa uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. As palavras são importantes na LGPD, então vale atentar que o consentimento genérico, sem uma finalidade específica, não é considerado válido pela lei [78]. Além disso outros pontos merecem atenção [33]:

1. **Manifestação livre:** O usuário deve concordar afirmativamente e ativamente;
2. **Manifestação informada:** Deve haver meios para que o usuário compreenda de que forma os dados serão tratados e qual a funcionalidade específica deles;
3. **Manifestação inequívoca:** Deve haver meios para comprovar que não há dúvidas da escolha do usuário a respeito do tratamento de dados.

Dessa forma, a LGPD determina que é necessário obter e documentar o consentimento do usuário. Algumas alternativas para realizar esse procedimento é obter a concordância do usuário por meio de um *opt-in* em uma política de privacidade, que deve ter disposições razoáveis, claras e bem escritas sobre como e para que finalidades específicas a empresa irá utilizar os dados do usuário, incluindo como o usuário pode exercer seus direitos [33]. Um *opt-in* no contexto de privacidade é uma autorização em que o usuário ativamente expressa que está de acordo com o documento [79]. Na prática o *opt-in* é normalmente um botão ou uma caixa de seleção que o usuário pode interagir. Uma outra alternativa é obter o consentimento por meio de um aviso de cookies (cookies são considerados dados pessoais tanto pela LGPD, quanto GDPR, assim como qualquer outra tecnologia que atribui um identificador único, ainda que aleatório, a um usuário).

O artigo 9º da LGPD afirma que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados. Além disso, as operações envolvidas com o tratamento de dados devem ser disponibilizadas de forma clara, adequada e ostensiva. A forma legal de documentar essas operações é por meio de uma política de privacidade. Também é dever da política de privacidade fornecer informações acerca da [80]:

1. Finalidade específica do tratamento;
2. Forma e duração do tratamento, observados os segredos comerciais e industriais;
3. Identificação do controlador;
4. Informações de contato do controlador;
5. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
6. Responsabilidades dos agentes que realizaram o tratamento;
7. Direitos do titular, com menção explícita aos direitos contidos no artigo 18 desta lei.

É possível perceber que para construir suas diretrizes de proteção de dados, cada país se inspira em leis existentes. Seja nas medidas que se provaram eficazes, adotando estas mesmas medidas, ou naquelas que se

mostraram infrutíferas, abolindo-as de suas leis. Também é importante destacar que a GDPR se tornou a principal referência nesse sentido, motivando muitas outras nações a reformularem ou trabalharem em regras similares às da lei europeia, mas adaptando para sua realidade particular [81].

Após entender o princípio de algumas leis de privacidade, é válido estudar como cada empresa ou organização lida com os dados pessoais de seus usuários internamente através das políticas de privacidade, além de pontuar o que deve constar nesses documentos.

2.3 Políticas de privacidade

Uma política de privacidade pode ser definida como uma descrição abrangente das práticas de coletas de dados de um site ou aplicação [34]. Uma política de privacidade define quais informações são coletadas, a finalidade da coleta das informações e como os dados serão manipulados, armazenados e utilizados pela aplicação. Além disso, a política de privacidade também é responsável por fornecer informações se os clientes têm permissão para acessar as informações coletadas e para resolver disputas relacionadas à privacidade com o site [35].

Uma política de privacidade serve como o principal meio de comunicação com os usuários sobre quais e como as Informações Pessoais Sensíveis (do inglês, *Sensitive Personal Information* - SPI) foram acessadas, coletadas, armazenadas, compartilhadas (de um aplicativo para outro aplicativo e ou para terceiros), como foram usadas, processadas e a finalidade da coleta ou do processamento das SPI [82].

As políticas de privacidade geralmente consistem em vários parágrafos de linguagem natural, como o seguinte trecho disponibilizado por um aplicativo listado no Google Play:

“Poderemos de fato criar e atribuir ao seu dispositivo um identificador único, similar a um número de conta. Nós poderemos coletar o nome que você associou ao seu dispositivo, o tipo de dispositivo que você possui, o número do seu telefone, seu país e qualquer outra informação que você opte por nos fornecer, como um nome de usuário, geolocalização ou endereço de e-mail. Nós poderemos também acessar sua lista de contatos para permitir que você convide seus amigos para acessar nosso Website.”

As políticas de privacidade são particularmente importantes no contexto de aplicativos e aplicações web em geral devido à abordagem de “aviso e escolha” usada para abordar a privacidade online [36]. Sob essa estrutura, as empresas de aplicativos publicam suas políticas de privacidade e os usuários devem ler as políticas para tomar decisões informadas sobre aceitar os termos de privacidade antes de começar a utilizar as aplicações de fato [37].

A literatura apresenta um amplo histórico de que políticas de privacidade são particularmente difíceis de serem implementadas [38], muitas vezes resultando em documentos que são longos, difíceis de interpretar, confusos e que possuem uma linguagem técnica sofisticada [38]. Existe no meio acadêmico uma série de trabalhos que fazem análise de políticas de privacidade [18, 19, 20, 21] avaliando parâmetros como o nível de legibilidade dos documentos, conformidade com as práticas reais das aplicações relacionadas e se estão de acordo com a lei de privacidade vigente.

A maioria das políticas de privacidade preparadas pelas empresas responsáveis são difíceis de entender devido à sua natureza prolixa e ambígua, e isto pode fazer com que os usuários não realizem a leitura, mesmo que tenham dúvidas sobre as práticas de coleta de informações. Por outro lado, os desenvolvedores da aplicação podem não ser capazes de cumprir aquilo que está descrito na política de privacidade de maneira eficaz, podendo haver brechas entre o que está sendo realmente executado na aplicação e o que o documento descreve [39].

Um estudo conduzido em 2016 [40] verificou que várias empresas foram multadas pelos órgãos reguladores de privacidade uma vez que as políticas de privacidade que eles forneciam não eram consistentes com as práticas reais de coleta de dados. Para ajudar os desenvolvedores a verificar a inconsistência, eles desenvolveram uma estrutura semiautomática que vincula frases de políticas a métodos de *API* que tratam de informações confidenciais e detectam esses desalinhamentos. A avaliação feita considerou os 477 mais bem avaliados aplicativos Android e descobriu potencial violação da política de privacidade em 341 deles. Dessa forma, é possível identificar essa diferença e então corrigir o erro para evitar as multas.

Um grande obstáculo na compreensão e análise da política de privacidade é que não existe um formato canônico para a apresentação das informações [21]. O idioma, a organização e os detalhes específicos das políticas podem variar de aplicativo para aplicativo [83]. Existe uma incompatibilidade frequente entre as questões que as empresas desejam abordar em suas políticas, e o que os usuários querem saber sobre as práticas de negócios. As políticas de privacidade diferem muito de um local para outro e há uma falta de regulamentação ou padronização pela indústria. Isso se aplica tanto em termos da linguagem usada nas políticas e os problemas que elas abordam. Essa falta de padrão torna difícil comparar e contrastar políticas, diminuindo assim seu valor para os usuários [41].

Uma política de privacidade deve levar em consideração algumas informações específicas, já que é preciso ser bastante claro e adequado ao redigir. Algumas sessões importantes que devem estar contidas no documento [84]:

1. Qual o modelo de negócio adotado pela empresa;
2. As legislações pertinentes e que se aplicam;
3. Quais informações do usuário são coletadas;
4. Para qual finalidade as informações do usuário são coletadas;
5. Se haverá compartilhamento com outras aplicações ou com terceiros;
6. De que forma as informações coletadas são armazenadas e protegidas.

Os trabalhos de Karjoth [42], Carvalho [87] e Tavani [44] trouxeram em seus estudos uma abordagem simplificada sobre como escrever uma política de privacidade utilizando as melhores práticas para que seja coerente com o que se espera. Os autores trouxeram que:

Em primeiro lugar, é importante considerar que a política precisa ser pertinente para a área de atuação do modelo de negócio a que ela se propõe, visto que isso varia de produto para produto. No Brasil, a Lei Geral de Proteção de Dados Pessoais é a mais recente legislação a regulamentar o tema, trazendo

diversos direitos, responsabilidades e personagens, como os controladores, operadores e encarregados de proteção de dados. É fundamental que se tenha um conhecimento sobre as bases legais da LGPD ao escrever uma política de privacidade [87].

Em seguida, é necessário que seja descrito com especificidade como ocorre o tratamento dos dados, isto é, quais dados estão sendo coletados, para qual finalidade eles estão sendo coletados e de que forma isso acontece. Outro ponto que deve ser considerado é os direitos do usuário, como o acesso aos dados e a revogação do consentimento. Como nem todos os titulares conhecem seus direitos, é uma boa ideia apresentá-los [42].

É imprescindível que a política de privacidade tenha uma grande preocupação com a questão do acesso aos dados coletados. Uma boa prática é elencar todas as pessoas que terão contato com as informações dos usuários [42]. Se várias equipes participam do processo, é possível explicar a atuação de cada uma. Também deve ser mencionado se os dados são compartilhados com parceiros comerciais ou demais pessoas, naturais ou jurídicas. Caso estes parceiros tenham políticas de privacidade próprias, elas podem ser anexadas ao texto [44]. Essa prática é importante pois pode haver divergências entre o documento que está sendo escrito e as políticas dos parceiros e o usuário precisa estar ciente.

A política de privacidade também deve explicar como os dados são armazenados e quais medidas de segurança são tomadas [42]. Ainda se tratando de medidas mais técnicas, o usuário espera entender como as informações coletadas estão seguras. Portanto, é uma boa prática explicar como os dados são armazenados e por quanto tempo, para ganhar cada vez mais a confiança do usuário de que ele pode confiar as informações pessoais dele [44]. Caso exista algum protocolo a ser seguido em situações de emergência, como um vazamento de dados causado por algum hacker, é nesse momento que deve ser apresentado.

Caso a aplicação web utilize cookies, cuja principal função é entender o comportamento do usuário, personalizando a experiência de uso ou facilitando o transporte de informações entre páginas do mesmo site, é preciso que se tenha uma política de cookies para que o usuário se informe a respeito [87].

Por fim, após explicar todo o processo de tratamento de dados e apresentar os direitos do titular é indicado disponibilizar um canal de atendimento ao usuário para que se possa tirar possíveis dúvidas ou realizar solicitações referentes aos seus direitos [87]. Também é importante manter a política de privacidade atualizada e adequá-la a eventuais mudanças que ocorram em virtudes de novas leis ou atualizações de processos internos [87].

3. Metodologia

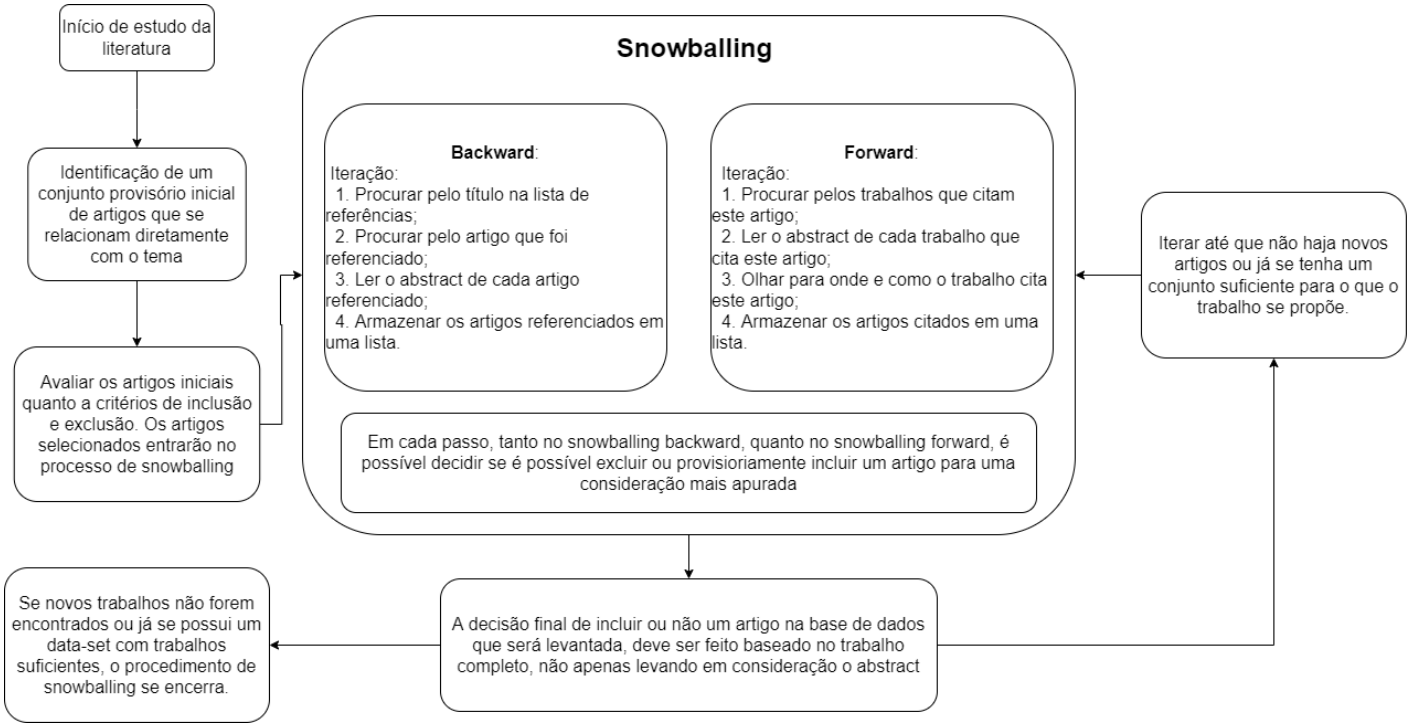
A metodologia adotada para executar esse trabalho consistiu de três etapas:

1. **Revisão de literatura**: foram investigados conceitos de privacidade, LGPD, políticas de privacidade e critérios de avaliação descritos no capítulo 2;
2. ***Snowballing***: a partir de um conjunto inicial de estudos, foram identificados novos trabalhos que abordam avaliação de políticas de privacidade;
3. **Elaboração do catálogo**: um conjunto de critérios para avaliação de políticas de privacidade.

3.1 *Snowballing*

Para elaborar o catálogo, foi conduzido um estudo sistemático da literatura existente sobre trabalhos que avaliam políticas de privacidade. A técnica abordada foi *snowballing* [45] que se refere ao uso da lista de referências bibliográficas de um artigo (*backward*) ou as citações deste artigo (*forward*) para identificar trabalhos adicionais. Este procedimento é conduzido de forma exaustiva, identificando as referências e citações dos novos trabalhos selecionados até que não se consiga encontrar novos artigos. A Figura 1 apresenta o fluxo que foi seguido para se aplicar a técnica de *snowballing* neste trabalho.

Figura 1 – Passos para aplicação da técnica de *snowballing*.



Fonte: O autor.

Ao aplicar a técnica de *snowballing*, o passo inicial é identificar um conjunto primário de artigos a serem usados como ponto de partida. Para este trabalho foi utilizado o Google Scholar a fim de identificar novos artigos, dessa forma, é evitado viés na seleção dos trabalhos. Foram identificadas palavras-chave e formuladas sequências de pesquisas acerca do tema abordado.

O conjunto inicial de artigos foram [18], [20] e [21]. Estes trabalhos foram escolhidos seguindo alguns critérios descritos em [45], a saber:

1. Devem ser trabalhos relevantes para a comunidade científica e que se relacionem diretamente com o tema escolhido.
2. Os artigos iniciais, preferencialmente, devem vir de diferentes comunidades para evitar o risco de um artigo referenciando ou citando o outro da mesma comunidade e enviesar a pesquisa.
3. O número de artigos no conjunto inicial não deve ser muito pequeno. O tamanho do conjunto inicial depende da amplitude da área de estudo. Uma área menor (com foco mais específico) requer menos artigos do que uma área ampla.
4. Caso muitos artigos tenham sido encontrados, por exemplo, devido a ter muitos termos de pesquisa gerais no Google Scholar, deve-se identificar os artigos mais relevantes e mais citados.
5. O conjunto inicial deve abranger vários editores diferentes, anos e autores para aumentar a diversidade.

Após a definição do conjunto inicial de artigos, o próximo passo foi a escolha de por qual artigo deve ser iniciada a técnica de *snowballing*. Para isso, foi feito um estudo entre esses artigos iniciais ponderando algumas questões entre eles:

1. Quantidade de trabalhos referenciados;
2. Quantidade de trabalhos que citam este artigo;
3. Ano de publicação;
4. Relevância direta com o tema.

A Tabela 2 mostra a comparação entre esses pontos nos trabalhos do conjunto inicial considerado.

Tabela 2 – Comparação entre os artigos iniciais para *snowballing*.

Critério:	**Artigo [18]**	**Artigo [20]**	**Artigo [21]**
Quantidade de trabalhos referenciados	29	54	60
Quantidade de trabalhos que citam este artigo	142	7	24
Ano de publicação	2002	2020	2016

Relevância direta com o tema	Sim	Sim	Sim

Após essa análise inicial, foi escolhido o trabalho [18] para se iniciar a técnica de *snowballing* pois ele apresenta uma quantidade elevada de citações e está relacionado diretamente com o tema, conforme discutido na seção de trabalhos relacionados.

A cada iteração do *snowballing*, tanto *backward* quanto *forward*, foram aplicados critérios de inclusão e exclusão em cada artigo, para determinar se o trabalho iria ser selecionado ou não.

Para esse estudo foram considerados os seguintes critérios de inclusão:

1. Artigos escritos em português ou em inglês;
2. Artigos que se aplicam ao tema.

Os critérios de exclusão aplicados foram os seguintes:

1. Não são escritos em inglês ou português;
2. É literatura cinza (livros, sites, teses, dissertações etc.);
3. Não realizam avaliações de políticas de privacidade;
4. Não descreve os critérios usados na avaliação das políticas de privacidade.

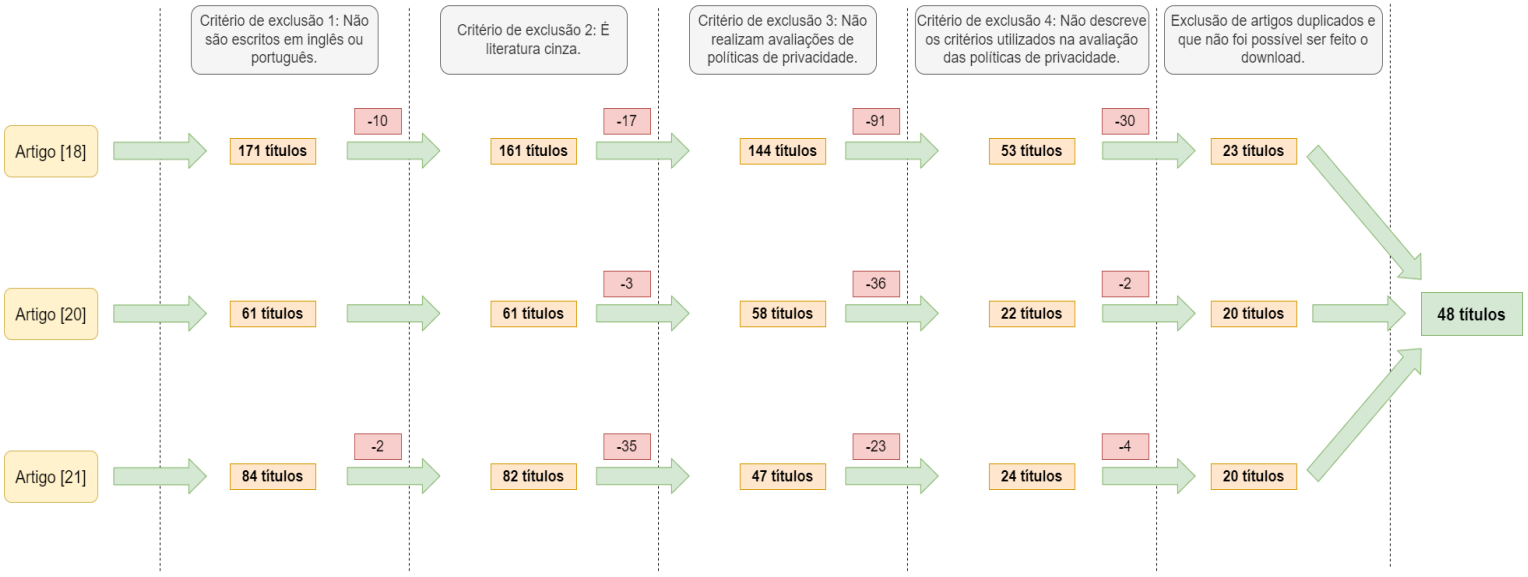
Foram excluídos artigos que se aplicam ao tema, porém escritos em espanhol e em mandarim, e, portanto, esses trabalhos não foram considerados na análise.

Não foram analisados também trabalhos relacionados ao tema que são considerados literatura cinza, isto é, estão disponíveis em livros, sites, são teses, dissertações, entre outros. Estes trabalhos não foram publicados e, por isso, não é possível ter um controle adequado sobre a validade das informações neles expostas, sendo assim, foi preferível descartar esses tipos de estudos.

Também foram descartados trabalhos que não realizam avaliações de políticas de privacidade ou, por algum motivo, não deixam claro quais os critérios utilizados para avaliar as políticas. Como o objetivo deste estudo é elaborar um catálogo de critérios para avaliar políticas de privacidade, foram desconsiderados trabalhos que não fazem isso.

Iniciou-se então a técnica de *snowballing backward* com as referências do trabalho [18]. Foi identificado que este trabalho foi publicado em 2002, há quase duas décadas e foi pioneiro no tema abordado. Dessa forma, os 29 artigos referenciados por ele não se adequaram aos objetivos do catálogo, descartando então a possibilidade de selecionar alguma das referências deste trabalho para a base de dados. O próximo passo consistiu na busca por trabalhos que citam este artigo, aplicando a técnica de *snowballing forward*. Foi utilizado o Google Scholar para identificar se haviam citações ao trabalho [18] cuja busca ocorreu em novembro de 2021. Foi constatado, então, que esse artigo era citado por 142 outros trabalhos, dessa forma, iniciou-se a análise destes trabalhos. O processo de seleção dos estudos é apresentado na Figura 2.

Figura 2 – Processo de seleção de estudos no *snowballing*.



Fonte: O autor.

A primeira série de seleção ocorreu com os 142 artigos que citam o trabalho [18] considerando os critérios de inclusão e exclusão descritos anteriormente. Após se aplicar o primeiro critério, selecionando apenas os trabalhos escritos em inglês ou em português, 10 trabalhos foram descartados. Em seguida, foram descartados os trabalhos que eram considerados literatura cinza, isto é, publicações não convencionais e não comerciais, difíceis de encontrar em canais tradicionais de distribuição, como livros, sites, jornais, teses e dissertações, com isso, mais 7 citações foram eliminadas. Depois, foram eliminados os artigos que não realizam avaliação de políticas de privacidade, pois não se relacionam diretamente com o tema do catálogo que se busca desenvolver, assim, 72 artigos foram descartados. Foram eliminados também artigos que não descrevem os critérios utilizados para avaliar as políticas de privacidade, após aplicar esse critério, mais 30 artigos foram descartados. Por fim, mais 1 artigo foi excluído pois não foi possível fazer o download dele. Sendo assim, um conjunto final de 19 artigos foram selecionados para leitura completa.

Continuando o processo de *snowballing*, foram analisadas todas as 60 referências e as 24 citações de [21], totalizando 84 artigos. Aplicando-se novamente os critérios de inclusão e exclusão, 2 trabalhos foram excluídos por não estarem escritos nem em português nem em inglês, 35 trabalhos foram excluídos por serem considerados literatura cinza, 23 foram excluídos por não avaliarem políticas de privacidade e mais 4 trabalhos foram descartados por não descrever os critérios de avaliação das políticas de privacidade. Dessa forma, após executar o *snowballing* em [21] e aplicar os critérios de inclusão e exclusão, 20 artigos foram adicionados à base de dados para serem considerados.

Por último, foi executado o *snowballing* em [20], foram estudadas as 54 referências e 7 citações deste artigo, totalizando 61 trabalhos. Foi iniciada a filtragem, considerando apenas os trabalhos escritos em inglês e português, nenhum artigo foi descartado, 3 artigos foram descartados pois eram literatura cinza, 36 trabalhos foram excluídos pois não realizam a avaliação de políticas de privacidade e mais 2 artigos foram desconsiderados porque não descrevem os

critérios de avaliação das políticas. Portanto, 20 artigos foram incluídos na base de dados.

Após realizar a técnica de *snowballing* tanto *forward* quanto *backward* no conjunto inicial de artigos, obtivemos 59 trabalhos para serem estudados e analisados para a construção do catálogo. Entretanto, foi observado que existiam alguns artigos repetidos nesta amostragem, ou seja, chegou-se no mesmo artigo após aplicar o *snowballing forward* ou *backward* em diferentes trabalhos. Isto era esperado pois, embora tenham sido escolhidos artigos de diferentes épocas, autores e comunidades, todos abordavam a avaliação de políticas de privacidade, então, é natural que alguns deles citem ou referenciam os outros. Foram eliminados então, os 11 artigos que estavam duplicados.

Finalmente, chegou-se ao número de 48 artigos selecionados no banco de dados para serem avaliados. Foi optado por não realizar outra iteração do *snowballing* pois os artigos contemplados já possuem uma quantidade considerável de critérios de avaliação de políticas de privacidade. Constatou-se também que os critérios estavam começando a se repetir. Além disso, os artigos selecionados são bem variados, avaliando documentos de subconjuntos distintos de sites e aplicações, englobando diversas áreas.

3.2 Elaboração do catálogo

Após a seleção dos estudos, foi iniciada a extração dos critérios de avaliação de políticas de privacidade em cada artigo. Em um primeiro momento, cada artigo selecionado foi analisado individualmente e os critérios foram extraídos. Após a extração inicial, foi identificado que muitos critérios eram semelhantes de artigo para artigo. Sendo assim, os critérios correlacionados foram agrupados. Por exemplo, a Política de Privacidade menciona que o nome do usuário está sendo coletado e menciona que o e-mail do usuário está sendo coletado, estes e outros critérios foram agrupados no critério: A Política de Privacidade menciona claramente quais dados estão sendo coletados. Além disso, os critérios foram divididos em categorias gerais para facilitar o processo de avaliação. Por exemplo, os critérios: A Política de Privacidade especifica claramente como os dados são coletados e A Política de Privacidade especifica claramente como os dados do usuário são utilizados, foram agrupadas na categoria Conteúdo da Política de Privacidade.

3.3 Ameaças à validade

Para reduzir ameaças à validade dessa pesquisa, foram utilizados os critérios de seleção dos estudos iniciais propostos em [45]: Os trabalhos selecionados são relevantes para a comunidade científica, isto é, publicados em conferências e periódicos reconhecidos por alta qualidade; e que se relacionam diretamente com o tema escolhido. Esses artigos também apresentam uma alta quantidade de citações, o que confirma a relevância deles para o estudo. Os artigos iniciais também vieram de diferentes comunidades científicas com o objetivo de não ocorrer o risco de um trabalho referenciando o outro, aumentando dessa forma a variedade entre os trabalhos recolhidos.

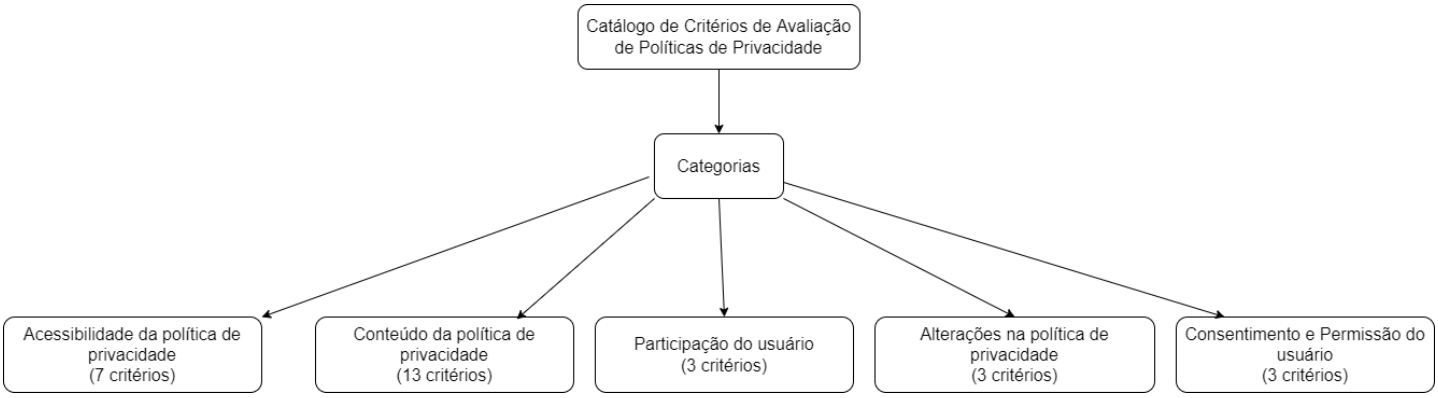
4. Catálogo de critérios de avaliação de políticas de privacidade

A partir dos estudos selecionados, foram identificadas cinco categorias listadas a seguir:

1. **Acessibilidade da Política de Privacidade**: Avalia a experiência do usuário quanto ao acesso ao documento;
2. **Conteúdo da Política de Privacidade**: Avalia a Política de Privacidade em relação ao seu conteúdo;
3. **Participação do usuário**: Avalia a participação do usuário na Política de Privacidade;
4. **Alterações na Política de Privacidade**: Avalia como é tratada eventuais alterações na Política;
5. **Consentimento e Permissão do Usuário:** Avalia como ocorre o processo de consentimento e permissão do usuário a Política de Privacidade.

Foram extraídos 29 critérios que foram agrupados nas cinco categorias listadas acima. A Figura 3 apresenta as categorias e a quantidade de critérios em cada uma.

Figura 3 – Critérios por cada categoria.



Fonte: O autor.

A divisão de critérios por categoria foi a seguinte: 7 critérios foram atribuídos à categoria de Acessibilidade da Política de Privacidade, 13 critérios foram atribuídos à categoria de Conteúdo da Política de Privacidade, 3 critérios foram atribuídos a categoria de Participação do usuário, 3 critérios foram incluídos na categoria de alterações na Política de Privacidade, 3 critérios foram incluídos na categoria de Consentimento e Permissão do usuário.

Cada categoria é descrita a seguir juntamente com seus critérios associados. Para cada categoria, foi gerada uma tabela com seus critérios e a referência do artigo cujo critério foi extraído para fins de rastreabilidade. Os

artigos utilizados para extração dos critérios estão listados no apêndice A e as referências das tabelas baseadas nos identificadores dessa listagem.

4.1 Acessibilidade da Política de Privacidade

A responsabilidade dessa categoria é avaliar a capacidade de acesso e acessibilidade dos artefatos do documento. Os critérios associados são listados na tabela 3.

Tabela 3 – Critérios relacionados a acessibilidade da política e fontes.

Critério	Descrição	Fonte
A aplicação apresenta a Política de Privacidade no momento que o usuário acessa a plataforma?	Para esse critério é necessário avaliar se o usuário consegue ter acesso à Política de Privacidade por meio de um link externo ou um *pop-up* assim que ele entra na aplicação.	[10, 19, 25, 27]
Quão fácil é para o usuário encontrar a Política de Privacidade na aplicação?	Local onde o link para a Política de Privacidade está alocado e qual a visibilidade dele para o usuário.	[10, 19, 25, 27]
O documento está devidamente traduzido para todas as línguas que a aplicação suporta?	É necessário que a Política de Privacidade da aplicação esteja corretamente escrita e traduzida para todos os idiomas que a aplicação dá suporte. Isso vai garantir que o documento passe credibilidade para o usuário confiar suas informações pessoais à organização.	[3, 7, 9, 12, 32]
A Política de Privacidade é acessível para Pessoas Com Deficiência (PCD)?	O texto do documento deve apresentar ajustes visuais, como aumento e diminuição da fonte do texto ou ajuste de cores, para auxiliar a leitura de usuários com baixa visão. Outra opção é incluir leitores de tela automatizados, por meio de voz sintetizada, que leem o conteúdo da Política e expõem para o usuário.	[10, 16, 19, 46]
O documento apresenta um nível de legibilidade compatível com o que os usuários da aplicação conseguem ler?	A Política de Privacidade precisa ser lida e compreendida pelos usuários da aplicação, não deve ser uma leitura demorada e	[4, 14, 17, 21, 39, 47]

	cansativa. Deve-se evitar o uso de termos técnicos e difíceis de entender. Existem ferramentas automatizadas que medem o nível de legibilidade do texto e podem auxiliar nesse controle.	
O documento é responsivo?	É necessário que a Política esteja disponível em dispositivos com diferentes tamanhos de tela, seja *desktop* ou *mobile*.	[1, 20, 21, 34]
O documento apresenta uma boa usabilidade em dispositivos com diferentes tamanhos de tela?	A experiência do usuário ao ler a Política de Privacidade deve ser boa, inclusive em dispositivos móveis. É preciso ter cuidado com o tamanho da fonte e tamanho do documento. Como muitos usuários acessam aplicações através do celular deve-se levar em consideração esse tamanho de tela para a escrita da política.	[1, 20, 21, 34]

4.2 Conteúdo da Política de Privacidade

O objetivo dessa categoria é avaliar a Política de Privacidade em relação ao seu conteúdo. Os critérios associados a essa categoria são listados na tabela 4.

Tabela 4 – Critérios relacionados ao conteúdo da política e fontes.

Critério	Descrição	Fonte
A Política de Privacidade se baseia no pressuposto de que a visita à aplicação implica no consentimento do usuário à Política, independente do usuário ler o documento ou não?	É necessário que o usuário confirme ativamente que está de acordo com as práticas de coleta de dados da aplicação, não basta considerar que o usuário confirma os termos de uso se ele apenas utiliza a aplicação.	[2, 5, 6, 11, 30]
A Política específica claramente quais dados são coletados?	É importante que a Política de Privacidade detalhe claramente quais dados serão coletados pela aplicação. Os dados coletados se dividem em categorias bem definidas e a	[13, 18, 22, 23, 24, 32]

	Política deve indicar essas áreas. As seguintes categorias merecem destaque: 1. Informações do dispositivo: identificador do dispositivo, endereço de IP, sistema operacional, cookies; 2. Informações não-sensíveis que não identifique o usuário: Gênero, idade e demais interesses não sensíveis; 3. Informações sensíveis que não identifiquem o usuário: Raça, religião, orientação sexual, condições de saúde, saldo bancário; 4. Informações que identifiquem o usuário: Nome, contato pessoal; 5. Dados de geolocalização: Coordenadas de GPS, localização aproximada de WiFi	
A Política específica claramente como os dados são coletados?	A Política precisa expressar com clareza quais ferramentas a aplicação utiliza para coletar dados.	[13, 18, 22, 23, 24, 32]
A Política específica claramente se a aplicação faz o uso de alguma ferramenta ou serviço externo?	Caso seja utilizado algum serviço externo, é necessário que se tenha um link para a Política de Privacidade dessa ferramenta terceira.	[8,16, 18, 22, 24]
A Política de Privacidade específica claramente como a empresa pode usar os dados coletados?	A Política deve indicar qual o propósito da coleta de informações dos usuários. É necessário afirmar, por exemplo, se os dados estão sendo coletados para contactar o usuário, melhorar os serviços fornecidos, análise e monitoramento durante o uso da aplicação, personalizar a experiência, publicidade direcionada, entre outras ações.	[8, 13, 16, 18, 22, 24, 32]
A Política de Privacidade claramente especifica se as informações podem ser	Caso envolva terceiros, é necessário descrever que tipo de informações são compartilhadas, quem são os	[13, 18, 22, 24, 32]

compartilhadas ou vendidas para terceiros?	terceiros e como os terceiros podem ser classificados, além de estar anexada a Política de Privacidade dessa empresa terceira. É necessário afirmar também caso não haja o compartilhamento com outras organizações.	
A Política de Privacidade claramente especifica se o fornecimento dos dados solicitados é voluntário ou obrigatório, bem como as consequências de uma recusa em fornecer as informações solicitadas?	Este critério busca avaliar se a Política de Privacidade é flexível. Isto é, o que acontece caso o usuário opte por não fornecer determinada informação. Por exemplo, há aplicações que utilizam diversas ferramentas do smartphone como microfone, GPS, acesso à lista de contatos. Se o usuário optar por não querer que a aplicação acesse sua a lista de contatos a aplicação deve idealmente fornecer algum tipo de flexibilidade para a escolha do usuário, em especial quando este tipo de acesso não é crucial para a funcionalidade ao qual o aplicativo se propõe.	[15, 18]
A política de privacidade claramente especifica quais são as medidas adotadas pela aplicação para garantir a confidencialidade, a integridade e a qualidade dos dados?	Este critério busca avaliar se a aplicação possui algum método para garantir a confidencialidade e integridade dos dados do usuário. Por exemplo, se o armazenamento dos dados é criptografado ou alguma máscara de IP é utilizada.	[8, 13, 18, 22, 42]
A política de privacidade claramente específica como os dados são armazenados?	Ao informar como os dados são armazenados a empresa passa uma maior credibilidade para seus usuários.	[8, 13, 18, 22, 42]
A política de privacidade menciona estar de acordo com a lei vigente?	A política deve trazer explicitamente se está de acordo com alguma lei de privacidade e indicar qual lei é essa.	[13, 18, 22, 35, 36, 48]
A política menciona sobre o acesso de pessoas menores de idade?	Caso a aplicação permita o acesso a pessoas menores de idade, é preciso que a	[37, 43]

	política de privacidade aborda esse tema.	
A política trata questões relacionadas à privacidade de crianças?	É necessário que a Política explique claramente como se dá questões relacionadas à privacidade com crianças que acessam a aplicação.	[37, 43]
A política explica claramente o que acontece com os dados do usuário caso ele exclua a conta?	É importante que esteja descrito na política o que acontece caso o usuário se desvincule da aplicação.	[18, 28, 29]

4.3 Participação do usuário

O objetivo dessa categoria é avaliar a Política de Privacidade sobre a participação do usuário no documento. Os critérios associados a essa categoria são listados na tabela 5.

Tabela 5 – Critérios relacionados a participação do usuário e fontes.

Critério	Descrição	Fonte
O usuário tem liberdade para acessar os dados sobre si mesmo armazenados pela aplicação?	É uma boa prática permitir que o usuário visualize os dados armazenados pela aplicação. Assim, os usuários podem contestar a precisão e a integridade desses dados.	[18, 44, 45]
A política de privacidade claramente especifica os direitos do usuário?	As leis de privacidade apresentam direitos que os usuários possuem. É uma boa prática que a política descreva esses direitos em relação a seus dados pessoais.	[13, 22, 35, 38]
A política de privacidade claramente informa dados para contato com a empresa?	Idealmente deve haver o contato da área da empresa que trate de questões de privacidade dos dados de seus usuários.	[13, 26, 32]

4.4 Alterações na Política e Privacidade

O objetivo dessa categoria é avaliar a Política de Privacidade sobre práticas executadas em eventuais alterações no documento. Os critérios associados a essa categoria são listados na tabela 6.

Tabela 6 – Critérios relacionados a alterações na política de privacidade e fontes.

Critério	Descrição	Fonte
Como as alterações nas políticas são tratadas?	Após uma eventual alteração na política de privacidade, os usuários precisam ser informados e notificados sobre isso.	[31, 32, 39, 44]
Qual carga uma alteração de política de privacidade a aplicação impõe ao usuário?	Os usuários são induzidos a ler a nova versão da política de privacidade? Uma boa prática é quando o usuário entrar na aplicação ele ser redirecionado a uma página demonstrando de forma clara a comparação entre a versão antiga e a nova do documento.	[31, 32, 39]
Como se dá a frequência de modificação da política de privacidade?	Mudanças constantes na política de privacidade faz com que a empresa perca a credibilidade do usuário.	[31, 32, 39]

4.5 Consentimento e Permissão do usuário

O objetivo dessa categoria é avaliar a Política de Privacidade quanto a forma de consentimento do usuário e permissão. Os critérios associados a essa categoria são listados na tabela 7.

Tabela 7 – Critérios relacionados ao consentimento e permissão do usuário e fontes.

Critério	Descrição	Fonte
Qual o método de escolha do usuário para consentimento ou não com a política de privacidade?	O usuário deve marcar ativamente que está de acordo com a Política de Privacidade da aplicação. Como em um formato de *opt-in,* por exemplo.	[5, 18, 39, 40, 41]
O usuário tem a opção de não concordar com a Política de Privacidade da aplicação?	A aplicação deve tratar o fato do usuário possivelmente	[5, 18, 23, 33, 41]

	não concordar com a Política de Privacidade.	
É permitido que o usuário selecione qual informação ele permite ser coletada?	É uma boa prática que o usuário selecione quais informações ele permite ser coletada e que a aplicação trate cada um dos casos caso o usuário não aceite que determinada informação seja coletada.	[18, 23, 33, 41]

O catálogo desenvolvido está disponível nesse link. No site é possível ver os critérios agrupados por categorias e uma breve descrição de cada um, como mostra as figuras 4 e 5.

Figura 4 – Catálogo de critérios para avaliação de políticas de privacidade site - categorias.

Fonte: O autor.

Figura 5 – Catálogo de critérios para avaliação de políticas de privacidade site critérios.

Fonte: O autor.

5. Conclusões

Muitos usuários de aplicativos e websites têm levantado o questionamento sobre quão seguras suas informações estão sob o domínio das empresas que realizam o processamento de seus dados [1]. Nesse contexto, diversas leis que visam regulamentar e fortalecer as práticas de segurança e privacidade de dados pessoais por parte das empresas surgiram.

As leis de privacidade requerem que as empresas sejam claras quanto à finalidade da coleta, hipóteses de tratamento de dados, existência de compartilhamento com outras empresas entre outras informações. A disponibilização dessas informações para o usuário deve ocorrer por meio de um documento legal denominado “Política de Privacidade”. O documento possui o intuito de informar aos usuários sobre as práticas de coleta e processamento de dados pessoais nas aplicações.

Entretanto, pesquisas [18, 19, 20] mostram que as Políticas de Privacidade dificilmente são lidas pelos usuários. Isso acontece porque esses documentos normalmente são longos, apresentam um nível de legibilidade elevado e possuem uma natureza prolixa e ambígua, com muitos termos técnicos. Trabalhos anteriores [13, 14, 21] também constataram que muitas Políticas de Privacidade não refletem a real prática de coleta de dados da organização ou não apresentam todas as informações necessárias relacionadas à privacidade dos usuários. Isso é um problema pois os órgãos reguladores podem aplicar multas severas em organizações cuja Política de Privacidade não está de acordo com a lei de privacidade vigente.

Sendo assim, este trabalho apresentou um catálogo de critérios de avaliação de Políticas de Privacidade com o intuito de auxiliar no processo de construção do documento. O catálogo foi desenvolvido após o estudo de um conjunto de 48 artigos que fazem avaliação de Políticas de Privacidade. A construção do catálogo ocorreu por meio da aplicação da técnica de *snowballing*, que consistiu em coletar novos artigos a partir de um conjunto inicial de trabalhos publicados, considerando as referências e as citações deles, sendo, portanto, um método sistemático de revisão da literatura.

5.1 Contribuições da pesquisa

O catálogo de critérios de avaliação de políticas de privacidade é um corpo de conhecimento sobre o tema abordado que agrega diversas visões de diferentes autores da área. Portanto, espera-se atingir benefícios diferentes ao utilizar o catálogo proposto dependendo do público-alvo:

- Os redatores de políticas de privacidade podem se basear neste trabalho para a criação de documentos mais completos e corretos, que apresentem informações referentes a diversos aspectos contemplados em leis de privacidade;
- Os analistas e os responsáveis pela aplicação também se beneficiam com esse trabalho, pois fica mais claro para eles quais informações devem ser devidamente documentadas sobre a prática de coleta de dados;

- Os usuários finais também podem utilizar o catálogo criado para verificar se a aplicação possui boas práticas ao redigir a Política de Privacidade e tirar eventuais dúvidas sobre a necessidade de inclusão de uma determinada informação;
- A comunidade acadêmica pode utilizar o catálogo desenvolvido como forma de aprender boas práticas relacionadas à especificação do tratamento de dados pessoais.

5.2 Trabalhos Futuros

A partir da condução deste trabalho e dos resultados obtidos, os seguintes direcionamentos para novos trabalhos são propostos:

- Realizar uma validação do catálogo desenvolvido com especialistas de Privacidade e leis de Privacidade;
- Avaliar Políticas de Privacidade de empresas e companhias com os critérios descritos no catálogo;
- Ampliar as buscas de critérios de avaliação de Políticas de Privacidade, utilizando outros artigos existentes no meio acadêmico;
- Desenvolver uma ferramenta para avaliação automática de Políticas de Privacidade com os critérios descritos neste catálogo utilizando técnicas de *machine learning* e processamento de linguagem natural.

Referências

[1] - DEMARTINI, Felipe. Brecha expõe 1,7 bilhão de registros da plataforma brasileira de e-commerce.

[2] - FRANCO, Marcela. Estudo revela os aplicativos que coletam mais dados de usuários. Techtudo, 2021. Disponível em: https://www.techtudo.com.br/noticias/2021/03/estudo-revela-os-aplicativos-que-coletam-mais-dados-de-usuarios-entenda.ghtml. Acesso em: 18/11/2021.

[3] - MARTINS, Mendes. O Marketing digital tende a crescer mais de 80% em 2022. Adnews, 2021. Disponível em: https://adnews.com.br/assim-como-em-2020-o-marketing-digital-sera-tendencia-ate-2022/. Acesso em 18/11/2021.

[4] - MONTE, Leonardo. As principais estratégias da Amazon e como ela pode acabar com sua empresa no Brasil. Administradores, 2018. Disponível em: https://administradores.com.br/noticias/as-principais-estrategias-da-amazon-e-como-ela-pode-acabar-com-sua-empresa-no-brasil. Acesso em 18/11/2021.

[5] - Wobbrock, Jacob O., Andrew D. Wilson, and Yang Li. "Gestures without libraries, toolkits or training: a $1 recognizer for user interface prototypes." *Proceedings of the 20th annual ACM symposium on User interface software and technology*. 2007.

[6] - LEMOS, Robert. Citizens are increasingly worried about how companies use their data. Darkreading, 2020. Disponível em: https://www.darkreading.com/privacy/citizens-are-increasingly-worried-about-how-companies-use-their-data. Acesso em 18/11/2021.

[7] - Uber announces new data breach. NortonLifeLock, 2021. Disponível em: https://uk.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html. Acesso em 18/11/2021.

[8] - Turow, Joseph, et al. "The federal trade commission and consumer privacy in the coming decade." *ISJLP* 3 (2007): 723.

[9] - WebsitePolicies, 2019.

[10] - Singh, Ravi Inder, Manasa Sumeeth, and James Miller. "Evaluating the readability of privacy policies in mobile environments." *International Journal of Mobile Human Computer Interaction (IJMHCI)* 3.1 (2011): 55-78.

[11] - Miller, J, 2016. Evaluating the Readability of Privacy Policies.

[12] - Acquisti, Alessandro, and Jens Grossklags. "Privacy attitudes and privacy behavior." *Economics of information security*. Springer, Boston, MA, 2004. 165-178.

[13] - Jenssen, Carlos, 2004.

[14] - McDonald, Aleecia M., and Lorrie Faith Cranor. "The cost of reading privacy policies." *Isjlp* 4 (2008): 543.

[15] - (Vila et al., 2003;)

[16] - Reay, Ian, Scott Dick, and James Miller. "A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations." *ACM Transactions on the Web (TWEB)* 3.2 (2009): 1-34.
[17] - Saiba o que acontece se sua empresa descumprir a LGPD. Stefanini Group, 2019. Disponível em: https://stefanini.com/pt-br/trends/artigos/saiba-o-que-acontece-se-sua-empresa-descumprir-a-lgpd. Acesso em 18/11/2021.
[18] - J. Graber, D. D'Alessandro, and J. Johnson-West, "Reading level of privacy policies on Internet health websites," J. Family Practice, vol. 51, no. 7, pp. 642-645, 2002.
[19] - S.D. Lewis, R.G. Colvard, and N.C. Adams, "A comparison of the readability of privacy statements of banks, credit counseling companies, and check cashing companies," J. Organizational Culture, Communication & Conflict, vol. 12, no. 2, pp. 87-93, 2008.
[20] - Barbara Krumay(B) and Jennifer Klar. "Readability of Privacy Policies", 2020
[21] - Sherali Zeadally and Stephanie Winkler. "Privacy Policy Analysis of Popular Web Platforms", 2016
[22] - Keilla Costa, 2016
[23] - (ARENDT, 2007)
[24] - (Pires Neto, 2008)
[25] - Privacidade na internet é um mito, afirma Luli Radfahrer. 2016. http://jornal.usp.br/atualidades/privacidade-na-internet-e-um-mito-afirma-luli-radfahrer. Acesso em 20/11/2021
[26] - Warren, Samuel, and Louis Brandeis. "The right to privacy." *civilistica. com* 2.3 (2013): 1-22.
[27] - Sales, Fábio Augusto Cornazzani, GTr LIMA, and RBarros de MIRANDA. "Privacidade e Internet." *Revista de Direito das*.
[28] - Marcelino, Luis, and Catarina Silva. "Location privacy concerns in mobile applications." *Developments and advances in intelligent systems and applications*. Springer, Cham, 2018. 241-249.
[29] - Coupofy (2016) Study: How millennials consume news & social media on their smartphones. Retrieved from
[30] - Wisniewski, Pamela, et al. "F acebook apps and tagging: The trade-off between personal privacy and engaging with friends." *Journal of the Association for Information Science and Technology* 66.9 (2015): 1883-1896.
[31] - Anderson, Patrick D. "Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange." *Ethics and Information Technology* (2020): 1-14.
[32] - Baik. Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA)
[33] - O novo conceito de consetimento para tratamento de dados pessoais da LGPD - Disponível em: https://ndmadvogados.jusbrasil.com.br/artigos/762892926/o-novo-conceito-de-

consentimento-para-tratamento-de-dados-pessoais-da-lgpd. Acesso em 20/11/2021.

[34] - Story, L. (2007, November 1). FTC to review online ads and privacy. TheNewYorkTimes. Retrieved from http://www.nytimes.com/

[36] - J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. M. McDonald, T. B. Norton, R. Ramanath, et al. Disagreeable privacy policies: Mismatches between meaning and usersŠ understanding. 2014.

[37] - M. Rowan and J. Dehlinger. Encouraging privacy by design concepts with privacy policy auto-generation in eclipse (page). In Proceedings of the 2014 Workshop on Eclipse Technology eXchange, pages 9–14. ACM, 2014.

[38] - Singh, R. I., Sumeeth, M., & Miller, J. (2011). Evaluating the Readability of Privacy Policies in Mobile Environments. International Journal of Mobile Human Computer Interaction

[40] - Slavin, Wang - “Toward a Framework for Detecting Privacy Policy Violations in Android Application Code”

[41] - Jenssen, Pots - “Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices”

[42] - Karjoth, Günter, and Matthias Schunter. "A privacy policy model for enterprises." *Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15*. IEEE, 2002.

[43] - House, Stirling. "Privacy Policy." *White House* (2020)..

[44] - Tavani, Herman T. "Philosophical theories of privacy: Implications for an adequate online privacy policy." *Metaphilosophy* 38.1 (2007): 1-22.

[45] - Claes Wohlin - “Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering”

[46] - LEITE, Henrique Specian. The Importance of Privacy on the Internet. 2016.

[47] - Z. Papacharissi and J. Fernback, “Online privacy and consumer protection: An analysis of portal privacy statements,” J. Broadcasting & Electronic Media, vol. 43, no. 3, pp. 259-281, 2015.

[48] - Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em 22/11/2021.

[49] - O que é web scraping e como ocorre? Disponível em: https://canaltech.com.br/seguranca/o-que-e-web-scraping/. Acesso em 22/11/2021.

[50] - Cinco estratégias de Jeff Bezos que fizeram da Amazon uma das empresas de maior sucesso da história. Disponível em: https://www.infomoney.com.br/negocios/cinco-estrategias-de-jeff-bezos-que-fizeram-da-amazon-uma-das-empresas-de-maior-sucesso-da-historia/. Acesso em 22/11/2021.

[51] - 10 coisas que você precisa saber sobre a Lei Geral de Proteção de Dados. Disponível em: https://www.juridoc.com.br/fr/blog/noticias/8289-10-coisas-que-voce-precisa-saber-sobre-a-lei-geral-de-protecao-de-dados/. Acesso em 22/11/2021.

[52] - Tepedino, Gustavo. “Desafios da Lei Geral de Proteção de Dados.”

[53] - França multa Google e Amazon por violação de lei de privacidade - Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/10/franca-multa-google-e-amazon-por-por-violacao-de-lei-de-privacidade.ghtml

[54] - 8 casos de vazamentos de dados tratados com a LGPD. Disponível em: https://www.softwall.com.br/blog/vazamentos-de-dados-tratados-com-a-lgpd/.

[55] - We Read 150 Privacy Policies. They were an Incomprehensible Disaster. Disponível em: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

[56] - The Average Reading Level of a Privacy Policy. Disponível em: https://www.varonis.com/blog/gdpr-privacy-policy/. Acesso em: 22/11/2021.

[57] - The Privacy Foundation. EEOC v. Burlington Northern Santa Fe Railroad. Available at: http://www.privacyfoundation.org/legal/case/show.asp?id=25&t=2. Acessado em Maio de 2002.

[58] - Definição catálogo. Disponível em: https://www.dicio.com.br/catalogo/. Acesso em 28/11/2021.

[59] - Rozeno, Cristiana. Catálogo de dados dos trabalhos científicos de gestão ambiental e saúde da Escola Nacional de Saúde Pública Sérgio Arouca (ENSP/FIOCRUZ).

[60] - M.Peixoto, C. Silva, H. Maia. Towards a Catalog of Privacy Related Concepts.

[61] - H. Precht, S. Wunderlich, J. Gómez. Applying Software Quality Criteria to Blockchain Applications: A Criteria Catalog.

[62] - J. Saraiva, S. Soares, F. Castor. Towards a Catalog of Object-Oriented Software Maintainability Metrics.

[63] - Assembleia Geral da ONU. (1948). "Declaração Universal dos Direitos Humanos"

[64] - Thomson on Privacy. Author(s): Thomas Scanlon. Source: Philosophy and Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 315-322.

[65] - Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change*, *167*, 120681

[66] - BRASIL. Constituição (1988). Constituição da República Federativa do Brasil.

[67] - Apple é a marca mais valiosa do mundo pelo 6º ano, diz Forbes. Disponível em: http://g1.globo.com/economia/midia-e-marketing/noticia/2016/05/apple-e-marca-mais-valiosa-do-mundo-pelo-6-ano-diz-forbes.html

[68] - Google fatura US $4,7 bilhões da indústria de notícias e jornais questionam. Disponível em: https://acontecendoaqui.com.br/propaganda/google-fatura-us-47-bilhoes-da-industria-de-noticias-e-jornais-questionam

[69] - Data brokers e a comercialização dos dados pessoais. Disponível em: https://emporiododireito.com.br/leitura/os-data-brokers-e-a-comercializacao-dos-dados-pessoais

[70] - Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, *3*(2), 405-413.

[71] - Why should developers care about privacy. Disponível em: https://xmode.io/why-should-developers-care-about-privacy/

[72] - How many websites are there? Disponível em: https://websitesetup.org/news/how-many-websites-are-there/#:~:text=It's%20estimated%20that%20over%201.7,world%20contribute%20with%20online%20interactions.

[73] - GDPR - European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council.

[74] - 2019. BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD).

[75] - CCPA - California Consumer Privacy Act (CCPA).

[76] - CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2000/C 364/01).

[77] - Proteção de dados: cenário mundial das leis. Disponível em: https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/

[78] - SEU CONSENTIMENTO É LEI! - Disponível em: https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei

[79] - O que é opt-in? Disponível em: https://neilpatel.com/br/blog/opt-in-o-que-e/

[80] - de Teffé, C. S., Viola, M. (2020). Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica. com*, *9*(1), 1-38.

[81] - Worldwide Data Privacy Regulations Compared - NetApp.

[82] - GDPR: Approaches for Protecting Personally Identifiable Information (PII) and Sensitive Personal Information (SPI). Disponível em: https://www.intelisecure.com/gdpr-approaches-for-protecting-personally-identifiable-information-pii-and-sensitive-personal-information-spi/

[83] - Ur, Blase, Manya Sleeper, and Lorrie Faith Cranor. "{Privacy, Privacidad, Приватност} policies in social media: Providing translated privacy notice." Proceedings of the 1st Workshop on Privacy and Security in Online Social Media. 2012.

[84] - What to Include in Your Website's Privacy Policy - Disponível em: https://www.nolo.com/legal-encyclopedia/what-to-include-in-your-website-s-

privacy-
policy.html#:~:text=Your%20policy%20should%20disclose%20that,email%20addresses%2C%20and%20so%20forth.
[85] - Carvalho, Rainara Maia, Rossana Maria de Castro Andrade, and Káthia Marçal de Oliveira. "Catalog of invisibility correlations for UbiComp and IoT applications." *Requirements Engineering* (2021): 1-34.
[86] - Chung L, Nixon BA, Yu E, Mylopoulos J (2000) Non-functional requirements in software engineering, vol 5. Springer Science and Business Media, New York
[87] - Carvalho, Thaís Abreu. "Aplicabilidade da lei geral de proteção de dados e da metodologia" privacy by design" nos termos de uso e de política de privacidade." (2019).

APÊNDICE A – Artigos selecionados para extração de critérios de avaliação de políticas de privacidade

ID	Artigo	Referência
1	A Privacy Policy Comparison of Health and Fitness Related Mobile Applications	Rowan, M., & Dehlinger, J. (2014). A privacy policy comparison of health and fitness related mobile applications. *Procedia Computer Science*, *37*, 348-355.
2	Comparing Privacy Policies of Government Agencies and Companies: A Study using Machine-learning-based Privacy Policy Analysis Tools	Zaeem, R. N., & Barber, K. S. (2021). Comparing Privacy Policies of Government Agencies and Companies: A Study using Machine-learning-based Privacy Policy Analysis Tools. In *ICAART (2)* (pp. 29-40).
3	{Privacy, Privacidad, Приватност } Policies in Social Media: Providing Translated Privacy Notice	Ur, B., Sleeper, M., & Cranor, L. F. (2012, April). {Privacy, Privacidad, Приватност} policies in social media: Providing translated privacy notice. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media* (pp. 1-4).
4	Large-Scale Readability Analysis of Privacy Policies	Fabian, B., Ermakova, T., & Lentz, T. (2017, August). Large-scale readability analysis of privacy policies. In *Proceedings of the international conference on web intelligence* (pp. 18-25).
5	PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining	Zaeem, R. N., German, R. L., & Barber, K. S. (2018). Privacycheck: Automatic summarization of privacy policies using data mining. *ACM Transactions on Internet Technology (TOIT)*, *18*(4), 1-18.
6	A study of web privacy policies across industries	Nokhbeh Zaeem, R., & Barber, K. S. (2017). A study of web privacy policies across industries. *Journal of Information Privacy and Security*, *13*(4), 169-185.
7	Privacy Policy Practices on New Zealand Websites.	Tjhin, I., Vos, M., & Munaganuri, S. (2016). Privacy Governance Online: Privacy Policy Practices on New Zealand Websites.
8	Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies	Fernback, J., & Papacharissi, Z. (2007). Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. *New Media & Society*, *9*(5), 715-734.
9	China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent	Fu, T. (2019). China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent. *Global Media and Communication*, *15*(2), 195-213.
10	Examining Usability of Web Privacy Policies	Proctor, R. W., Ali, M. A., & Vu, K. P. L. (2008). Examining usability of web privacy policies. *Intl. Journal of Human–Computer Interaction*, *24*(3), 307-328.
11	Are They Actually Any Different? Comparing	Cranor, L. F., Idouchi, K., Leon, P. G., Sleeper, M., & Ur, B. (2013, June). Are they actually any different?

	Thousands of Financial Institutions' Privacy Practices	Comparing thousands of financial institutions' privacy practices. In *Proc. WEIS* (Vol. 13).
12	A study on privacy concerns across social networking sites: An Indian perspective	BHANDARI, R. S., & BANSAL, S. A study on privacy concerns across social networking sites: An Indian perspective.
13	A Longitudinal Study of Google Privacy Policies	Peslak, A., Kovalchick, L., & Conforti, M. (2020). A Longitudinal Study of Google Privacy Policies. *Journal of Information Systems Applied Research*.
14	A Longitudinal Assessment of Online Privacy Notice Readability	Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238-249.
15	In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites	Sheehan, K. B. (2005). In poor health: an assessment of privacy policies at direct-to-consumer web sites. *Journal of Public Policy & Marketing*, *24*(2), 273-283.
16	The Complexity of Mental Health App Privacy Policies:A Potential Barrier to Privacy	Powell, A., Singh, P., & Torous, J. (2018). The complexity of mental health app privacy policies: A potential barrier to privacy. *JMIR mHealth and uHealth*, *6*(7), e158.
17	Readability of Privacy Policies of Healthcare Websites	Ermakova, T., Fabian, B., & Babina, E. (2015). Readability of Privacy Policies of Healthcare Websites. *Wirtschaftsinformatik*, *15*, 1-15.
18	Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies	Cranor, L. F., Hoke, C., Leon, P., & Au, A. (2014, March). Are they worth reading? An in-depth analysis of online advertising companies' privacy policies. In *2014 TPRC Conference Paper*.
19	An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies	Vail, M. W., Earp, J. B., & Antón, A. I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, *55*(3), 442-454.
20	Prominent issues for privacy establishment in privacy policies of mobile apps	Yamauchi, E. A., de Souza, P. C., & Junior, D. P. (2016, October). Prominent issues for privacy establishment in privacy policies of mobile apps. In *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems* (pp. 1-9).
21	Evaluating the Readability of Privacy Policies in Mobile Environments	Singh, R. I., Sumeeth, M., & Miller, J. (2011). Evaluating the readability of privacy policies in mobile environments. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, *3*(1), 55-78.
22	Analyzing privacy policies based on a privacy-aware profile: The Facebook and LinkedIn case studies	Caramujo, J., & Da Silva, A. M. R. (2015, July). Analyzing privacy policies based on a privacy-aware profile: The Facebook and LinkedIn case studies. In *2015 IEEE 17th Conference on Business Informatics* (Vol. 1, pp. 77-84). IEEE.
23	Privacy issues and solutions in social network sites	Chen, X., & Michael, K. (2012). Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine*, *31*(4), 43-53.
24	Privacy compliance risks for Facebook	Johnston, A., & Wilson, S. (2012). Privacy compliance risks for Facebook. *IEEE Technology and Society Magazine*, *31*(2), 59-64.

25	Do web privacy policies still matter?	Malaga, R. A. (2014). Do web privacy policies still matter?. *Journal of Management Information and Decision Sciences*, *17*(1), 95.
26	Online privacy: Overview and preliminary research	Mekovec, R. (2010). Online privacy: overview and preliminary research. *Journal of information and organizational sciences*, *34*(2), 195-209.
27	Online privacy and consumer protection: An analysis of portal privacy statements	Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media*, *49*(3), 259-281.
28	A typology of communicative strategies in online privacy policies: Ethics, power and informed consent	Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, *62*(3), 221-235.
29	A review and an empirical analysis of privacy policy and notices for consumer Internet of things	Perez, A. J., Zeadally, S., & Cochran, J. (2018). A review and an empirical analysis of privacy policy and notices for consumer Internet of things. *Security and Privacy*, *1*(3), e15.
30	RSL-IL4Privacy: a domain-specific language for the rigorous specification of privacy policies	Caramujo, J., da Silva, A. R., Monfared, S., Ribeiro, A., Calado, P., & Breaux, T. (2019). RSL-IL4Privacy: a domain-specific language for the rigorous specification of privacy policies. *Requirements Engineering*, *24*(1), 1-26.
31	Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram	Soumelidou, A., & Tsohou, A. (2019). Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram. *Information Technology & People*.
32	Users' privacy at online social networks in Indian context: comprehensive multiaged group survey and discussion	Ashetakr, R., Mahalle, P. N., & Shinde, G. R. (2019). 5. Users' privacy at online social networks in Indian context: comprehensive multiaged group survey and discussion. In *The Internet of Everything* (pp. 95-108). De Gruyter.
33	Privacy policy annotation for semi-automated analysis: a cost-effective approach	Audich, D. A., Dara, R., & Nonnecke, B. (2018, July). Privacy policy annotation for semi-automated analysis: a cost-effective approach. In *IFIP International Conference on Trust Management* (pp. 29-44). Springer, Cham.
34	Analyzing privacy policies of zero knowledge cloud storage applications on mobile devices	Baalous, R., Poet, R., & Storer, T. (2018, April). Analyzing privacy policies of zero knowledge cloud storage applications on mobile devices. In *2018 IEEE International Conference on Cloud Engineering (IC2E)* (pp. 218-224). IEEE.
35	"Take it or leave it": Effective visualization of privacy policies	Dhotre, P. S., Bihani, A., Khajuria, S., & Olesen, H. (2017). take it or leave it": Effective visualization of privacy policies. *Cybersecurity and Privacy. River Publishers*, 39-64.
36	Is Privacy Dead? Does it Matter?	Boatwright, B. C., & White, C. (2020). Is Privacy Dead? Does it Matter?. *The Journal of Public Interest Communications*, *4*(1), 78-78.
37	Agents presenting themselves as Strangers	Zwart, N. A. (2021). *Agents presenting themselves as Strangers duringPrivacy Permission Requests:*

	duringPrivacy Permission Requests: Effects on Disclosureand Privacy Awareness of Children	*Effects on Disclosureand Privacy Awareness of Children* (Master's thesis, University of Twente).
38	Lattice-based Contextual Integrity Analysis of Social Network Privacy Policies	Kaplan, S., Bulmer, D., Gosselin, A., & Ghanavati, S. (2021, September). Lattice-based Contextual Integrity Analysis of Social Network Privacy Policies. In *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)* (pp. 394-399). IEEE.
39	Privacy policies and users' trust: does readability matter?	Ermakova, T., Baumann, A., Fabian, B., & Krasnova, H. (2014, August). Privacy policies and users' trust: does readability matter?. In *AMCIS*.
40	Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site	Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial management & data Systems*.
41	Privacy regulation and online advertising.	Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management science*, *57*(1), 57-71.
42	The effect of online privacy policy on consumer privacy concern and trust.	Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, *28*(3), 889-897.
43	Fixing broken doors: strategies for drafting privacy policies young people can understand.	Micheti, A., Burkell, J., & Steeves, V. (2010). Fixing broken doors: Strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology & Society*, *30*(2), 130-143.
44	Examining Internet privacy policies within the context of user privacy values.	Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, *52*(2), 227-237.
45	The Lack of Clarity in Financial Privacy Policies and the Need for Standardization.	Anton, A., Earp, J. B., Bolchini, D., He, Q., Jensen, C., & Stufflebeam, W. (2003). The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. North Carolina State University Technical Report# TR-2.
46	A comparative study of online privacy policies and formats.	McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009, August). A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium* (pp. 37-55). Springer, Berlin, Heidelberg.
47	Defining Privacy: How Users Interpret Technical Terms in Privacy Policies.	Tang, J., Shoemaker, H., Lerner, A., & Birrell, E. (2021). Defining Privacy: How Users Interpret Technical Terms in Privacy Policies. *Proc. Priv. Enhancing Technol.*, *2021*(3), 70-94.
48	CompLicy: Evaluating the GDPR Alignment of Privacy Policies-A Study on Web Platforms	CompLicy: Evaluating the GDPR Alignment of Privacy Policies-A Study on Web Platforms