PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Programa de Pós-Graduação em Informática

Daphne Fernanda Freitas Bueno de Carvalho

IDENTIFICAÇÃO E ANÁLISE DE HEURÍSTICAS DE PRIVACIDADE DA DIVULGAÇÃO DE DADOS DE USUÁRIOS DE REDES SOCIAIS

Belo Horizonte

2022

Daphne Fernanda Freitas Bueno de Carvalho

IDENTIFICAÇÃO E ANÁLISE DE HEURÍSTICAS DE PRIVACIDADE DA DIVULGAÇÃO DE DADOS DE USUÁRIOS DE REDES SOCIAIS

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Mestre em Informática.

Orientador: Prof. Dr. Humberto Torres Marques Neto

Área de Concentração: Ciência da Computação

Belo Horizonte

2022

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Carvalho, Daphne Fernanda Freitas Bueno de
C331i Identificação e análise de heurísticas de privacidade da divulgação de dados de usuários de redes sociais / Daphne Fernanda Freitas Bueno de Carvalho. Belo Horizonte, 2022.
101 f. : il.

Orientador: Humberto Torres Marques Neto

Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática

1. Brasil. Lei geral de proteção de dados (2018). 2. Dados pessoais. 3. Segurança de dados. 4. Direito à privacidade. 5. Redes sociais on-line. 6. Algoritmos. 7. Heurística. 8. Divulgação de informação. I. Marques Neto, Humberto Torres. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática. III. Título.

SIB PUC MINAS

CDU: 681.3.055

Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Daphne Fernanda Freitas Bueno de Carvalho

IDENTIFICAÇÃO E ANÁLISE DE HEURÍSTICAS DE PRIVACIDADE DA DIVULGAÇÃO DE DADOS DE USUÁRIOS DE REDES SOCIAIS

Dissertação apresentada ao Programa de Pós-Graduação em Informática como requisito parcial para qualificação ao Grau de Mestre em Informática pela Pontifícia Universidade Católica de Minas Gerais.

Área de Concentração: Ciência da Computação

Professor Dr. Humberto Torres Marques Neto
PUC Minas (Orientador)

Professora Drª. Cristiane Neri Nobre
PUC Minas (Banca Examinadora)

Professora Drª. Maria da Graça Campos Pimentel
Universidade de São Paulo (Banca Examinadora)

Belo Horizonte, 30 Novembro de 2022.

À minha mãe, Marília Madalena de Freitas.

AGRADECIMENTOS

A todo corpo docente e funcionários da Pontifícia Universidade Católica de Minas Gerais — São Gabriel e Coração Eucarístico.

Ao meu orientador, Professor Dr. Humberto Torres Marques Neto, pelos ensinamentos ofertados durante todo o curso e especialmente pelo suporte, estando sempre disponível e disposto a ajudar durante todo este trabalho.

A Professora Dra. Cristiane Neri Nobre, pelos ensinamentos e parceria durante a realização deste estudo. Agradeço pelos conselhos e apoio recebido durante todo o curso.

Aos meus pais pelo amor e apoio. Agradeço muitíssimo a minha mãe, Marília Madalena de Freitas, maior incentivadora e apoiadora crucial para que eu conseguisse enfrentar os momentos de incerteza e pudesse chegar a alcançar o objetivo de ser Mestre em Informática.

Obrigada, em especial, a Giovana Cassia da Silva, que sempre me auxiliou com paciência e carinho!

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigada.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"You must never give in to despair.
Allow yourself to slip down that road,
and you surrender to your lowest instincts.

In the darkest times,
hope is something you give yourself.

That is the meaning of inner strength."

Iroh - Avatar: The Last Airbender

RESUMO

A privacidade tem sido frequentemente identificada como uma das principais preocupações durante o desenvolvimento de sistemas que lidam com informações pessoais. A ruptura da privacidade de um indivíduo pode ameaçar a sua autonomia, não apenas como consumidor, mas como cidadão. Por consequência, em diversos países têm sido sancionadas novas legislações que regulamentam a proteção de dados pessoais. No Brasil, foi sancionada a Lei Geral de Proteção de Dados Pessoais (LGPD), em agosto de 2018, para regulamentar a gestão da segurança da privacidade dos indivíduos. A proteção da privacidade tem sido uma questão desafiadora nas redes sociais *online*, como Facebook e Instagram. No entanto, apesar dos esforços regulatórios para proteger dados pessoais *online*, os usuários tendem a consentir em divulgar mais informações pessoais do que pretendem e tendem a revelar mais do que sabem. Com isso em mente, o objetivo principal deste estudo é identificar heurísticas que influenciam a divulgação de dados e realizar uma análise das heurísticas de privacidade nas redes sociais *online* Facebook e Instagram para identificar a presença dos fatores que influenciam a divulgação de informações do usuário e verificar o consentimento informado por meio da análise das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok. No Facebook e Instagram foram observadas uma quantidade notável de heurísticas que aumentam a divulgação de informações. No entanto, a heurística de "Intrusão" também foi detectada, violando o princípio do *Privacy by Design* (PbD) de "Privacidade como configuração padrão". Assim, compreender o número e a diversidade de sugestões (heurísticas) às quais os usuários estão suscetíveis permite a criação de diretrizes explícitas abordando questões de privacidade. A principal contribuição esperada é que com a realização deste trabalho de pesquisa identifiquem-se heurísticas específicas orientadas à privacidade que possam ajudar a comunidade de *design* e os engenheiros de *software* a projetar e desenvolver sistemas que apresentem pistas, sugestões e oportunidades para promover uma computação mais segura e confiável.

Palavras-chave: Privacidade, Heurística, Dados pessoais, Conformidade, Redes sociais, LGPD.

ABSTRACT

Privacy has often been identified as a major concern when developing systems that handle personal information. The disruption of an individual's privacy can threaten his autonomy, not just as a consumer, but as a citizen. As a result, in several countries, new laws have been approved that regulate the protection of personal data. In Brazil, the General Data Protection Law (LGPD) was sanctioned in August 2018 to legislate the management of individuals' privacy security. Privacy protection has been a challenging issue on online social networks such as Facebook and Instagram. However, despite regulatory efforts to protect personal data online, users tend to consent to disclosing more personal information than they intend and tend to reveal more than they know. With that in mind, the main objective of this study is to identify heuristics that influence data disclosure and to perform an analysis of privacy heuristics in the online social networks Facebook and Instagram to identify the presence of factors that influence the disclosure of user information and verify informed consent through the analysis of the privacy policies of the social networks Facebook, Instagram, Twitter, LinkedIn and TikTok. On Facebook and Instagram, a remarkable amount of heuristics were observed that increase the dissemination of information. However, the "Intrusion" heuristic was also detected, violating the Privacy by Design (PbD) principle of "Privacy as Default Setting". Thus, understanding the number and diversity of suggestions (heuristics) to which users are susceptible allows the creation of explicit guidelines addressing privacy issues. The main expected contribution is that with the realization of this research project, specific privacy-oriented heuristics will be identified that can help the design community and software engineers to design and develop systems that present clues, suggestions and opportunities to promote more efficient computing, safe and reliable.

Keywords: Privacy, Heuristic, Personal data, Compliance, Social networks, LGPD.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ACM	*Association for Computing Machinery*
ANPD	Autoridade Nacional de Proteção de Dados
APF	*Annual Privacy Forum*
ARES	*Availability, Reliability and Security*
BSI	*British Standards Institution*
CFTV	Circuito Fechado de Televisão
CTS	*Collaboration Technologies and Systems*
DFD	Diagrama de Fluxo de Dados
DPIA	*Data Protection Impact Assessment*
DPO	*Data Protection Officer*
EHS	*Environment, Health and Safety*
EJIS	*European Journal of Information Systems*
EUA	Estados Unidos da América
FIPPs	*Fair Information Practice Principles*
GDPR	*General Data Protection Regulation*
ICSOFT	*International Joint Conference on Software Technologies*
ICCTS	*International Conference on Collaboration Technologies and Systems*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
IPI	Informação Pessoalmente Identificável
LDA	*Latent Dirichlet Allocation*
LGPD	Lei Geral de Proteção de Dados Pessoais
LINDDUN	*Linkability Identifiability Non-repudiation Detectability Disclosure of information Unawareness Non-compliance*
PbD	*Privacy by Design*
PETS	*Privacy Enhancing Technologies Symposium*
PIA	*Privacy Impact Assessment*
PIAF	*Privacy Impact Assessment Framework*
PRAIS	*PRivacy impact Analysis for Information Sharing*
PRIPARE	*Preparing Industry to Privacy by Design by supporting its Application in Research*
ProPAn	*Problem-based Privacy Analysis*
RSL	Revisão Sistemática da Literatura
RSOs	Redes Sociais *Online*
SAC	*Symposium on Applied Computing*

SPW	*Security and Privacy Workshops*
TELERISE	*TEchnical and LEgal Aspects of Data PRivacy and SEcurity*
TI	Tecnologia da Informação
TIS	*The Information Society*
UE	União Europeia
UML	*Unified Modeling Language*
UML4PF	*UML 4 Problem Frames*
URL	*Uniform Resource Locator*
Wi-Fi	*Wireless Fidelity*

SUMÁRIO

1 INTRODUÇÃO

A privacidade tem sido frequentemente identificada como uma das principais preocupações durante o desenvolvimento de sistemas que lidam com informações pessoais. As atividades que antes eram privadas ou compartilhadas com poucos usuários agora deixam rastros de dados que expõem os interesses, características, crenças e intenções. De acordo com Acquisti, Brandimarte e Loewenstein (2015), informações são reveladas pelas pessoas – intencionalmente e involuntariamente – entre si, com entidades comerciais e com o governo. Enserink e Chin (2015) afirmam que "a tecnologia capacita pesquisadores e o público – mas torna as noções tradicionais de privacidade obsoletas". Às vezes, compartilha-se dados intencionalmente – por exemplo, ao postar fotos de família no Facebook; ao fazer um *tweet* sobre política; Mas grandes quantidades de informação sobre um indivíduo são coletadas apenas com consentimento superficial ou nenhum – por exemplo, em milhares de pesquisas do Google revelam-se interesses, preocupações e desejos (ENSERINK; CHIN, 2015).

A ruptura da privacidade de um indivíduo pode ameaçar a sua autonomia, não apenas como consumidor, mas como cidadão. Segundo Acquisti, Brandimarte e Loewenstein (2015), compartilhar mais dados pessoais nem sempre se traduz em mais progresso, eficiência ou igualdade. Com as crescentes preocupações pessoais com a garantia da privacidade durante o uso de diferentes aplicações, tais como aplicativos móveis e serviços *online*, diversos países têm sancionado novas legislações que regulamentam a mesma questão para coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD)[1] foi sancionada em agosto de 2018 e entrou em vigor em setembro de 2020. Como principal influência para a criação e maturação da LGPD, tem-se a GDPR[2] (*General Data Protection Regulation*), que entrou em vigor em 25 de maio de 2018 e regulamenta a questão para países europeus.

A GDPR estabeleceu uma mudança de paradigma na proteção de dados e privacidade das pessoas, servindo de modelo para muitos outros países adotarem disposições semelhantes ou reforçarem políticas pré-existentes. A Lei visa garantir a privacidade digital, sendo o regulamento norteado por princípios tais como: licitude, lealdade e transparência, adequação e limitação da finalidade, necessidade ou minimização, qualidade dos dados ou exatidão, limitação da conservação, segurança, integridade e confidencialidade, prestação de contas ou responsabilização (CHASSANG, 2017).

Dentre as questões abordadas na GDPR, o mesmo discorre ainda sobre o consentimento explícito, em que o usuário deve optar por compartilhar quaisquer dados de IPI (Informação Pessoalmente Identificável) antes que uma empresa possa armazená-los. A GDPR expande a definição de IPI muito além do nome, endereço e data de nascimento

[1]Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>
[2]Disponível em: <https://gdpr-info.eu/>

tradicionais, abrangendo a localização do usuário (incluindo endereço IP), saúde, dados genéticos (incluindo dados biométricos), orientação sexual, raça, etnia, crenças religiosas ou opiniões política. A GDPR regulamenta os direitos dos usuários, entre os quais se destacam o direito de apagar e o direito de ser esquecido (European Commission, 2016).

Com a LGPD, o Brasil entra para o rol dos 126 países que possuem lei específica para a proteção de dados pessoais, cujos pilares são a transparência, gestão e governança. A LGPD estabelece regras para coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o seu não cumprimento (LGPD Brasil, 2019). Com a entrada em vigor da LGPD a forma com que as empresas e organizações captam, armazenam e utilizam os dados de seus clientes, tanto no meio *online* quanto *offline*, são afetados.

Com o advento da Internet e os avanços tecnológicos deram origem às Redes Sociais *Online* (RSOs), que são hoje o principal meio de conexão à Internet para milhões de pessoas. Os RSOs permitem que os usuários compartilhem informações com amigos e facilitem a comunicação e interação interpessoal. No entanto, o risco mais significativo dos usuários ao ingressar em uma rede social é controlar os dados sobre si mesmos (BADEN et al., 2009; RODRIGUES; VALENTIM; CONTE, 2017). Conforme relatado por Estivill-Castro e Nettleton (2015), as redes sociais oferecem aos usuários muitos benefícios, incluindo socialização virtual, ampla transmissão, colaboração e comunicação. No entanto, eles não podem regular a restrição dos círculos em que os dados são compartilhados. O grau em que eles controlam seus dados é, no entanto, uma das medidas de privacidade mais comuns.

Tem sido bem documentado e confirmado por vários autores que as disposições de outros podem influenciar as decisões de privacidade dos usuários. Exemplos incluem Gambino et al. (2016), Vincent et al. (2017), Wu et al. (2018). De acordo com Wu et al. (2018), os comportamentos de divulgação dos usuários provavelmente são influenciados por várias heurísticas. Por exemplo, a divulgação de informações já divulgadas por outros, a retenção de informações quando um item é encomendado inesperadamente ou o uso de configurações de privacidade padrão de mídia social. A aplicação de heurísticas é um método eficaz para resolver problemas rapidamente e fazer julgamentos precisos, sendo uma técnica de pensamento e comportamento praticamente automática nos humanos, os quais agem de modo intuitivo e inconsciente para achar prováveis respostas para aquilo que procuram - portanto, a heurística pode ser considerada um “atalho mental”.

Ao confiar em heurísticas, as pessoas podem ter um desempenho melhor, pois não serão obrigadas a pensar constantemente em seu próximo passo. Sundar et al. (2020) declaram que heurísticas não são inventadas na interação, mas representam associações estáveis formadas na mente do usuário. Segundo os autores, um fator determinante para acionar uma heurística ao utilizar uma interface é o grau de acessibilidade dessa heurística na mente do indivíduo. Contudo, as heurísticas também podem levar a vieses cognitivos,

os quais preconceitos influenciam o modo como os indivíduos pensam e os julgamentos que fazem.

De acordo com o Artigo 35 do GDPR, os controladores de dados são obrigados a realizar uma Avaliação de Impacto de Privacidade - *Privacy Impact Assessment* (PIA) para garantir a proteção de dados confidenciais (European Commission, 2016). A LGPD importou o conceito, sob o nome de relatório de impacto à proteção de dados pessoais (Art. 5º - XVII), o qual consiste basicamente em uma documentação que descreve os processos de tratamento de dados pessoais que podem gerar algum risco aos direitos dos titulares, além das medidas e mecanismos empregados para mitigar esses riscos. No Artigo 38 da LGPD é determinado que a Autoridade Nacional de Proteção de Dados (ANPD) poderá determinar ao controlador que elabore o relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (Lei Nº 13.709, 2018). As PIAs são ferramentas usadas em muitos domínios para avaliar ou estimar os impactos de determinadas intervenções ou ações (EDWARDS; VEALE, 2018). Uma PIA visa realizar uma avaliação sistemática de riscos, a fim de identificar ameaças à privacidade e impor controles técnicos e organizacionais para mitigar essas ameaças e promover políticas totalmente informadas (AHMADIAN et al., 2018).

1.1 Problema

Desta forma, o problema de pesquisa deste trabalho é sintetizado nas seguintes perguntas:

1) Ao realizar uma análise de heurísticas das redes sociais Facebook e Instagram quais heurísticas cognitivas de privacidade podem ser observadas?

2) Sendo as heurísticas cognitivas de privacidade identificadas durante a análse, quais impactos a presença das mesmas pode ocasionar a privacidade do usuário?

3) Qual a relação das heurísticas cognitivas de privacidade com os princípios do conceito de "Privacidade desde a concepção" (*Privacy by Design* - PbD) e os princípios das leis LGPD e GDPR?

1.2 Objetivos

Esta subseção apresenta o objetivo geral e os objetivos específicos que norteiam esta pesquisa.

1.2.1 Objetivo Geral

O principal objetivo deste trabalho é identificar heurísticas que influenciam a divulgação de dados e realizar uma análise das heurísticas de privacidade nas redes sociais

online Facebook e Instagram para identificar os fatores que influenciam a divulgação de informações do usuário e verificar a presença de consentimento informado por meio da análise das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok.

1.2.2 Objetivos Específicos

Para atingir o objetivo proposto foram definidos os seguintes objetivos específicos:

a) Realizar uma revisão sistemática da literatura para identificar quais são as metodologias propostas e como é realizada a elaboração de uma *Avaliação de Impacto de Privacidade*;

b) Realizar uma análise qualitativa das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok conforme metodologia identificada para elaboração de uma PIA;

c) Realizar um levantamento das heurísticas cognitivas de privacidade que influenciam as decisões dos indivíduos de proteger ou renunciar à sua privacidade;

d) Avaliar o possível impacto à privacidade do usuário de acordo com as heurísticas cognitivas de privacidade observadas durante a análise das redes sociais Facebook e Instagram;

e) Realizar a análise da relação das heurísticas cognitivas de privacidade com os princípios do *Privacy by Design* e os princípios das leis LGPD e GDPR;

1.3 Justificativa

Segundo Acquisti, Brandimarte e Loewenstein (2015), os indivíduos raramente têm conhecimento claro de quais informações outras pessoas, empresas e governos têm sobre eles ou como essas informações são usadas e com quais consequências. Enquanto alguns danos à privacidade são tangíveis, como os custos financeiros associados ao roubo de identidade, muitos outros, como estranhos que tomam conhecimento da história de vida de alguém, são intangíveis.

Muitas violações de bancos de dados e perdas de dados pessoais mantidos pelo governo e pela indústria receberam publicidade negativa na mídia. Contudo, sem dúvida, existem mais violações e perdas que não foram relatadas. Mesmo assim, aqueles que foram denunciados têm seu peso na quebra da confiança pública. De acordo com Wright (2011), a maioria das pessoas simplesmente não acredita que seus dados pessoais estejam seguros.

No entanto, mesmo diante das preocupações e desafios citados anteriormente, o *Privacy by Design* (PbD), abordagem pela qual a privacidade é implementada desde a

concepção de novos sistemas, ainda não obteve adoção ativa e difundida na prática de engenharia, devido a uma incompatibilidade entre a mentalidade jurídica e tecnológica (BIRNHACK; TOCH; HADAR, 2014). De fato, na mentalidade dos engenheiros, a privacidade é geralmente considerada apenas na perspectiva da segurança dos dados, se houver; e tendem a desconsiderar a privacidade e a proteção de dados nos projetos técnicos e arquitetura de *software*, baseando-se em políticas de privacidade para conformidade jurídica (HADAR et al., 2018). Em vez disso, é necessária uma abordagem prática, que forneça orientações específicas para desenvolvedores e engenheiros em geral, como peças-chave para obter proteção efetiva de dados (MARTIN; KUNG, 2018). Torna-se fundamental facilitar que os desenvolvedores de *software* incorporem a privacidade aos sistemas de *software* projetados.

De acordo com Clarke (2009), diretrizes foram publicadas, algumas por órgãos de supervisão da privacidade, algumas por agências centrais e outras por consultores. Todavia, muitos conjuntos de diretrizes são da natureza de listas de verificação e podem facilmente levar à geração de documentos que evidenciam uma compreensão superficial dos problemas de privacidade decorrentes do projeto. Segundo Ahmadian et al. (2018), essas diretrizes descrevem um conjunto de etapas genéricas e abstratas em relação as PIAs e não consideram o *design* concreto de um sistema para identificar falhas e ameaças específicas de *design*. Por fim, Oetzel e Spiekermann (2014) afirmam que mesmo que as PIAs se tornem obrigatórias, não existem padrões sobre como conduzir PIAs; além disso, as abordagens atuais carecem de uma metodologia clara e de fácil aplicabilidade.

A principal contribuição esperada é que com a realização deste projeto de pesquisa seja possível apoiar aos Engenheiros de *Software* no desenvolvimento de sistemas norteados na proteção de privacidade (*privacy-aware*), com foco na preservação dos dados pessoais de um indivíduo ao longo do ciclo de vida da informação. Dessa maneira, favorecendo ao desenvolvimento de sistemas de *software* com vulnerabilidades de privacidade reduzidas e que contemplem uma análise constante e abrangente dos problemas de privacidade decorrentes da integração contínua de desenvolvimento de software.

1.4 Organização da Dissertação

Esta dissertação está organizada da seguinte maneira: No Capítulo 2 são apresentados conceitos ligados à privacidade que embasam esta pesquisa e são descritas questões tratadas em regulamentações de tratamentos de dados pessoais, particularmente na Lei LGPD (Brasil). O Capítulo 3 contém os trabalhos relacionados levantados por meio de uma revisão sistemática da literatura. O Capítulo 4 detalha as técnicas e métodos de pesquisa aplicados para alcançar os objetivos traçados. O Capítulo 5 apresenta os resultados encontrados e as discussões da pesquisa realizada. Por fim, o Capítulo 6 traz as considerações finais e os trabalhos futuros que podem ser desenvolvidos a partir dessa dissertação.

2 REFERENCIAL TEÓRICO

Neste Capítulo são apresentados conceitos que embasam este estudo. Na Seção 2.1 aborda-se sobre o contexto, a definição, a terminologia, os princípios e os objetivos de proteção de privacidade; além disso, é descrita a diferença entre privacidade e segurança. A Seção 2.2 apresenta informações sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) sancionada no Brasil. Por fim, a Seção 2.3 discorre sobre os desafios para a implantação da LGPD.

2.1 Privacidade

A privacidade é um conceito multifacetado que foi objeto de várias definições e refinamentos. Para tal, foram propostas diferentes técnicas de proteção de dados com o propósito de atender a essas definições. As quais, se for examinado ao redor do mundo, os regulamentos de privacidade compõem um caleidoscópio, diferindo de maneira sutil e substancial de país para país.

2.1.1 Definições de Privacidade

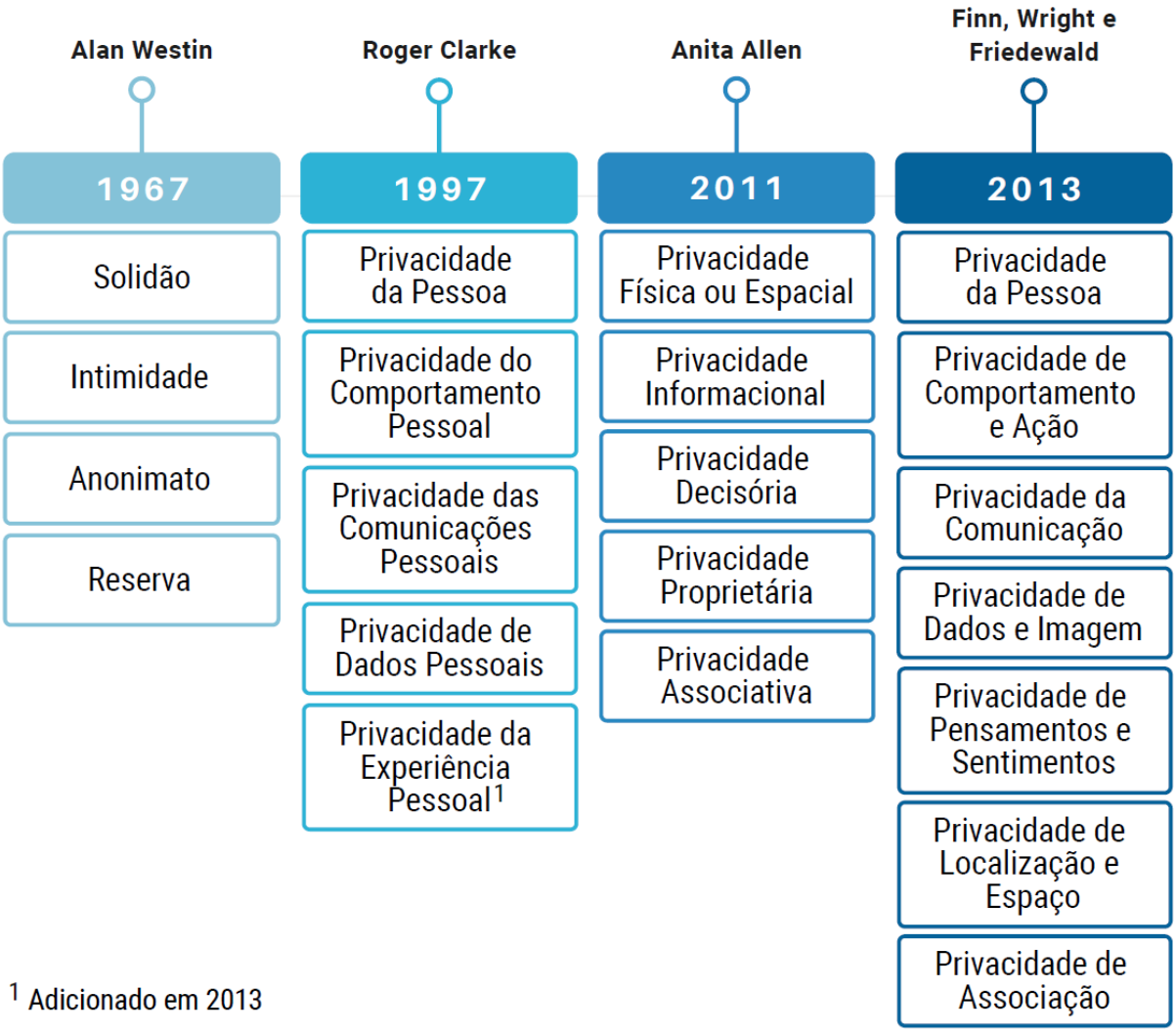
Segundo Meis (2018), o entendimento e a interpretação da privacidade variam entre as disciplinas e também entre a literatura do mesmo campo de pesquisa. Koops et al. (2016) discutem várias tentativas importantes de classificar a privacidade na literatura. Os autores não discutem todas as tentativas classificatórias existentes, mas oferecem uma visão cronológica dos trabalhos acadêmicos mais relevantes reconhecidos na pesquisa sobre privacidade (Figura 1).

2.1.1.1 Os quatro estados de privacidade individual de Alan Westin

O livro "*Privacy and Freedom*" de Westin (1967), lançou as bases filosóficas dos atuais debates sobre tecnologia e liberdade pessoal e é considerado um texto fundamental no campo do direito à privacidade. Westin (2003) definiu privacidade "como a reivindicação de um indivíduo para determinar quais informações sobre si mesmo devem ser conhecidas pelos outros". Além disso, o autor afirma que é relevante considerar o uso e as circunstâncias para as quais essas informações são obtidas por outros usuários.

Segundo Westin (2003), existem três níveis para abordar a privacidade em uma sociedade: o *político*, o *sociocultural* e o *individual*. No nível *político* toda sociedade com base em sua filosofia política estabelece um equilíbrio distinto entre a esfera privada e a ordem pública. No nível *sociocultural* fatores ambientais, como grandes cidades, classe de riqueza e raça, moldam as reais oportunidades que as pessoas têm para reivindicar a liberdade da observação de outras pessoas. A privacidade a nível *individual* se concentra no indivíduo e na experiência cotidiana dele ao interagir diretamente com outras pessoas, sendo uma função da vida familiar, educação, classe social e composição psicológica.

Figura 1 – Evolução cronológica nas definições de privacidade



Fonte: Elaborado pela autora baseado nas classificações de privacidade de Westin (1967), Clarke (1997), Allen (2011), Finn, Wright e Friedewald (2013)

Conforme Westin (2003), a privacidade a nível *individual* reflete as necessidades e desejos particulares de cada indivíduo e mudará constantemente em termos de progresso do ciclo de vida e eventos situacionais. Diante disso, foram identificados quatro condições psicológicas ou estados de privacidade individual: solidão, intimidade, anonimato e reserva. Solidão refere-se à liberdade de ser observado por outras partes, existe quando um indivíduo é separado dos outros. Intimidade significa estar em posição de se tornar um membro de um pequeno grupo (incluindo uma ou apenas duas pessoas), que mantém um relacionamento próximo, honesto e descontraído. Anonimato refere-se a não ser submetido a vigilância em público. Por fim, reserva refere-se à liberdade de limitar quais informações sobre uma pessoa são divulgadas a outras pessoas (WESTIN, 2003; KOOPS et al., 2016).

2.1.1.2 Classificação de Roger Clarke

Clarke (1997) desenvolveu um sistema "atualizado" de pensamento sobre privacidade que, ele argumentou, poderia suportar o novo desenvolvimento tecnológico na sociedade – especificamente, o computador e os primeiros esboços de uma Internet comercial. Clarke baseia sua categorização de privacidade na pirâmide de valores de Maslow[1]. Tomando os valores centrais dessa categorização das necessidades da vida – autorrealização, status (ou auto-estima), amor ou pertencimento, segurança e necessidades fisiológicas ou biológicas – transformando tais necessidades de vida em necessidades de privacidade, levando a um sistema de "valores de privacidade" baseados no indivíduo (KOOPS et al., 2016). Clarke argumenta que, "interpretado de maneira mais ampla, a privacidade diz respeito à integridade do indivíduo. Portanto, abrange todos os aspectos das necessidades sociais do indivíduo.". As categorias de Clarke são as seguintes.

- **Privacidade da Pessoa:** também chamada de privacidade corporal. Isso significa que o corpo físico e sua privacidade física estão ligados às necessidades fisiológicas e de segurança da pirâmide de Maslow. Os exemplos incluem danos físicos e não solicitados ao organismo: "imunização compulsória, transfusão de sangue sem consentimento, fornecimento obrigatório de amostras de fluidos e tecidos corporais e esterilização compulsória" (KOOPS et al., 2016).

- **Privacidade do Comportamento Pessoal:** refere-se a todos os aspectos do comportamento, mas especialmente a questões delicadas, como preferências e hábitos sexuais, atividades políticas e práticas religiosas, tanto em locais privados quanto em locais públicos. Inclui o que às vezes é chamado de "privacidade da mídia" (CLARKE, 1997). O autor vincula às necessidades de pertencimento e auto-estima da hierarquia de Maslow e, talvez, à auto-atualização (KOOPS et al., 2016).

- **Privacidade das Comunicações Pessoais:** trata-se da liberdade de comunicação sem interceptação e/ou monitoramento de rotina da comunicação de alguém por outros (KOOPS et al., 2016).

- **Privacidade de Dados Pessoais:** os indivíduos afirmam que os dados sobre eles mesmos não devem estar automaticamente disponíveis para outros indivíduos e organizações e que, mesmo quando os dados são de terceiros, o indivíduo deve ser capaz de exercer um grau substancial de controle sobre esses dados e seu uso. Às vezes, isso é chamado de "privacidade de dados" e "privacidade de informações" (CLARKE, 1997). Relaciona-se às camadas mais altas da pirâmide, sendo auto-atualização e status ou auto-estima (KOOPS et al., 2016).

[1]Pirâmide de Maslow: coloca as necessidades humanas em hierarquia, sendo elas: fisiologia, segurança, amor e relacionamentos, estima e realização pessoal.

- **Privacidade da Experiência Pessoal:** categoria adicionada em 2013 pelo autor, depois de perceber que a Web 2.0 e a mídia móvel tiveram um impacto grave e imprevisto na sociedade e, portanto, também na privacidade. As atividades de leitura e visualização migraram para telas, são realizadas sob o controle de empresas e registradas; a maioria das conversas se tornou "comunicações eletrônicas armazenadas", cada evento é gravado e os "registros de chamadas" e o conteúdo podem ser retidos; a localização de muitas pessoas é rastreada e são realizadas correlações para descobrir quem está localizado com quem e com que frequência; e os ingressos para eventos são pagos usando instrumentos de pagamento identificados. Essa consolidação maciça da experiência pessoal dos indivíduos está disponível para exploração e é explorada (CLARKE, 1997).

2.1.1.3 "Privacidade impopular" de Anita Allen

Allen (2011) adota uma abordagem diferente baseando a classificação da privacidade em valores morais e sociais, combinando estudos jurídicos com uma perspectiva enraizada nos estudos feministas. Allen argumenta que os governos devem impor certas leis e deveres "impopulares" de privacidade para proteger o bem comum – mesmo que isso signifique forçar a privacidade de pessoas que talvez não o desejem – e também não permitir que os indivíduos optem por não participar ou renunciarem a seus direitos de privacidade. Ela identifica várias categorias de privacidade, sem estruturá-las sistematicamente além de identificá-las e descrevê-las brevemente. São elas:

- **Privacidade Física ou Espacial:** refere-se às expectativas de privacidade dentro e fora de casa, por exemplo. Uma invasão de privacidade aqui é, por exemplo, o olhar que invade a privacidade da vida íntima de duas pessoas, olhando pela janela do quarto e tirando fotografias (KOOPS et al., 2016).

- **Privacidade Informacional:** é um conceito mais amplo, que engloba informações/dados/fatos sobre pessoas ou suas comunicações. Um exemplo de categoria híbrida seria a privacidade "local" – a privacidade das informações sobre a localização física (geográfica) de alguém (KOOPS et al., 2016).

- **Privacidade Decisória:** trata-se em grande parte de uma proteção contra invasões estatais contra o direito dos cidadãos de fazer certas escolhas íntimas em relação a suas vidas e à maneira como eles escolhem viver, incluindo escolhas sobre casamento entre pessoas do mesmo sexo ou suicídio assistido (KOOPS et al., 2016).

- **Privacidade Proprietária:** pertence à reputação. É semelhante ao "direito à honra" encontrado em certas constituições. Allen usa um exemplo de um editor que usa o retrato de uma família numerosa sem permissão, para ilustrar uma história divertida sobre experimentos com cafeína, a qual é capaz de aumentar a motilidade

espermática – rompendo (expectativas de) privacidade reputacional ou "proprietária" (KOOPS et al., 2016).

- **Privacidade Associativa:** diz respeito a grupos e suas relações internas de associação – incluindo seus valores e critérios de inclusão e exclusão. Na visão de Allen, isso inclui não apenas o direito de um membro de manter sua associação em grupos, mas também o direito do grupo de determinar quem deve ser incluído ou excluído e quais motivos eles podem usar para fazê-lo (KOOPS et al., 2016).

2.1.1.4 Tipos de privacidade de Finn, Wright e Friedewald

Finn, Wright e Friedewald (2013) apresentam uma tipologia[1], desenvolvida no contexto da legislação da União Europeia (UE), projetada para enfrentar as ameaças à privacidade relacionadas à tecnologia moderna no século XXI. Trabalhando a perspectiva da proteção de dados da UE, os autores tratam os titulares de dados como a unidade de análise. Ao fazer sua tipologia, baseiam-se principalmente no trabalho de Clarke (1997) e Solove (2006). Sendo a privacidade dividida nos sete tipos a seguir.

- **Privacidade da Pessoa:** direito de "manter as funções e características do corpo (como códigos genéticos e biométricos) privadas". Faz menção a códigos biométricos e genéticos e antecipa, por exemplo, a digitalização da íris à distância e o potencial crescimento da bioinformática. Pensa-se que a privacidade da pessoa conduz a sentimentos individuais de liberdade e ajuda a apoiar uma sociedade democrática saudável e bem ajustada.

- **Privacidade de Comportamento e Ação:** conforme descrito por Clarke, esse tipo envolve atividades que acontecem em locais públicos e privados e abrange questões delicadas, como religião, política ou preferências sexuais.

- **Privacidade da Comunicação:** um ator viola esse tipo de privacidade, por exemplo, interceptando comunicações pessoais (como abrir ou ler e-mails ou usar escuta espiã), interceptar ou acessar as comunicações armazenadas sem consentimento.

- **Privacidade de Dados e Imagem:** tratam-se de preocupações sobre formas automatizadas de compartilhamento de dados e imagens e a facilidade com que terceiros podem acessar dados sem o conhecimento do titular dos dados. Os autores expressam o sentimento de que as pessoas devem ser capazes de "exercer um grau substancial de controle sobre esses dados e seu uso".

- **Privacidade de Pensamentos e Sentimentos:** diante da afirmação de que a privacidade é tanto um dano causado aos sentimentos quanto intrusões físicas, há

[1]Tipologia: ciência que estuda os tipos, diferença intuitiva e conceptual de formas de modelo ou básicas; muito usada na área de estudos sistemáticos, para definir diferentes categorias.

uma necessidade de proteger a privacidade dos pensamentos e sentimentos, tendo em vista que as tecnologias do futuro próximo, como as interfaces cérebro-computador, podem possibilitar o acesso aos pensamentos e sentimentos de outras pessoas. Isso torna o domínio dos pensamentos e sentimentos uma nova área de preocupação com a privacidade, "porque os indivíduos devem ser capazes de pensar o que quiserem".

- **Privacidade de Localização e Espaço:** nos espaços público e semi-público, os indivíduos devem poder se movimentar livremente e de maneira anônima. Todavia, CFTV inteligente, rastreamento Wi-Fi e *software* de reconhecimento de rosto, são exemplos que tornam isso cada vez mais difícil. Os autores observam que "essa concepção de privacidade também inclui o direito à solidão e o direito à privacidade em espaços como a casa, o carro ou o escritório".

- **Privacidade de Associação:** os indivíduos devem poder se conectar e associar-se livremente com quem ou com qualquer grupo que escolherem sem serem monitorados, os autores observam que "isso há muito é reconhecido como desejável (necessário) para uma sociedade democrática, pois promove a liberdade de expressão, incluindo discurso político, liberdade de culto e outras formas de associação".

De acordo com Koops et al. (2016), o resultado geral da classificação da privacidade estendida de Clarke (1997), proposta por Finn, Wright e Friedewald (2013), permanece um pouco confusa. Às vezes, os autores falam sobre danos à privacidade no sentido de "aquilo que precisa ser protegido", enquanto em outras ocasiões falam sobre um direito à privacidade e, às vezes, sobre os possíveis impactos das novas tecnologias em um tipo de privacidade. Isso faz com que a tipologia varie na forma como é abordada, podendo ser confuso discernir se cada tipo de privacidade mencionado está realmente vinculado a um direito à privacidade ou a uma ameaça à privacidade, ou a um aspecto da privacidade que precisa de atenção ou regulamentação.

Solove (2006) acredita que a privacidade não é uma coisa única, ou seja, não existe um denominador comum. Finn, Wright e Friedewald (2013) concordam com este ponto de vista – na medida em que identificaram sete tipos de privacidade. No entanto, os autores acreditam que existe um denominador comum e esse denominador comum é a noção mal definida de privacidade em si. Os autores corroboram que a privacidade tem um valor social, e que se relaciona com a integridade e autonomia do indivíduo, de modo que quando a privacidade é comprometida – independentemente do tipo de privacidade – o indivíduo está sendo prejudicado de alguma maneira.

2.1.2 Terminologia de Privacidade

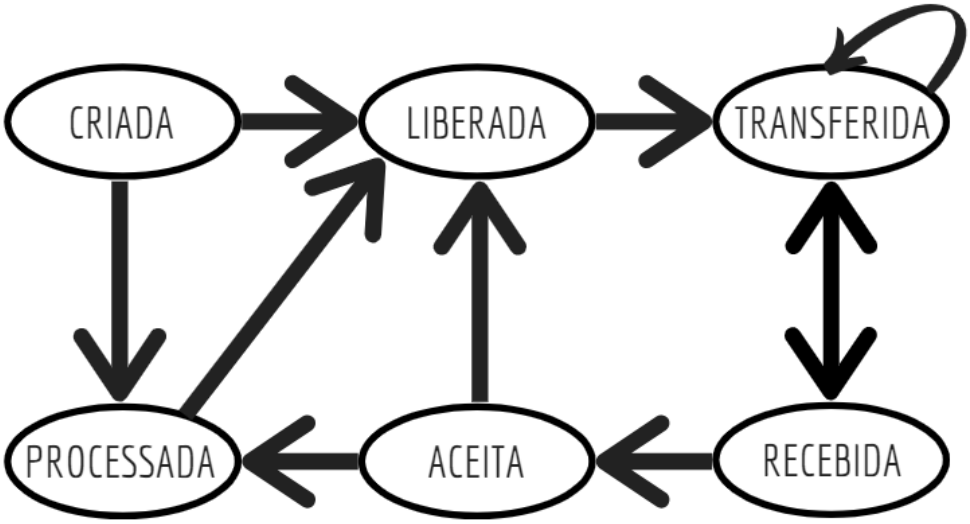
Os termos centrais no contexto da privacidade são os seguintes:

a) **Titular:** "pessoa natural a quem se referem os dados pessoais que são objeto de

tratamento" (Lei Nº 13.709, 2018). Portanto, o titular dos dados é o indivíduo cujos dados são processados pelo sistema de software.

b) **Dado pessoal:** "informação relacionada a pessoa natural identificada ou identificável" (Lei Nº 13.709, 2018). Além do termo "dado pessoal", o termo **Informação Pessoalmente Identificável (IPI)**, ou como conhecido em inglês – *Personally Identifiable Information* (PII), é amplamente utilizado no contexto da privacidade. IPI é definido como sendo informações que contenham uma referência a uma única entidade identificável. Cada IPI refere-se ao(s) seu(s) proprietário(s) no sentido em que ele representa uma entidade distinguível no mundo. Portanto, se a informação x leva à identificação de um indivíduo, x é IPI. Por conseguinte, existem dois tipos de IPI: 1) IPI Atômico: onde a IPI se refere a um único proprietário; 2) IPI Composto: em que a IPI se refere a mais de um proprietário. Dessa forma, são informações que podem ser recebidas (chegam e são aceitas), processadas, criadas, liberadas e transferidas. Um sistema de fluxo (Figura 2) representa os estágios nos quais as informações estão em vários estados exclusivos. Os estados de IPI nesse sentido se referem à sua condição, como nos estados da matéria: sólido, líquido e gás (AL-FEDAGHI; JERAGH, 2011). Consequentemente, segundo Al-Fedaghi e Jeragh (2011), as operações em IPI são limitadas a seis operações, o que torna as regras de manipulação de IPI muito específicas e fáceis de descrever nas leis de privacidade.

Figura 2 – Sistema de fluxo da Informação Pessoalmente Identificável (assumindo que a informação liberada não é retornada)



Fonte: Adaptado de Al-Fedaghi e Jeragh (2011)

c) **Dado pessoal sensível:** "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Lei Nº 13.709, 2018).

d) **Dado anonimizado:** "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Lei Nº 13.709, 2018). A European Commission (2016) define o termo **pseudonimização**, o qual refere-se ao "tratamento de dados pessoais de forma que os dados pessoais não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável".

e) **Tratamento:** "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (Lei Nº 13.709, 2018).

f) **Controlador:** "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Lei Nº 13.709, 2018). Coleta dados pessoais e toma todas as decisões em relação à forma e finalidade do tratamento dos dados, é responsável por como os dados são coletados, para que estão sendo utilizados e por quanto tempo serão armazenados.

g) **Operador:** "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Lei Nº 13.709, 2018).

h) **Agentes de tratamento:** "o controlador e o operador" (Lei Nº 13.709, 2018).

i) **Encarregado:** "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". (Redação dada pela Lei Nº 13.853 (2019))

j) **Relatório de impacto à proteção de dados pessoais:** "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (Lei Nº 13.709, 2018). O Artigo 35 do GDPR determina que os controladores de dados são obrigados a realizar uma Avaliação de Impacto de Privacidade - *Privacy Impact Assessment* (PIA) para garantir a proteção de dados confidenciais (European Commission, 2016).

   Wright (2011) apresenta quatro etapas principais existentes nas diretrizes publicadas por órgãos de supervisão da privacidade, por agências centrais e por consultores, são elas:

(1) *Iniciação do projeto:* determinar se uma PIA é necessária. Identificar se uma proposta apresenta riscos significativos à privacidade;

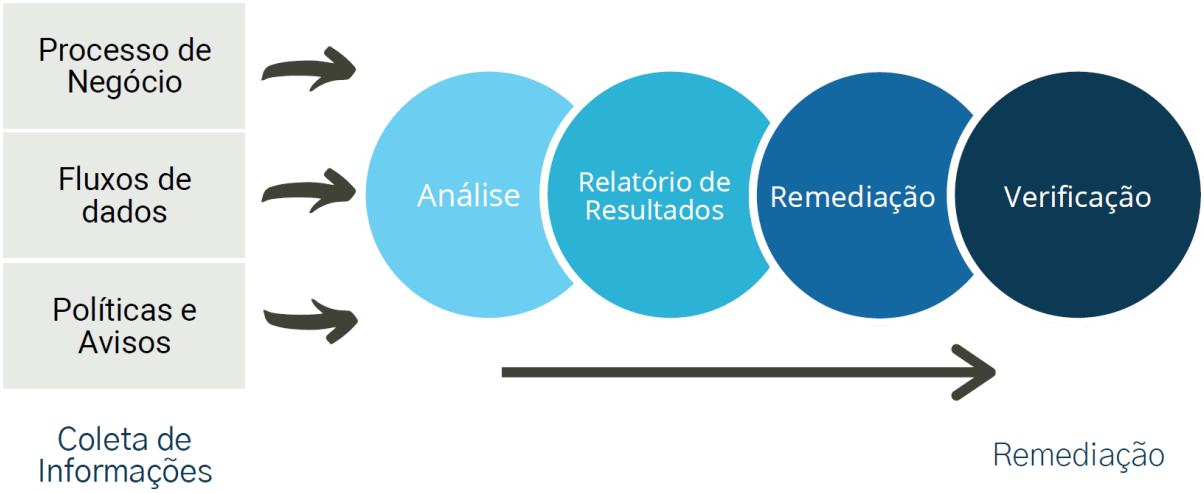
(2) *Análise de fluxo de dados:* examinar como as informações pessoais serão coletadas, usadas, divulgadas e mantidas;

(3) *Análise de privacidade:* responder a uma série de perguntas destinadas a ajudar a identificar os riscos ou vulnerabilidades de privacidade associados à proposta;

(4) *Análise de impacto na privacidade:* preparar um relatório que contenha uma avaliação documentada dos riscos à privacidade e as implicações associadas a esses riscos, além de uma discussão sobre possíveis soluções.

Dennedy, Fox e Finneran (2014) afirmam que além de interativas, as PIAs são iterativas. À medida que os produtos, sistemas, processos e aplicativos evoluem, os fluxos de dados e o uso de controles e medidas mudam, dessa forma as informações precisarão ser reunidas, reanalisadas, reportadas e possivelmente re-estimadas e definitivamente reconfirmadas. O processo de PIA não termina até que os dados sejam descartados ou excluídos. Dependendo de onde no ciclo de desenvolvimento a PIA está sendo conduzida, ela pode servir como uma ferramenta para indicar o que é necessário ou para confirmar o que está em vigor ou planejado. A Figura 3 apresenta cinco fases para a elaboração da PIA. Na fase de **Relatório de Resultados** são identificadas as lacunas entre o estado atual e o estado desejado, controles e mitigações, quando necessário, e recomendações.

Figura 3 – Fases para a elaboração da Avaliação de Impacto de Privacidade - *Privacy Impact Assessment* (PIA)



Fonte: Dennedy, Fox e Finneran (2014)

2.1.3 Princípios de Privacidade

Os exemplos mais reconhecidos de princípios de privacidade são: Fair Information Practice Principles (FIPPs) (US Federal Trade Commission, 1998; NISTIR 8062, 2017),

framework de privacidade da OECD (OECD, 2020), ISO 29100 (ISO/IEC, 2011) e os princípios do *Privacy by Design* (CAVOUKIAN, 2009). O regulamento da União Europeia (GDPR) também fornece um conjunto de princípios semelhantes aos mencionados anteriormente (European Commission, 2016).

A OECD forneceu um framework de privacidade (OECD, 2020), que consiste nos oito princípios a seguir: *(i)* limitação de coleta, *(ii)* qualidade dos dados, *(iii)* especificação de finalidade, *(iv)* limitação de uso, *(v)* salvaguardas de segurança, *(vi)* abertura, *(vii)* participação individual e *(viii)* prestação de contas (HAZEYAMA et al., 2016). Os princípios definidos na FIPPs assemelham-se aos princípios do framework da OECD, enquanto o princípio de *transparência* é abordado além dos demais (US Federal Trade Commission, 1998).

2.1.3.1 Princípios da LGPD para tratamento de dados pessoais

A LGPD, no Art. 6º define as atividades de tratamento de dados pessoais que deverão observar a boa-fé e destaca dez princípios (Lei Nº 13.709, 2018). São eles:

I) **Finalidade:** "tratamento para propósitos legítimos, específicos, explícitos e informados ao titular." (Lei Nº 13.709, 2018). Meis (2018) apresenta o princípio de "**consentimento e escolha**", no qual os controladores devem solicitar aos titulares dos dados seu consentimento informado e explícito antes de processar seus dados pessoais. Os titulares dos dados devem ter a opção para quais fins seus dados são processados.

II) **Adequação:** "compatibilidade do tratamento com as finalidades informadas ao titular." (Lei Nº 13.709, 2018). Segundo Meis (2018), corresponde aos tipos e quantidade de dados pessoais processados por um controlador, os propósitos para os quais são utilizados e os procedimentos com o qual o controlador processa os dados pessoais, os quais devem ser equilibrados com os tipos e quantidade de dados pessoais realmente necessários para os fins para os quais os titulares dos dados forneceram seus dados, as expectativas dos titulares de dados em relação ao processamento de seus dados e às necessidades de proteção dos dados pessoais processados.

III) **Necessidade:** "limitação do tratamento ao mínimo necessário, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades." (Lei Nº 13.709, 2018).

IV) **Livre acesso:** "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais." (Lei Nº 13.709, 2018).

V) **Qualidade dos dados:** "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados." (Lei Nº 13.709, 2018). US Federal Trade Commission (1998) e OECD (2020) citam o princípio de "**participação individual**", o qual os titulares dos dados devem poder exercer direitos sobre seus dados, por exemplo, correção e exclusão de seus dados pessoais e objeção ao processamento de dados pessoais.

VI) **Transparência:** "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento." (Lei Nº 13.709, 2018).

VII) **Segurança:** "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão." (Lei Nº 13.709, 2018).

VIII) **Prevenção:** "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais." (Lei Nº 13.709, 2018).

IX) **Não discriminação:** "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos." (Lei Nº 13.709, 2018).

X) **Responsabilização e prestação de contas:** "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (Lei Nº 13.709, 2018). US Federal Trade Commission (1998) e OECD (2020) citam o princípio de "***accountability***", em que os controladores devem garantir que todos os princípios sejam seguidos e documentar as ações que adotaram. Esta documentação deve incluir políticas, procedimentos e práticas de privacidade.

2.1.3.2 Princípios do *Privacy by Design*

O *Privacy by Design* (PbD) é um conceito pioneiro da Comissária de Informação e Privacidade do Ontário, Ann Cavoukian. Cavoukian (2009) afirma que "o futuro da privacidade não pode ser assegurado apenas pela conformidade com as estruturas regulatórias; em vez disso, a garantia da privacidade deve, idealmente, tornar-se o modo de operação padrão de uma organização". O PbD é uma abordagem proativa, em vez de reativa, para a proteção da privacidade, que considera as implicações de privacidade das novas tecnologias durante a fase de projeto, e não como uma reflexão tardia. De acordo com Kroener e Wright (2014), durante a fase de concepção de novas tecnologias ou sistemas que coletam e processam dados pessoais devem ser levados em conta seis princípios de PbD, são eles: minimização de dados, controlabilidade (consentimento e objeção), transparência, confidencialidade de dados, qualidade de dados e segregação (por exemplo, em nuvem).

Cavoukian (2009) apresenta os sete princípios para o PbD, como segue:

1) **Proativo não reativo:** ação preventiva não corretiva: antecipa e evita eventos invasivos de privacidade antes que eles aconteçam.

2) **Privacidade como configuração padrão:** se um indivíduo não faz nada, sua privacidade deve permanecer intacta. Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - ela é incorporada ao sistema, por padrão.

3) **Privacidade incorporada ao design:** privacidade torna-se um componente essencial da funcionalidade principal sendo entregue. A privacidade é integral ao sistema, sem diminuir a funcionalidade do sistema.

4) **Funcionalidade total – soma positiva, não soma zero:** acomodar todos os interesses e objetivos legítimos de maneira positiva, com ganhos mútuos, e não por meio de uma abordagem datada de soma zero, na qual se realiza *trade-offs* desnecessários entre interesses diferentes.

5) **Segurança de ponta a ponta - garantindo a proteção completa do ciclo de vida:** garante que todos os dados sejam retidos com segurança e, em seguida, destruídos com segurança no final do processo, em tempo hábil.

6) **Compromisso de visibilidade e transparência:** operar de acordo com as promessas e objetivos declarados, sujeito a verificação independente.

7) **Respeito pela privacidade do usuário - todos os desenvolvimentos precisam permanecer centrados no usuário:** manter os interesses do indivíduo em primeiro lugar, oferecendo medidas tais como padrões de privacidade, notificação apropriada e aplicação de opções fáceis de usar.

O Quadro 1 relaciona os princípios das diferentes fontes entre si. A primeira coluna contém os princípios e as outras colunas representam uma fonte de princípios de privacidade, são mapeados os princípios contidos nessa fonte para um ou mais dos princípios contidos na primeira coluna. O quadro apresentado é uma adaptação de Meis (2018), no qual foi adicionado o mapeamento dos princípios abordados na LGPD.

Quadro 1– Visão geral dos princípios de privacidade

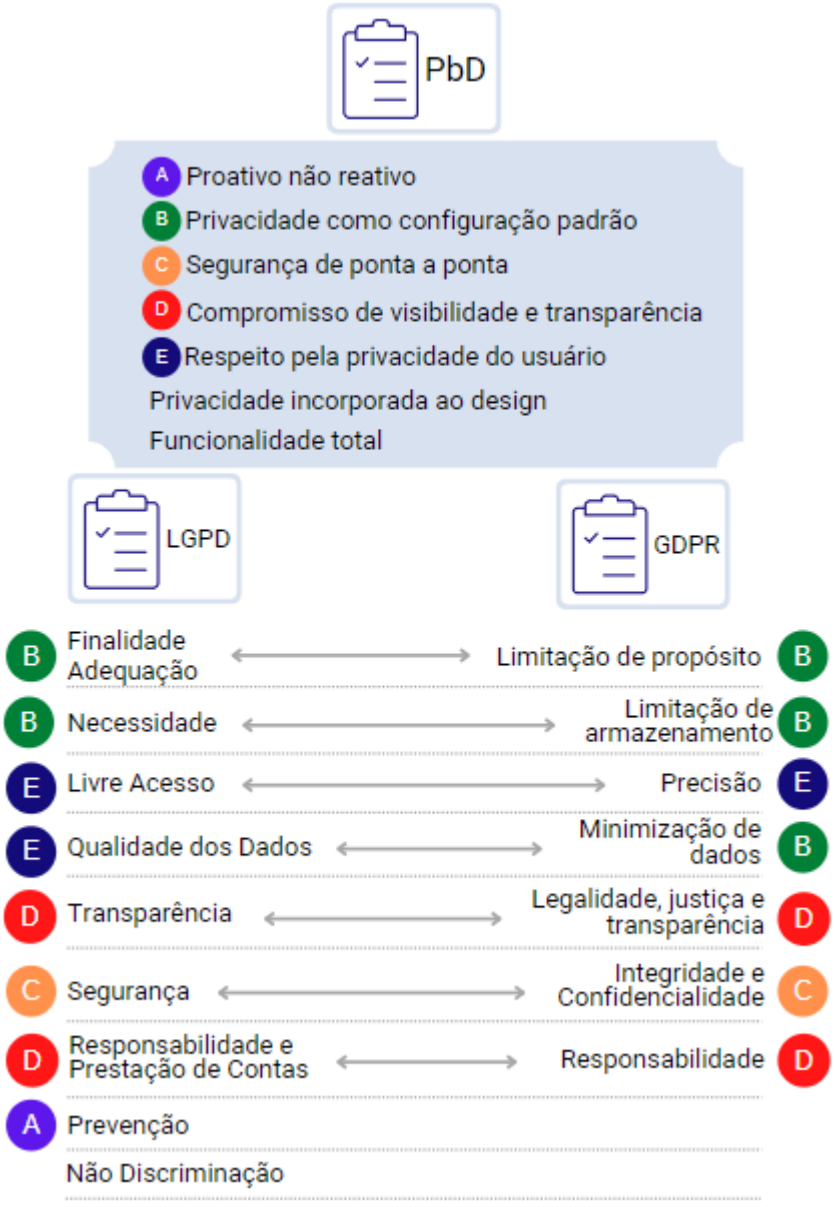
Princípio	ISO 29100	OECD	FTC FIPPs	NIST FIPPs	PbD	GDPR	LGPD
Justiça (Fairness)						Legalidade, justiça e transparência	
Conformidade	Conformidade com a privacidade						
Abertura e Transparência	Abertura, transparência e aviso	Abertura	Aviso prévio/ Consciência	Transparência	Visibilidade e transparência		Transparência
Acesso	Participação individual e acesso		Acesso/ Participação	Acesso e alteração	Respeito pela privacidade do usuário		Livre acesso
Participação individual		Participação individual		Participação individual			
Consentimento e escolha	Consentimento e escolha		Escolha/ Consentimento				Finalidade
Legitimidade da finalidade	Legitimidade da finalidade e especificação			Autoridade			
Especificação de finalidade		Especificação de finalidade		Especificação de finalidade e limitação de uso			Adequação
Limitação de uso	Limitação de uso, retenção e divulgação	Limitação de uso				Limitação de finalidade	
Limitação de armazenamento						Limitação de armazenamento	
Limitação de coleta	Limitação de coleta	Limitação de coleta		Minimização		Minimização de dados	Necessidade
Minimização de dados	Minimização de dados						
Segurança	Segurança da informação	Salvaguardas de segurança	Integridade Segurança	Segurança	Segurança de ponta a ponta	Integridade e confidencialidade	Segurança/ Prevenção
Precisão e qualidade	Precisão e qualidade	Qualidade dos dados		Qualidade e integridade		Precisão	Qualidade dos dados
Responsabilização (Accountability)	Accountability	Accountability	Execução/ Reparação	Accountability		Accountability	Responsabilização e Prestação de contas

Fonte: Adaptado de Meis (2018) – adicionado o mapeamento dos princípios da LGPD

Meis (2018) observa que a ISO 29100 (ISO/IEC, 2011) fornece os princípios de privacidade mais refinados e uma melhor cobertura deles. O autor também constata que o princípio de *Justiça* (*Fairness*) pode ser visto como um princípio transversal que não é explicitamente listado pela maioria das fontes como princípio separado, mas mencionado

nos princípios de legitimidade da finalidade, minimização de dados e limitação de uso, armazenamento e coleta. O princípio da justiça também cruza os princípios de privacidade de abertura e transparência, acesso, participação individual, consentimento e escolha, especificação de finalidade, segurança e precisão e qualidade. Por fim, Meis (2018) conclui que o princípio de "justiça" deve ser usado como orientação para a implementação dos princípios acima mencionados. A Figura 4 resume a relação entre os princípios do PbD e os princípios descritos nas leis LGPD e GDPR.

Figura 4 – Relação entre os princípios de *Privacy by Design* (PbD), Lei Geral de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR)



Fonte: Elaborada pela autora

2.1.4 Objetivos de Proteção de Privacidade

Hansen, Jensen e Rost (2015) introduzem seis objetivos de proteção para a engenharia de privacidade. Esses objetivos de proteção incluem os três objetivos clássicos de segurança: **confidencialidade**, **integridade** e **disponibilidade** que são reconhecidos como elementos-chave de segurança da informação na literatura e nos padrões, por exemplo, ISO 27000 (ISO/IEC, 2018).

No contexto da privacidade, a *confidencialidade* corresponde a manter segredo e impedir a divulgação de dados pessoais para contrapartes. A *integridade* está fortemente relacionada ao princípio de precisão e qualidade. Ou seja, é necessário garantir que apenas os dados pessoais corretos sejam processados e que o processamento não modifique involuntariamente os dados pessoais processados. A *disponibilidade* do objetivo de proteção visa a disponibilidade dos dados pessoais para fins de processamento acordados pelo titular dos dados e também a possibilidade de os titulares de dados terem acesso aos seus dados pessoais (MEIS, 2018). Hansen, Jensen e Rost (2015) complementam os três objetivos de proteção de segurança com três novos objetivos, são eles: **desconectabilidade**, **transparência** e **interveniência**.

A *desconectabilidade* pode ser vista como uma espécie de meta-confidencialidade. Ou seja, a relação entre dados pessoais ou entre os titulares e seus dados pessoais deve ser mantida em segredo. A desconectabilidade não implica necessariamente que os dados pessoais sejam mantidos em segredo, desde que não permitam a criação de links indesejados. A desconexão inclui o anonimato dos requisitos de privacidade (não deve ser possível vincular dados pessoais ao seu titular), pseudonimato (um pseudônimo é usado para vincular os dados pessoais ao titular) e indetectabilidade (os conselheiros não devem saber sobre a ocorrência de eventos ou a existência de dados pessoais) (MEIS, 2018; HANSEN; JENSEN; ROST, 2015).

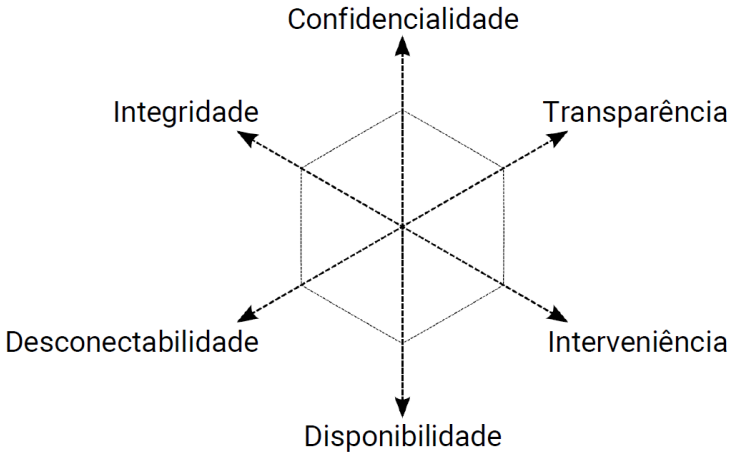
A *transparência* se preocupa em fornecer aos titulares dos dados e às autoridades de supervisão informações sobre como e por que seus dados pessoais são processados e as práticas e procedimentos do controlador. A *interveniência* do objetivo de proteção exige que o controlador forneça medidas para capacitar os titulares de dados a controlar se, como e para quais fins o controlador os processa (MEIS, 2018).

De acordo com Hansen, Jensen e Rost (2015), observando de perto o conjunto completo de objetivos de proteção, pode-se ver que não há possibilidade de garantir 100% de cada um dos objetivos simultaneamente: por exemplo, se um sistema fornece confidencialidade, isso implica que o acesso a determinados dados seja restrito a determinadas entidades – violando a disponibilidade. A integridade conflita com a interveniência, pois o primeiro não permite alterações subsequentes nos dados e processos críticos à integridade, e o último requer exatamente essa capacidade para modificações subsequentes. A transparência e a impossibilidade de conexão também se revelam de natureza conflitante,

pois o primeiro pretende aumentar a compreensão do processamento real dos dados, por exemplo, registrando as ações de usuários e administradores, e o último tenta evitar esse conhecimento, pois pode ser mal utilizado para vínculo não intencional.

Normalmente, cada um desses conflitos pode ser mitigado, dependendo do sistema de TI específico em consideração, mas para o modelo geral de objetivos de privacidade e proteção de dados, esses três pares de objetivos de proteção que afetam mutuamente são representado como oponentes. Portanto, o conjunto completo de aspectos é comumente representado como uma estrela de três eixos, cada um representando um par de objetivos de proteção opostos (Figura 5) (HANSEN; JENSEN; ROST, 2015).

Figura 5 – Objetivos de proteção para a engenharia de privacidade



Fonte: Adaptado de Hansen, Jensen e Rost (2015)

2.1.5 Privacidade versus *Segurança*

As organizações geralmente acreditam que manter os dados confidenciais protegidos contra *hackers* significa que estão em conformidade com os regulamentos de privacidade de dados, porém, este não é o caso. A segurança dos dados e a privacidade dos dados são frequentemente usadas de forma intercambiável, mas existem diferenças entre as mesmas.

> "A privacidade dos dados é focada no uso e controle de dados pessoais - coisas como implementar políticas para garantir que as informações pessoais dos consumidores sejam coletadas, compartilhadas e usadas de maneira apropriada. A segurança se concentra mais na proteção de dados contra ataques maliciosos e na exploração de dados roubados com fins lucrativos. Embora a segurança seja necessária para proteger os dados, não é suficiente para abordar a privacidade." (IAPP, 2020).

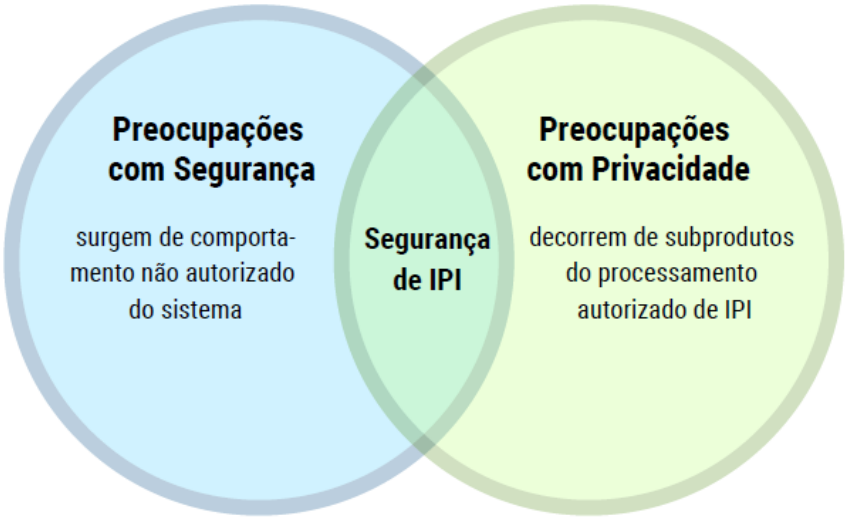
De acordo com NISTIR 8062 (2017) o uso de "privacidade" como um termo separado pressupõe que a privacidade tenha um significado e traga consigo problemas distintos

da segurança. É por isso que é importante entender a relação – particularmente as distinções – entre segurança da informação e privacidade. Isso melhorará a compreensão de como aplicar os processos estabelecidos de engenharia de sistemas e gerenciamento de riscos para tratar de questões de privacidade.

Há um reconhecimento claro de que a confidencialidade da IPI desempenha um papel importante na proteção da privacidade. No entanto, existem problemas de segurança não relacionados à privacidade (por exemplo, confidencialidade de segredos comerciais), assim como há problemas de privacidade não relacionados à segurança. Vários outros FIPPs tratam da criação, coleta, uso, processamento e retenção, disseminação ou divulgação de limitações de uso (NISTIR 8062, 2017).

No modelo de risco de segurança, as preocupações se concentram em atividades não autorizadas que causam perda de confidencialidade, integridade ou disponibilidade de informações ou sistemas. Algumas preocupações com a privacidade surgem de atividades não autorizadas, e também podem surgir com o processamento autorizado de informações sobre indivíduos (NISTIR 8062, 2017). A Figura 6 mostra uma representação não proporcional do relacionamento entre os domínios de privacidade e segurança da informação.

Figura 6 – Relação entre Segurança da Informação e Privacidade



Fonte: NISTIR 8062 (2017)

2.1.6 Paradoxo da Privacidade

As discrepâncias entre as atitudes e comportamentos dos indivíduos são conhecidas como o paradoxo da privacidade, resultado das atitudes divergentes. Pode haver um desejo de proteger a privacidade em geral, mas dependendo dos custos e benefícios de uma situação particular, pode-se decidir não fazê-lo. Calcular custos e benefícios racionalmente é apenas uma parte de como as decisões de privacidade são tomadas. Outro fator que

influencia a tomada de decisão é a percepção errônea de custos e benefícios, normas sociais, emoções e heurísticas.

De acordo com Acquisti, Brandimarte e Loewenstein (2015), informações incompletas e assimétricas são a causa raiz da incerteza da privacidade. Segundo os autores, os indivíduos raramente têm uma compreensão clara de quais informações terceiros, empresas e governos têm sobre eles, como essas informações são usadas ou para que fim isso é feito. Enquanto alguns danos à privacidade são tangíveis, como os custos financeiros associados ao roubo de identidade, muitos outros danos são intangíveis, como estranhos que tomam conhecimento da história de vida de alguém (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Acquisti, Brandimarte e Loewenstein (2015) afirmam que indivíduos que não têm uma compreensão clara de suas preferências e geralmente examinam seus arredores para fornecer orientação. Em termos de privacidade, o contexto pode ser entendido como o grau em que um indivíduo demonstra extrema preocupação ou apatia em relação à sua privacidade, dependendo da situação.

Em relação à privacidade, as intenções declaradas não refletem necessariamente o comportamento dos indivíduos, uma vez que fatores independentes, como o processamento heurístico e a habituação, influenciam a escolha e o comportamento. Ao criar uma relação de confiança com os consumidores, Norberg, Horne e Horne (2007) argumentam que as organizações podem diminuir consideravelmente as preocupações com a privacidade.

Segundo Oliveira, Mattedi e Seabra (2021), as pessoas que usam aplicativos possuem uma relação subjetiva entre "vantagem percebida" e "riscos percebidos". Segundo os autores, quando essa relação é positiva, leva a uma atitude mais aberta em relação à tecnologia, mesmo quando há preocupações com segurança. A relação custo-benefício para dispositivos móveis, segundo os autores, é ainda mais delicada, pois os dispositivos móveis podem coletar dados confidenciais continuamente. Assim, a popularidade das redes sociais e dos aplicativos de compras *online* pode ser vista como o paradoxo da privacidade, pois informações confidenciais podem ser coletadas ou expostas.

De acordo com Kokolakis (2017), existem implicações significativas para o comércio eletrônico, governo eletrônico, redes sociais *online* e regulamentação de privacidade do governo em relação ao paradoxo da privacidade. Uma grande quantidade de informações pessoais é coletada por sites de comércio eletrônico e redes sociais. O autor afirma que o aspecto essencial do paradoxo é o fato de que muitas vezes as intenções de privacidade não levam a comportamentos de proteção. Wu (2018) argumenta que, no contexto das redes sociais online, o "paradoxo da privacidade" pode não ser um paradoxo em si. Em vez disso, as preocupações com a privacidade refletem a ideologia de um eu autônomo, enquanto a auto-revelação responde à necessidade de ser reconhecido pelos outros.

Young e Quan-Haase (2013) afirmam que uma melhor compreensão do paradoxo da privacidade tem implicações para o *design*. O desenvolvimento de políticas de privacidade

que espelhem mais de perto as necessidades e práticas dos usuários pode ser informado pela avaliação de como eles se protegem para desenvolver controles de privacidade que reflitam mais de perto essas estratégias.

2.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei Nº 13.709, foi sancionada em agosto de 2018 e entrou em vigor em setembro de 2020. A LGPD tenta unificar os mais de 40 estatutos diferentes que atualmente governam dados pessoais, *online* e *offline*, substituindo determinados regulamentos e complementando outros.

A LGPD detalha os papéis de quatro diferentes agentes: o titular, o controlador, o operador e o encarregado. A função de cada um dos papéis citados foram descritas anteriormente na subseção 2.1.2. A Figura 7 ilustra os principais objetivos da LGPD.

Figura 7 – Principais objetivos da LGPD

Fonte: LGPD Brasil (2019)

A LGPD aplica-se: aos dados pessoais de indivíduos localizados no Brasil; quando o tratamento se dá no Brasil; quando houver oferta de bens e serviços para indivíduos no Brasil. A LGPD não se aplica: para dados provenientes e destinados a outros países (que apenas transitem pelo território nacional), uso pessoal, uso não comercial, fins jornalísticos, acadêmicos, segurança pública (Lei Nº 13.709, 2018).

O Artigo 18 da LGPD apresenta nove direitos que o titular dos dados pessoais pode obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, são eles: *(i)* confirmação da existência de tratamento; *(ii)* acesso aos dados; *(iii)* correção de dados incompletos, inexatos ou desatualizados; *(iv)* anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; *(v)* portabilidade dos dados a outro fornecedor de serviço ou produto; *(vi)* eliminação dos dados pessoais tratados com o consentimento do titular; *(vii)* informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; *(viii)* informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; *(ix)* revogação do consentimento (Lei Nº 13.709, 2018).

A principal influência para a criação e maturação da LGPD foi o GDPR (*General Data Protection Regulation*), em vigor desde 25 de maio de 2018, que regulamenta a questão da coleta, armazenamento, tratamento e compartilhamento de dados pessoais para os países europeus.

O GDPR passou a ser uma mudança de paradigma na proteção de dados e privacidade, o mesmo foi projetado para garantir a privacidade digital e a minimização de dados. A lei torna o consentimento explícito, onde um usuário deve optar por compartilhar quaisquer dados de Informação Pessoalmente Identificável (IPI) antes que uma empresa possa armazená-los; expande-se a definição de IPI muito além do nome, endereço e data de nascimento tradicionais, abrangendo a localização do usuário (incluindo endereço IP), saúde, dados genéticos (incluindo dados biométricos) e orientação sexual, raça, etnia, crenças religiosas ou opiniões política (KHO, 2018).

O GDPR introduz várias novas disposições que, radicalmente, não conferem direitos individuais, mas tentam criar um ambiente no qual sistemas automatizados menos "tóxicos" serão construídos no futuro. Essas ideias surgem da longa evolução do conceito de *Privacy by Design* (PbD) como uma maneira de criar sistemas sensíveis à privacidade (*privacy-aware*) ou amigáveis à privacidade (*privacy-friendly*), geralmente de maneira voluntária e não obrigatória (EDWARDS; VEALE, 2018).

O GDPR dá, principalmente, dois direitos aos usuários o direito de apagar, ou o direito de ser esquecido. Se os dados não são desejados, tem-se o direito de solicitar sua remoção ou eliminação. Em segundo lugar, o direito de portabilidade, com o qual os avisos aos usuários devem ser claros e precisos quanto aos seus termos, quando se trata de cláusulas de "*opt-in/opt-out*" (DAYALU; PUNNAGAI, 2019).

2.2.1 Diferenças e Similaridades entre LGPD e GDPR

A primeira semelhança que a LGPD compartilha com a GDPR é a unificação de regulamentos anteriormente díspares e muitas vezes contraditórios. Outra semelhança é que a LGPD se aplica a qualquer empresa ou organização que processe os dados pessoais

de pessoas no Brasil, independentemente de onde essa empresa ou organização possa estar localizada. Portanto, se uma empresa possui algum cliente no Brasil, a mesma deve se preparar para a conformidade com a LGPD (GDPR EU, 2020).

A LGPD não possui uma definição única para dados pessoais. A Lei declara em vários lugares que dados pessoais podem significar quaisquer dados que, por si só ou combinados com outros dados, possam identificar uma pessoa natural ou submetê-los a um tratamento específico. A LGPD tem uma visão ampla de quais dados se qualificam como dados pessoais, ainda mais expansivos que a GDPR (GDPR EU, 2020).

O Artigo 18 é outra seção da LGPD que parecerá familiar para as empresas que lidaram com a conformidade com a GDPR, onde são apresentados nove direitos que o titular dos dados pode obter do controlador (citados na seção 2.2). Embora a GDPR seja conhecida por conceder a seus titulares oito direitos fundamentais, estes são essencialmente os mesmos direitos mencionados pela LGPD. Parece que a LGPD dividiu "o direito a informações sobre entidades públicas e privadas com as quais o controlador compartilhou dados" do "direito de ser informado" mais geral da GDPR para torná-lo mais explícito (GDPR EU, 2020).

Ambos os atos exigem que empresas e organizações contratem um DPO (*Data Protection Officer*). No entanto, enquanto a GDPR delineia quando um DPO é necessário, o Artigo 41 na LGPD simplesmente diz: "o controlador deverá indicar o encarregado pelo tratamento de dados pessoais", o que sugere que qualquer organização que processe os dados de pessoas no Brasil precisará contratar um DPO (GDPR EU, 2020).

No que diz respeito ao que se qualifica como base legal para o processamento de dados, a GDPR possui seis bases legais para processamento, e um controlador de dados deve escolher uma delas como justificativa para o uso das informações de um titular de dados. No entanto, no artigo 7, a LGPD lista 10 (GDPR EU, 2020).

Com relação a denúncia sobre violações de dados à autoridade local de proteção de dados, ambas LGPD e GDPR exigem que as organizações o façam. A GDPR deixa explícito que " uma organização deve relatar uma violação de dados dentro de 72 horas após sua descoberta.". Todavia, a LGPD não estabelece um prazo firme: o artigo 48 apenas declara que "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. (...) A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional (...).". Entretanto, como a ANPD ainda não foi estabelecida, não há orientação para o que constitui um "período de tempo razoável" (GDPR EU, 2020).

Outra diferença significativa entre a LGPD e a GDPR é correlação às multas. As multas máximas da GDPR são substanciais, exigindo que as organizações que cometem graves violações até € 20 milhões de euros ou 4% da receita anual global, o que for maior. As multas sob a LGPD são muito menos severas. O artigo 52 declara que a multa máxima por violação é de "até 2% do faturamento da pessoa jurídica de direito privado, grupo ou

conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões de reais por infração" (cerca de € 11 milhões de euros) (GDPR EU, 2020).

2.3 Desafios da Implantação da LGPD

Para a se adaptar ao que diz a norma é possível elencar três desafios principais nesse esforço: o mapeamento dos processos que envolvem dados pessoais; a revisão de contratos com fornecedores ou consumidores quando necessário e a mudança de cultura dentro de cada organização (Agência Brasil, 2020).

O primeiro passo é realizar um levantamento preliminar, que visa entender onde há tratamento de dados na organização. O segundo momento é o de produzir um inventário dos dados pessoais e dos procedimentos adotados quem envolvem esses registros, bem como de que maneira cada tratamento se dá e quais suas implicações. A terceira etapa tem como foco a classificação dos dados, ponto em que deve ser separado o conjunto de dados de constitui informações pessoais (Agência Brasil, 2020).

Após entender o que deve ser trabalhado, mapear os dados e classificá-los, deve-se promover a adequação ao que fala a lei, envolvendo: mudanças de processos, a implantação de ferramentas de gestão dos dados e eventuais ajustes jurídicos (por exemplo, alteração de contratos). A iniciativa mais importante, de acordo com o advogado Márcio Cots, é a mudança de cultura da organização (Agência Brasil, 2020).

Deve-se regularizar as atividades já transformadas, dessa maneira, é preciso identificar nos processos onde há riscos de responsabilização. E assim, adotar procedimentos como a anonimização ou até mesmo o descarte dos dados. Outra alternativa é obter consentimento dos usuários para determinadas finalidades pretendidas (Agência Brasil, 2020). As empresas devem documentar procedimentos entre o controlador e o operador para facilitar a demonstração dos processos à Autoridade Nacional de Proteção de Dados (ANPD). Ademais, as empresas devem promover ações educativas e treinamentos aos seus membros e colaboradores visando à mitigação de riscos e a devida informação aos titulares de dados (ICMP Consultoria em TI, 2020).

O advogado Márcio Cots recomenda a formulação de quatro políticas, são elas: *(1)* Política de gestão de dados, com caráter mais geral; *(2)* Política de tratamento de dados, com caráter de orientação interno; *(3)* Política de privacidade aos consumidores ou usuários externos de bens e serviços, explicitando quais dados são coletados, para qual finalidade e de que maneira estes são tratados; *(4)* Política de segurança da informação, que discrimine as ações empregadas para evitar vazamentos e proteger os registros tratados pelo ente (Agência Brasil, 2020).

A LGPD Brasil (2019) e ICMP Consultoria em TI (2020) listam 11 passos para implantar a LGPD em uma organização. São eles:

1. Estudo da LGPD e demais leis que regulamentam o seu negócio;

2. Mapear a entrada e o tratamento dos dados pessoais;
3. Mapear os riscos do tratamento;
4. Elaborar o Relatório de Impacto (PIA);
5. Criar a política de proteção de dados e adaptar os documentos internos e externos;
6. Gerenciar os pedidos dos titulares e dos órgãos;
7. Treinamento das equipes que tratam dados pessoais;
8. Ser *compliance* com a proteção de dados mediante governança;
9. Exigir o *compliance* da proteção de dados de seus fornecedores;
10. Concepção de novos produtos com o princípio de privacidade desde a concepção (PbD);
11. Eleger um DPO com conhecimentos regulatórios sobre proteção de dados.

3 TRABALHOS RELACIONADOS

Para identificar como é realizada a elaboração de uma Avaliação de Impacto de Privacidade, ou relatório de impacto à proteção de dados pessoais (conforme Art. 5º - XVII da LGPD), foi conduzida uma Revisão Sistemática da Literatura (RSL).

3.1 Revisão Sistemática da Literatura (RSL)

Conforme apresentado no Capítulo 1, com a entrada em vigor da Lei LGPD, a Avaliação de Impacto de Privacidade será um artefato essencial para as empresas que processam dados pessoais no Brasil anteciparem e evitarem eventos invasivos de privacidade, sendo uma atividade útil e positiva à conformidade jurídica. Dessa forma, a revisão de literatura teve como objetivo investigar o que tem sido reportado sobre a metodologia aplicada para a elaboração deste relatório.

Com base no procedimento definido por Kitchenham et al. (2009), foram realizadas as seguintes atividades: especificação das questões de pesquisa (veja a Subseção 3.1.1), definição do processo de pesquisa, composto pela estratégia de busca, filtragem e os critérios para avaliação da qualidade do estudo (veja a Subseção 3.1.2), por fim, foi executado o processo de extração (veja a Subseção 3.1.3) e síntese de dados (veja a Subseção 3.1.4). A subseção 3.1.5 discute e aborda as principais conclusões sobre os resultados encontrados com a RSL.

3.1.1 Questões de Pesquisa da RSL

Para este estudo, foram definidas cinco questões de pesquisa (QP):

QP1. Quais metodologias existem para conduzir uma Avaliação de Impacto de Privacidade - *Privacy Impact Assessment* (PIA)?

QP2. Quais artefatos são obtidos com a realização de uma Avaliação de Impacto de Privacidade?

QP3. Quais ameaças à privacidade foram abordadas na metodologia de Avaliação de Impacto de Privacidade?

QP4. Em quais contextos é aplicada a Avaliação de Impacto de Privacidade?

QP5. As metodologias para realizar uma Avaliação de Impacto de Privacidade fazem referência a lei (LGPD, GDPR, etc.)? Se não fazem, estão adequadas as exigências da lei?

3.1.2 Processo de Pesquisa da RSL

A pesquisa começou em agosto de 2019 e não foi imposta qualquer restrição com relação à data de publicação dos artigos.

A *string* de busca realizada foi baseada nos termos "*privacy impact assessment*" e "*methodology*". Como sinônimos para "*methodology*" foram utilizados: "*method*", "*procedure*", "*plan*", "*design*", "*strategy*", "*approach*", "*blueprint*" e "*technique*". Como fontes primárias de busca, foram utilizadas as seguintes bibliotecas digitais online: ACM Digital Library, IEEE Xplore, Science Direct e Google Scholar. Essas bibliotecas foram selecionadas pois atendem aos seguintes critérios: *(i)* o banco de dados de publicação é atualizado regularmente; *(ii)* os manuscritos estão disponíveis para download; *(iii)* os manuscritos são revisados por um processo de revisão por pares; *(iv)* e, na maior parte, eles são capazes de lidar com consultas avançadas. A *string* de busca foi aplicada aos metadados (títulos, resumos e palavras-chave) nas bibliotecas digitais selecionadas. A Tabela 1 apresenta a *string* de busca aplicada em cada uma das bibliotecas e a quantidade de resultados

encontrados.

Tabela 1 – Operacionalização da *string* de busca

Base de Dados	**String de Busca**	**Número de Resultados**
Google Scholar[1]	"privacy impact assessment" + methodology | procedure | plan | design | strategy | approach | method | blueprint | technique -site	2800
IEEE Xplore Digital Library[2]	(("All Metadata": privacy impact assessment) AND ("All Metadata": methodology OR "All Metadata": procedure OR "All Metadata": plan OR "All Metadata": design OR "All Metadata": strategy OR "All Metadata": approach OR "All Metadata": method OR "All Metadata": blueprint OR "All Metadata": technique))	96
Science Direct[3] [4]	(("privacy impact assessment") AND (methodology OR procedure OR plan OR design OR strategy OR approach OR method OR blueprint OR technique))	291
ACM Digital Library[5]		8
Total		**3195**

[1] <https://scholar.google.com.br/scholar?q=%22privacy+impact+assessment%22+%2B+methodology+%7C+procedure+%7C+plan+%7C+design+%7C+strategy+%7C+approach+%7C+method+%7C+blueprint+%7C+technique+-site&hl=pt-BR&as_sdt=0,5> [2] <https://ieeexplore.ieee.org/search/searchresult.jsp?action=search&matchBoolean=true&newsearch=true&queryText=(((%22All%20Metadata%22:%20privacy%20impact%20assessment)%0AAND%20(%22All%20Metadata%22:%20methodology%20OR%20%10All%0AMetadata%11:%20procedure%20OR%20%22All%20Metadata%22:%0Aplan%20OR%20%22All%20Metadata%22:%20design%20OR%20%10All%0AMetadata%11:%20strategy%20OR%20%22All%20Metadata%22:%20approach%0AOR%20%22All%20Metadata%22:%20method%20OR%20%10All%0AMetadata%11:%20blueprint%20OR%20%22All%20Metadata%22:%0Atechnique)))> [3] <https://www.sciencedirect.com/search?qs=%28%28%22privacy%20impact%20assessment%22%29%20AND%20%28%0Amethodology%20OR%20procedure%20OR%20plan%20OR%0Adesign%20OR%20strategy%29%29>

[4] <https://www.sciencedirect.com/search?qs=%28%28%22privacy%20impact%20assessment%22%29%20AND%20%28approach%20OR%20method%20OR%20blueprint%20OR%20technique%29%29>

[5] <https://dl.acm.org/action/doSearch?fillQuickSearch=false&target=advanced&expand=dl&AllField=AllField%3A%28%22privacy+impact+assessment%22%29+AND+AllField%3A%28methodology+OR+procedure+OR+plan+OR+design+OR+strategy+OR+approach+OR+method+OR+blueprint+OR+technique%29>

Fonte: Elaborada pela autora

Para a inclusão de um artigo, sua relevância foi determinada pela sua relação com a questão de pesquisa, por meio da análise do título, resumo e palavras-chave. O Quadro 2 apresenta os critérios de inclusão (CI) e critérios de exclusão (CE) que foram definidos. O processo de seleção dos estudos foi dividido em três etapas. Para a primeira etapa, somente foram avaliados os títulos, resumos e palavras-chave dos estudos com base nos critérios de inclusão e exclusão. Para a segunda etapa, foram lidas as seções de introdução e conclusão, também considerando os critérios de inclusão e exclusão. Para a terceira etapa, foi realizada a leitura do texto do estudo por completo para avaliar a qualidade do estudo.

Quadro 2– Critérios de inclusão e exclusão

Critérios de Inclusão	Artigos com foco no contexto dessa RSL
	Artigos revisados por pares
	Escrito em inglês ou português
Critérios de Exclusão	Estudos disponíveis apenas na forma de resumo (*abstract*) ou apresentações
	Artigos de discussão e opinião
	Duplicatas ou trabalhos repetidos em mais de uma fonte

Fonte: Elaborado pela autora

Para identificar os estudos mais relevantes que foram usados para responder às questões de pesquisa, foram formuladas cinco perguntas de controle de qualidade para avaliar a relevância, a integridade e a qualidade dos estudos. As perguntas para avaliação do critério de qualidade (CQ) dos estudos foram:

CQ1. O estudo compara e contrasta diferentes fontes de conhecimento sobre a mesma questão?

CQ2. Todos os passos do método foram definidos/descritos por completo (ferramentas)?

CQ3. Os pesquisadores avaliaram a qualidade/validade do método de PIA apresentado?

CQ4. O estudo apresenta evidência de adaptação e resposta do método a necessidades e problemas oferecidos pela vida real?

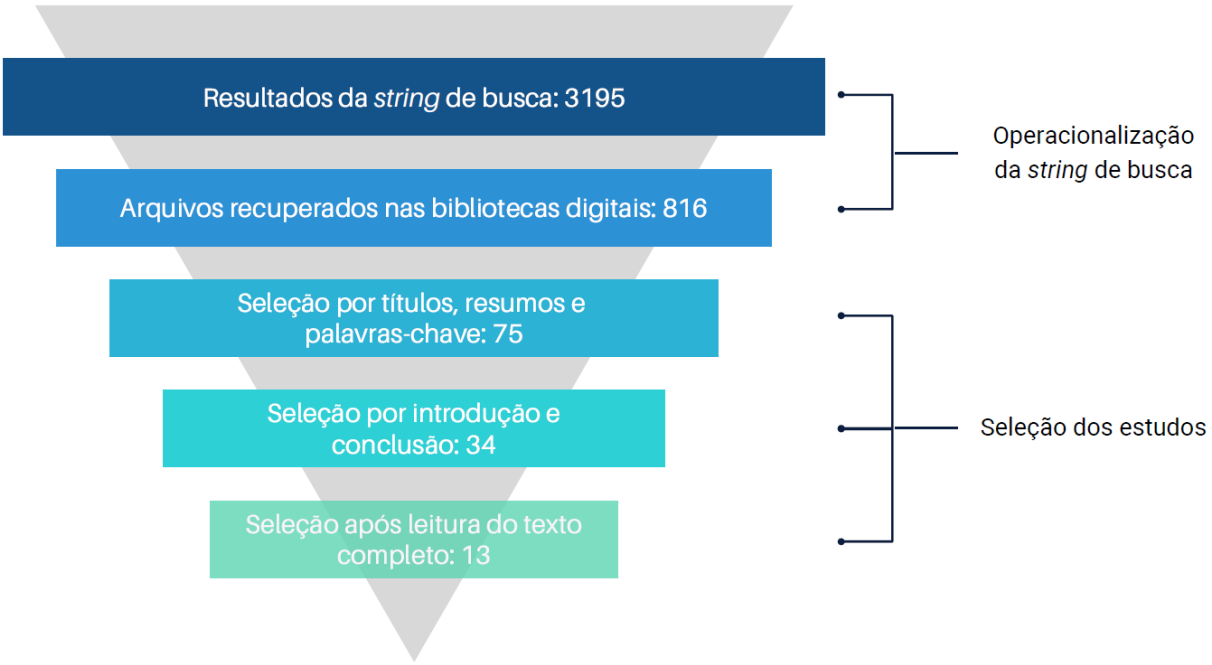
CQ5. Podem ser extraídas generalizações das conclusões oferecidas para a aplicação do método voltado a outros contextos (por exemplo, aplicações móveis e *Websites*)?

Para cada pergunta existem 3 opções de resposta: Sim (S) = 1 ponto, Parcial (P) = 0,5 ponto e Não (N) = 0 pontos. Dessa maneira, o cálculo da pontuação geral de qualidade foi realizado somando-se a pontuação relatada nos cinco critérios individuais. Assim, a

pontuação de qualidade total de cada estudo variou de 0 (muito ruim) a 5 (muito bom), e o trabalho foi selecionado apenas se obteve pelo menos um total de 4 pontos (bom).

A Figura 8 apresenta o número de artigos encontrados nas bibliotecas digitais após a execução da *string* de busca, devido a limitações para *download* dos resultados encontrados no Google Scholar, a quantidade de arquivos recuperados foi bem menor; na sequência, são apresentados o total de artigos que foram mantidos em cada uma das etapas de seleção.

Figura 8 – Processo de seleção dos estudos



Fonte: Elaborada pela autora

3.1.3 Artigos Selecionados com a RSL

Durante a pesquisa sistemática foram selecionados 13 artigos que apresentaram metodologias de elaboração de Avaliação de Impacto de Privacidade e que atendiam aos critérios e respondiam as questões de pesquisa estipuladas. No Quadro 3 são descritos o nome do(s) autor(es), o título do trabalho e em qual repositório de artigos científicos/periódico/conferência/*workshop* o trabalho encontrado foi apresentado.

Quadro 3– Artigos selecionados pela Revisão Sistemática da Literatura

Autor(es)	**Título**	**Repositório**
Harbird et al. (2008)	Privacy Impact Assessment with PRAIS	PETS
Wright (2013)	Making Privacy Impact Assessment More Effective	TIS
Oetzel e Spiekermann (2014)	A Systematic Methodology for Privacy Impact Assessments: a Design Science Approach	EJIS
Himmel et al. (2015)	Privacy Points as a Method to Support Privacy Impact Assessments	TELERISE
Meis e Heisel (2015)	Systematic Identification of Information Flows from Requirements to Support Privacy Impact Assessments	ICSOFT
Notario et al. (2015)	PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology	SPW
Wang e Nepali (2015)	Privacy Impact Assessment for Online Social Networks	CTS
Bieker et al. (2016)	A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation	APF
Reuben et al. (2016)	Privacy Impact Assessment Template for Provenance	ARES
Wang e Liu (2016)	An Attribute-based Statistic Model for Privacy Impact Assessment	ICCTS
Ahmadian et al. (2018)	Supporting Privacy Impact Assessment by Model-based Privacy Analysis	SAC
Wuyts et al. (2018)	Effective and Efficient Privacy Threat Modeling Through Domain Refinements	SAC
Al-Momani et al. (2019)	A Privacy-Aware V-Model for Software Development	SPW

Fonte: Elaborado pela autora

3.1.4 Resultados da RSL

Nas subseções seguintes, são apresentadas as respostas às questões de pesquisa.

[QP1] Quais metodologias existem para conduzir uma PIA?

No estudo de Harbird et al. (2008) é apresentado a metodologia PRAIS – Análise de Impacto de Privacidade para Compartilhamento de Informações. O objetivo do projeto PRAIS é desenvolver uma ferramenta baseada em políticas que possa analisar as decisões de compartilhamento de informações sob demanda.

Wright (2013) trabalhou em um projeto de 22 meses, chamado PIAF, acrônimo para Framework de Avaliação de Impacto de Privacidade. O projeto analisou as metodologias de PIA existentes nos países com mais experiência em PIA, ou seja, Austrália, Canadá, Irlanda, Nova Zelândia, Reino Unido e EUA.

Oetzel e Spiekermann (2014) propuseram uma metodologia que considera sistematicamente questões de privacidade usando um passo a passo para uma Avaliação de Impacto de Privacidade (PIA). Os autores desenvolveram uma metodologia de PIA de sete etapas, baseada no método de risco BSI, amplamente adotado. Uma PIA é acionada quando um novo sistema é planejado ou um existente é atualizado.

Outra proposta encontrada é no estudo de Himmel et al. (2015), no qual é apresentada uma abordagem de pontos de privacidade, em que à regulamentação de privacidade baseia-se na quantificação de aspectos que afetam a privacidade das pessoas. A ideia dos autores é transferir os princípios-chave do conceito de eco-pontos para o domínio da privacidade. A abordagem de pontos de privacidade consiste em recursos quantitativos, que permitem avaliar o nível de privacidade dos produtos de maneira quantitativa.

No estudo de Meis e Heisel (2015) foi realizada uma extensão do método de análise de privacidade baseada em problemas (ProPAn), que deriva as informações necessárias para conduzir uma PIA a partir de um modelo de requisitos na notação de estrutura de problemas. Os autores utilizaram uma estrutura UML4PF para criar modelos de quadros de problemas como diagramas de classes UML. O ProPAn estende a estrutura UML4PF com um perfil UML para requisitos de privacidade e uma técnica de raciocínio. Esse método é baseado em um modelo de requisitos na notação de quadro de problemas e, portanto, pode ser iniciado no início do processo de desenvolvimento de software, quando ainda é possível influenciar o projeto de software.

Notario et al. (2015) trabalharam no projeto financiado pela União Europeia (UE), PRIPARE (Preparando a Indústria para a Privacidade por Design, apoiando sua Aplicação em Pesquisa). O PRIPARE contribui, em primeiro lugar, para o fornecimento de um ponto de vista duplo, integrando abordagens baseadas em risco e orientadas a objetivos; e, em segundo lugar, integra a privacidade como um atributo na análise arquitetônica. A metodologia do PRIPARE combina explicitamente as duas abordagens, recomendando

uma abordagem orientada a objetivos que reduz a incerteza de privacidade em um estágio inicial do processo de desenvolvimento; e uma abordagem de análise do sistema para os riscos restantes específicos do sistema, identificando o tratamento adequado de acordo com vários fatores, como o nível de risco. No final, alguns riscos residuais podem permanecer, os quais devem ser identificados e documentados.

Wang e Nepali (2015) propõem uma abordagem de análise quantitativa para avaliar o impacto na privacidade das redes sociais *online*. Dois desafios específicos são considerados no artigo: a avaliação do impacto na privacidade quando informações parciais do usuário são divulgadas e a avaliação do impacto na privacidade quando um grupo de contas de usuário são comprometidas.

O estudo de Bieker et al. (2016) apresentam um processo que operacionaliza os requisitos estabelecidos pelo GDPR, garantindo a atenção adequada aos direitos fundamentais. Incorpora os novos requisitos da legislação e pode ser adaptado para atender às necessidades do controlador de dados. O processo consiste em três estágios: estágio de preparação, estágio de avaliação, relatório e estágio de salvaguardas.

Reuben et al. (2016) projetaram um modelo de Avaliação de Impacto na Privacidade (PIA) para identificar ameaças iminentes à privacidade que surgem de grafos de proveniência em uma configuração independente de aplicativo. Os dados de proveniência podem ser expressos como um grafo com links informando quem e quais atividades criaram, usaram e modificaram entidades. A semântica desses links e o raciocínio específico do domínio podem suportar a inferência de informações adicionais sobre os elementos no grafo. No qual, tais inferências podem revelar links inesperados entre elementos, expondo assim os dados pessoais além das intenções de um indivíduo.

O artigo de Wang e Liu (2016) propõem o desenvolvimento de um modelo estatístico baseado em atributos para medição da exposição à privacidade e avaliação de impacto na privacidade, com base em mineração de texto e aprendizado de máquina, baseado em informações pessoais identificáveis (IPI). O modelo inclui três componentes principais: atributos de privacidade, sensibilidades de privacidade e correlações de atributos. Atributos de privacidade são os atributos que podem afetar a privacidade, os quais descrevem o que é privacidade e o que inclui. Sensibilidades à privacidade descrevem como um atributo afeta a privacidade. As correlações de atributos descrevem como os atributos estão relacionados.

Ahmadian et al. (2018) propõem uma nova metodologia para dar suporte à PIA, realizando análises de privacidade e segurança baseadas em modelos nas fases iniciais do desenvolvimento do sistema. No entanto, também pode ser usado para realizar uma PIA em sistemas existentes. Na metodologia proposta pelos autores, o *design* de um sistema é analisado e, quando necessário, são sugeridos controles apropriados de segurança e privacidade para melhorar o design. A análise é realizada de maneira baseada em modelo, com base em um conjunto de verificações de privacidade e segurança.

O trabalho de Wuyts et al. (2018) apresentam uma abordagem para melhorar o LINDDUN, um método de engenharia de privacidade existente. Os autores criam um questionário de refinamento de domínio, que envolve a ativação e desativação de nós de árvores de ameaças, colocando perguntas específicas ao engenheiro de privacidade ou arquiteto de software, levando à exclusão a priori de ameaças não aplicáveis a análise. O questionário é estruturado de acordo com dois níveis diferentes de abstração: perguntas específicas da aplicação e perguntas específicas do diagrama de fluxo de dados (DFD).

Por fim, os autores Al-Momani et al. (2019) propõem o novo modelo W como uma extensão do modelo V com reconhecimento de privacidade, frequentemente usada na engenharia de software. Um estágio do modelo W lida com a análise da privacidade no sistema em que os engenheiros de privacidade realizam uma avaliação de impacto na privacidade, a fim de desencadear ameaças à privacidade e encontrar uma contramedida adequada para remediar cada ameaça, nas quais são requisitos que as contramedidas precisam atender para serem selecionados.

[QP2] Quais artefatos são obtidos com a realização de uma PIA?

No estudo de Harbird et al. (2008) a apresentação da decisão de compartilhamento de informações ao usuário é realizada como um relatório resumido na tela, evidenciando os motivos pelos quais o compartilhamento de informações é recomendado ou desencorajado. É realizada a avaliação das implicações de privacidade das ações de compartilhamento de informações dinamicamente, de forma a compartilhar informações com confiança, verbal ou eletronicamente.

No estudo de Oetzel e Spiekermann (2014) os artefatos obtidos em cada etapa do processo ajudam os profissionais e pesquisadores a entenderem o cenário relevante da regulamentação de privacidade e a analisar e avaliar problemas de privacidade. Os artefatos fornecem suporte sistemático para representar os requisitos de privacidade na forma de alvos de privacidade, avaliando quanta proteção esses alvos requerem e identificando sistematicamente ameaças e controles adequados.

Himmel et al. (2015) quantificam os aspectos de interesse; as métricas de privacidade atribuem valores (geralmente numéricos) a aspectos que afetam a privacidade em produtos e serviços.

A saída final do método de Meis e Heisel (2015) resume devido a quais requisitos, fatos ou suposições os dados pessoais fluem pelo sistema e podem ser usados como entrada para criar um relatório de PIA. O modelo UML contém: os dados pessoais das partes interessadas que são usados no sistema; as informações em que domínio do sistema, quais dados pessoais estão disponíveis e em que qualidade; links de rastreabilidade para identificar os requisitos, fatos e suposições que levam aos fluxos de informações; para cada domínio, pode-se derivar o conjunto de contra-partes interessadas que possivelmente têm acesso aos dados pessoais disponíveis no domínio que eles não deveriam poder acessar.

No estudo de Notario et al. (2015) as principais conclusões e quais elementos foram introduzidos na metodologia do PRIPARE são: cumprimento do quadro jurídico, medição do impacto, medição do risco e abordando questões de privacidade. O PRIPARE reconhece 8 fases principais da metodologia PbD: análise, projeto, implementação, verificação, liberação, manutenção, desativação e ambiente e infraestrutura.

A abordagem proposta por Wang e Nepali (2015) pode ser usada para avaliação de impacto na privacidade quando informações parciais do usuário são divulgadas ou quando um grupo de contas de usuário é comprometido. A perda e o impacto indiretos de dados devido à inferência e agregação de dados também podem ser avaliados.

A metodologia de Bieker et al. (2016) fornece um instrumento conveniente para os controladores de dados avaliarem riscos e lhes permite oferecer melhores serviços e aprimora sua capacidade de competir em um mercado de soluções favoráveis à privacidade, que também incorpora os requisitos impostos pela legislação da União Europeia em vigor.

Reuben et al. (2016) orientam sistematicamente os projetistas de sistemas de proveniência para reduzir as violações de privacidade que surgem em seus aplicativos. O modelo de PIA fundamenta a análise de riscos de privacidade na proveniência e foi projetado para ajudar os desenvolvedores de aplicativos que registram a proveniência sobre: a razão sobre ameaças à privacidade decorrentes da proveniência; e a gerenciar as ameaças identificadas e definir contramedidas.

Wang e Liu (2016) propõem o desenvolvimento de um modelo preciso para IPI para resolver desafios de privacidade, como medição de privacidade, avaliação de perda de dados, elaboração de políticas, etc.

Ahmadian et al. (2018) avaliam os resultados da análise e identificam ameaças e atividades prejudiciais que podem explorar as falhas e violações do projeto nos resultados da análise. Especificam o impacto das falhas e ameaças de *design* identificadas em um sistema. As metas de privacidade são derivadas dos princípios legais de privacidade prescritos nos regulamentos de proteção de dados. Na metodologia de PIA é fornecido um catálogo de controles de privacidade e segurança.

O estudo de Wuyts et al. (2018) apresenta como artefatos a remoção antecipada de ameaças não aplicáveis e desprezíveis (eficácia) e convergência mais rápida para o conjunto de ameaças relevantes, aplicáveis e de alta prioridade à privacidade (eficiência).

O estudo de Al-Momani et al. (2019) propõe soluções para realizar a elicitação de ameaças de privacidade. Com o objetivo de desencadear ameaças à privacidade e encontrar as medidas técnicas correspondentes para mitigar as ameaças desencadeadas.

[QP3] Quais ameaças à privacidade foram abordadas na metodologia de PIA?

Dentre os estudos avaliados, houve dois estudos que não explicitaram quais ameaças à privacidade a metodologia proposta abordava (WUYTS et al., 2018; AL-MOMANI et al., 2019). Sendo que Al-Momani et al. (2019) cita o levantamento de existência de

contramedidas adequadas para tratar cada tipo de ameaça.

Os demais estudos demonstram como foco principal ameaças relacionadas à informação. O PRAIS é um projeto criado para funcionar como parte de uma estrutura de avaliação de risco que avalia a previsibilidade de determinados resultados de compartilhamento de informações, podendo ser usado pelos profissionais em uma base ad hoc para explorar implicações de privacidade, onde as informações serão compartilhadas verbalmente (HARBIRD et al., 2008). O estudo de Oetzel e Spiekermann (2014) cita a qualidade dos dados, processando legitimidade, o direito de informação do titular dos dados, o direito de acesso do titular dos dados, o direito do sujeito de objeção de dados, a segurança de dados e a prestação de contas. Himmel et al. (2015) focam em tópicos como a coleta de dados, divulgação de dados, processamento de dados, aspectos de comunicação, configurações de usuário relacionadas à privacidade e outros índices sobre a aplicação da política de privacidade em uma empresa. Meis e Heisel (2015) tratam sobre o fluxo de informações, no qual para cada requisito de privacidade, o fluxo de informações a partir da parte interessada e os recursos de acesso da parte interessada são visualizados em um grafo de ameaças à privacidade, obtendo-se informações sobre a disponibilidade e a vinculação de dados pessoais nos domínios do sistema.

Notario et al. (2015) abordam sobre o relacionamento entre os requisitos de privacidade referentes a ameaças específicas e/ou princípios de alto nível que garantem a rastreabilidade e a responsabilidade de todo o processo de análise e design. Wang e Nepali (2015) focam no entendimento de como a privacidade de um usuário é afetada. Em seu estudo de 2016, Wang e Liu (2016), voltam a abordar sobre os ataques as informações pessoalmente identificáveis, as quais podem resultar no roubo de identidade. Bieker et al. (2016) afirmam que um DPIA permite uma melhor tomada de decisão no estágio de implementação e evita a necessidade de melhorias subsequentes dispendiosas ou possíveis vazamentos de dados pessoais. Reuben et al. (2016) apresentam foco em questões de privacidade para proveniência, o que os mesmos afirmam ser um facilitador da transparência e da responsabilidade. Ahmadian et al. (2018) identificam ameaças e atividades prejudiciais que podem explorar as falhas e violações do projeto nos resultados da análise.

[QP4] Em quais contextos é aplicada a PIA?

As metodologias de PIA avaliadas podem ser aplicadas ou visam ser aplicadas em:

1. O protótipo de Harbird et al. (2008) demonstra como o PRAIS pode ser usado na rotina diária de um assistente social. O PRAIS visa fazer parte integrante do processo comercial diário de compartilhamento de informações, podendo ser aplicado a uma ampla gama de setores da indústria, como finanças, educação e saúde.

2. Oetzel e Spiekermann (2014) consideram que a metodologia proposta pode ser formalmente integrada ao processo de desenvolvimento de sistemas e gerenciamento de

riscos existentes dentro de contextos organizacionais: pequenas empresas iniciantes, médias e grandes empresas. Todavia, a mesma foi testada apenas em um contexto teórico.

3. O método de Himmel et al. (2015) avalia o nível de proteção da privacidade de produtos e serviços individuais, no qual o procedimento pode ser adotado para vários setores, definindo catálogos específicos.

4. Meis e Heisel (2015) utilizam um subsistema de um sistema eletrônico de saúde (EHS) para ilustrar o método, cuja a ferramenta precisa ser analisada em mais detalhes quanto à usabilidade e aceitação do usuário.

5. O PRIPARE de Notario et al. (2015) foi aplicado a um cenário de cobrança de veículos elétricos. De acordo com os autores, a metodologia é validada na prática, em termos de ser eficiente, prática e alinhada às práticas de engenharia de sistemas do mundo real.

6. O estudo de Wang e Nepali (2015) fornece um documento com uma abordagem de análise quantitativa para agências governamentais, empresas e organizações para avaliar o impacto na privacidade das redes sociais *online* quando ocorre um incidente de segurança.

7. O estudo de Bieker et al. (2016) foi testado e aprovado na prática nos projetos da União Europeia PIAF e SAPIENT em uma extensa avaliação empírica dos esquemas de PIA existentes que os autores realizaram em colaboração com a Trilateral Research.

8. Reuben et al. (2016) validaram o método proposto para configurações específicas de aplicativos de proveniência, como fluxos de trabalho científicos e sistema de informações de assistência médica.

9. Ahmadian et al. (2018) avaliam a metodologia com base em três estudos de caso industriais e realizam uma comparação baseada em qualidade com o estado da arte.

10. Al-Momani et al. (2019) preveem que o modelo W seja usado em organizações que seguem o modelo V para desenvolvimento de *software* e que desejam projetar e introduzir sistemas de preservação da privacidade.

Para os três estudos faltantes, Wright (2013), Wang e Liu (2016), Wuyts et al. (2018), não ficou evidente em qual contexto a metodologia proposta seria aplicável.

[QP5] As metodologias para realizar uma PIA fazem referência a lei (LGPD, GDPR, etc.)? Se não fazem, estão adequadas as exigências da lei?

Dos treze estudos selecionados, seis estudos não fazem referência a nenhuma legislação. O estudo de Bieker et al. (2016) cita sobre o Artigo 35 do GDPR que prescreve sobre a execução de uma Avaliação de Impacto na Proteção de Dados (DPIA). Em observância aos princípios definidos para as atividades de tratamento de dados pessoais (Artigo 6 - LGPD), o estudo de Harbird et al. (2008) demonstra-se adequado a exigência dos itens: III - necessidade - limitação do tratamento ao mínimo necessário; I - finalidade - tratamento para propósitos legítimos. O estudo de Himmel et al. (2015) demonstra compatibilidade com o item VII - segurança - utilização de medidas aptas a proteger os dados pessoais. Meis e Heisel (2015) cita o rascunho da GDPR e sua metodologia demostra auxiliar no item VIII - prevenção - prevenir a ocorrência de danos em virtude do tratamento.

Demais estudos analisados, explicitamente abordam sobre medidas legislativas em vigor, mais comumente, a GDPR que entrou em vigor em 24 de maio de 2016 e se tornou aplicável a partir de 25 de maio de 2018. Oetzel e Spiekermann (2014) afirmam que as metas de privacidade propostas foram sistematicamente derivadas de requisitos legais de proteção de dados e princípios de privacidade. Em particular, a lista proposta de metas de privacidade pode e deve ser adaptada à legislação e regulamentação nacional ou regional ou tecnologia ou regulamentação específica do setor.

O estudo de Notario et al. (2015) apresenta os pontos da metodologia indicando a sua conformidade com artigos do GDPR, abordando o princípio de responsabilidade e o empoderamento e a usabilidade do usuário, um dos principais desafios da PbD. Reuben et al. (2016) cita sobre um dos principais direitos dos titulares de dados, onde os indivíduos têm o direito de: (a) acessar seus dados pessoais e (b) ser informados sobre o processamento de dados e seus propósitos. Bem como os conceitos de transparência e responsabilidade. Ahmadian et al. (2018) apresentam os pontos da metodologia indicando a sua conformidade com artigos do GDPR, os autores indicam que a metodologia facilita o Privacy by Design, conforme prescrito no artigo 25 do GDPR. Por fim, o estudo de Al-Momani et al. (2019) aponta a indicação de contramedidas adequadas, demonstrando conformidade com o item VII - segurança - do artigo 6 da LGPD.

3.1.5 Discussão

Os regulamentos de privacidade solicitam aos engenheiros de *software* que sigam os princípios do *Privacy by Design* (PbD) e apliquem soluções de proteção de dados em seus projetos. No entanto, os engenheiros de *software* estão acostumados a pensar em termos de sistemas e software: suas habilidades habituais incluem trabalhar com, por exemplo, modelos de fluxo de dados, estruturas de banco de dados ou arquiteturas de implantação do sistema em desenvolvimento. Dessa forma, há uma certa dificuldade em traduzir

questões regulatórias em itens de trabalho e atividades operacionais para os projetos que gerenciam. Não tendo conhecimento de quais ameaças específicas seus usuários enfrentam, que medidas técnicas devem optar para atender aos direitos do usuário, se os direitos de acesso ou portabilidade implicam na vulnerabilidade do bancos de dados, etc. (MARTIN; KUNG, 2018).

De acordo com Wright (2013), uma PIA deve ser utilizada mais do que para simplesmente verificar se um projeto está em conformidade com a legislação. A PIA permite que uma organização demonstre sua conformidade com a legislação de privacidade no contexto de uma reclamação subsequente, auditoria de privacidade ou investigação de conformidade. No caso de ocorrer um risco inevitável de violação da privacidade, o relatório da PIA pode fornecer evidências de que a organização agiu adequadamente na tentativa de impedir a ocorrência. O que pode ajudar a reduzir ou até eliminar qualquer responsabilidade, publicidade negativa e perda de reputação.

Segundo Wright (2011), as PIAs devem ser obrigatórias não apenas como uma maneira de responder a violações e perdas, mas como uma maneira de responder a projetos e serviços potencialmente intrusivos à privacidade. Uma PIA é mais do que uma ferramenta: é um processo que deve começar nos estágios mais iniciais possíveis, quando ainda existem oportunidades para influenciar o resultado de um projeto. E se trata de um processo que deve continuar até mesmo após a implantação do projeto (WRIGHT; FINN; RODRIGUES, 2013).

4 METODOLOGIA

Neste Capítulo é apresentada a caracterização da pesquisa e é descrito o método a ser utilizado para alcançar o objetivo deste estudo.

4.1 Caracterização da Pesquisa

Este estudo quanto à finalidade caracteriza-se como pesquisa **Fundamental**, visto que apresenta como resultado final a análise da presença de heurísticas cognitivas de privacidade nas redes sociais estudadas, contribuindo para o progresso da ciência no âmbito da privacidade. Quanto aos objetivos este estudo se caracteriza como uma pesquisa **Descritiva**, proporcionando mais informações sobre as questões de proteção da privacidade do indivíduo e identifica a existência de relações entre as heurísticas cognitivas de privacidade e os princípios do PbD e das leis LGPD e GDPR (GIL, 2002).

4.2 Técnicas e Métodos de Pesquisa

Para a condução da pesquisa, visando alcançar resultados que permitam atingir o objetivo delineado, serão executadas as atividades descritas nas subseções a seguir.

4.2.1 Levantamento Bibliográfico e Revisão Sistemática da Literatura

Com o intuito de fundamentar este estudo e buscar trabalhos elaborados sobre o tema proposto, foi realizada uma revisão sistemática da literatura, apresentada no Capítulo 3. Os resultados permitiram identificar metodologias para a elaboração de uma Avaliação de Impacto de Privacidade (PIA), sendo observado o atual panorama de métodos e técnicas propostos para abordagens voltadas a proteção da privacidade. Uma PIA é uma das maneiras pelas quais o ciclo de vida da informação pode ser gerenciado e os riscos à privacidade minimizados, bem como ser utilizada para verificar se um projeto está em conformidade com a legislação.

No final do processo da RSL, foram encontrados treze trabalhos que atendiam as questões de pesquisa. O resultado da RSL encontra-se na Seção 3.1.4.

Durante esta etapa, foi realizado também o levantamento bibliográfico sobre os princípios e os objetivos de proteção de privacidade, apresentados nas subseções 2.1.3 e 2.1.4, respectivamente. Com a finalidade de obter uma conscientização sobre o problema, observando os pontos chaves sobre proteção de dados pessoais contemplados na regulamentação da LGPD (Seção 2.2).

4.2.2 Análise Heurística das Redes Sociais

A inspeção aplicada neste estudo foi realizada com base na análise de heurísticas com foco em privacidade que influenciam os usuários do Facebook e Instagram a divulgar informações e definir quais dados eles dão consentimento e por quem podem ser vistos.

Este método analítico visa identificar problemas de acordo com um conjunto de heurísticas ou diretrizes. O processo envolveu quatro etapas, a fase inicial envolveu as etapas 1 e 2 e a fase de análise envolveu as etapas 3 e 4. São elas: 1) Selecionar um conjunto de heurísticas de privacidade a serem inspecionadas; 2) Identificar quais recursos das redes sociais a serem inspecionados; 3) Inspecionar a interface da rede social para identificar heurísticas que influenciam a divulgação de dados dos usuários; 4) Revisar as observações e resultados coletados durante a inspeção. A Figura 9 apresenta as etapas da análise heurística e os parágrafos seguintes as descrevem com mais detalhes.

Figura 9 – Metodologia de inspeção proposta para a análise das redes sociais em relação às preocupações com a privacidade dos usuários

Fonte: Elaborada pela autora

Durante a etapa *(1) Selecionar um conjunto de heurísticas de privacidade para inspecionar*, foi realizada uma revisão de literatura para levantar heurísticas cognitivas que influenciam as decisões dos indivíduos de proteger ou renunciar à privacidade. Assim, esta pesquisa teve um caráter exploratório. Quanto aos procedimentos técnicos utilizados, foi realizado um levantamento bibliográfico sobre o assunto em questão. Nesta pesquisa, foram examinados vários repositórios digitais do mundo da computação, incluindo a Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), Springer e Science Direct. Utilizando os termos (*privacy AND heuristic*) e (*heuristic AND disclosure*), os artigos foram pesquisados por título e assunto.

Após esse levantamento, um total de 25 artigos foram devolvidos dos repositórios digitais, os quais foram lidos em sua totalidade para a seleção das heurísticas de privacidade. Os autores dos artigos citados identificaram heurísticas que influenciam a divulgação das informações dos usuários, que é o foco deste estudo. Outros estudos, não mencionados, não apresentaram heurísticas com as características discutidas acima, em que observaram investigações que abordavam aspectos relacionados à usabilidade (heurísticas de Nielsen) e segurança; outros trabalhos apresentaram algoritmos heurísticos para

preservar a privacidade. Assim, um conjunto de heurísticas identificadas nos resultados das pesquisas elaboradas pelos autores foi compilado ao final, Gambino et al. (2016), Vincent et al. (2017) e Sundar et al. (2020). Os resultados desta pesquisa são apresentados na Seção 5.1.

Para a etapa *(2) Identificar quais recursos das redes sociais a serem inspecionados*, para o Facebook e Instagram avaliou-se por meio de pesquisas em sites de notícias o que o presidente da empresa, Mark Zuckerberg, aponta como uma tendência entre os usuários em todo o mundo. Segundo Zuckerberg, o movimento dos usuários é no sentido de divulgar vídeos e a linguagem das histórias, publicações que ficam disponíveis por um período máximo de 24 horas. Em 2018, Mark Zuckerberg relatou mudanças nas estratégias da empresa, trazendo três grandes tendências e desafios (Agência Brasil, 2020). Sendo estes:

1. Mudança de pessoas das redes sociais tradicionais para mensagens privadas e a linguagem das histórias (*stories*);

2. Crescimento do vídeo entre as plataformas, prevendo-se que nos próximos dez anos as formas de interação sejam baseadas em grupos, ou "comunidades";

3. Preocupações relacionadas às "ameaças de segurança" dos usuários.

Zuckerberg mudou o nome da empresa para Meta em outubro de 2021. Ele afirmou que o foco da empresa é dar vida ao metaverso e permitir que pessoas e empresas se conectem, encontrem comunidades e expandam seus negócios por meio de realidade aumentada e virtual. Eles imaginam que as pessoas podem se beneficiar não apenas como consumidores, mas como criadores. Além disso, eles prometeram que privacidade e segurança serão adicionadas desde o primeiro dia (PbD) (Meta, 2021).

Na etapa *(3) Inspecionar a interface da rede social*, buscou-se identificar se as redes sociais implementam as heurísticas selecionadas, identificadas na etapa 1, em suas funcionalidades disponibilizadas aos usuários da rede social. A plataforma de cada Rede Social foi inspecionada - tentando completar tarefas e passando pelos diferentes momentos da experiência. Os pontos avaliados da plataforma de rede social foram verificados nas versões web e mobile.

A avaliação heurística envolve ter um pequeno conjunto de avaliadores examinando individualmente a interface e julgando sua conformidade com princípios de usabilidade reconhecidos ("heurística"de usabilidade). Neste trabalho, ao invés de avaliar a usabilidade usando heurísticas de usabilidade, as redes sociais foram avaliadas com base nas heurísticas de privacidade levantadas na etapa 1, que favorecem o aumento ou inibição da divulgação de informações.

Dadas as heurísticas selecionadas, para o Facebook foi analisada a seção de *Marketplace*. Para o segundo desafio, foi inspecionado a forma de interação disponível entre

indivíduos em grupos, órgãos governamentais, figuras públicas, empresas de mídia ou marcas. Para o terceiro desafio, foi avaliada as opções disponíveis em "Configurações e privacidade". Para o Instagram avaliou-se a linha do tempo (*feed*), a criação de nova publicação e postagem de stories, avaliou-se também a publicação de Reels e o perfil do usuário. Por fim, avaliou-se as opções disponíveis em "Configurações" e em específico na opção "Privacidade e segurança".

Após a inspeção da interface foi realizada a etapa *(4) Revisar as observações e resultados coletados durante a inspeção*. Na Seção 5.2, são relatadas as observações e resultados obtidos durante a inspeção das redes sociais. Este trabalho apresenta uma comparação das heurísticas cognitivas de privacidade identificadas na literatura. Trazendo um ponto crítico para evidenciar a ativação de tais heurísticas ao realizar uma tarefa específica de interface. Tal formato de análise é aplicado em termos de consentimento para divulgação de dados. São apresentados contrastes com os conceitos de *Privacy by Design* e os princípios regulatórios presentes nas leis GDPR e LGPD (Seção 5.2.4).

4.2.3 Análise Qualitativa das Políticas de Privacidade das Redes Sociais

Neste estudo é realizada a análise qualitativa das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok. Observando os tópicos contemplados pelas políticas de privacidade disponíveis para o usuário, sendo avaliado requisitos de privacidade (4.2.3.1) e a coleta de IPI obrigatória e voluntária (4.2.3.2).

4.2.3.1 Análise de Requisitos de Privacidade

Para realizar a análise dos requisitos de privacidade de um sistema optou-se pela aplicação do método "Problem-based Privacy Analysis (ProPAn) – A Computer-aided Privacy Requirements Engineering Method" proposto por Meis (2018). De acordo com Meis (2018), para derivar os requisitos de privacidade de um sistema e as ameaças a eles, deve-se verificar como os dados pessoais processados pelo sistema fluem por ele. Isso inclui a obtenção das informações:

1. **como** os dados pessoais dos titulares dos dados são coletados;
2. **em que quantidade** os dados pessoais estão disponíveis nos domínios do sistema;
3. **por quanto tempo** os dados pessoais são retidos nos domínios do sistema;
4. **devido a quais declarações** os dados pessoais estão **disponíveis** em um domínio;
5. **para o qual propósito** os dados pessoais devem estar disponíveis no domínio;
6. **quais dados pessoais** disponíveis em um domínio **precisam ser vinculáveis** (*linkable*) entre si.

4.2.3.2 Distinção entre coleta de IPI obrigatória e voluntária

Conforme a Lei LGPD, os controladores de dados deverão informar sobre a coleta, o uso, o armazenamento e o tratamento de dados pessoais, bem como de suas finalidades específicas. O usuário, conforme o conceito de consentimento livre, deverá poder escolher quais dados fornecer e quais dados não deseja fornecer, e por fim, deverá poder revogar seu consentimento a qualquer momento.

Existem hipóteses em que o tratamento de dados é essencial ao regular o funcionamento da aplicação ou sistema. Nesses casos, é justificável que se condicione o acesso/uso à aceitação do tratamento de dados essenciais. Todavia, para determinar quais dados são fundamentais à prestação dos serviços, é importante determinar o escopo da aplicação ou sistema em questão.

Dessa maneira, durante a análise das políticas de privacidade das redes sociais pretende-se identificar a coleta de IPI obrigatória e voluntária para funcionamento das mesmas. Não obstante, o consentimento para tratamento de dados essenciais deverá ser destacado dos demais, subsistindo a liberdade de escolha do usuário quanto ao fornecimento de dados não obrigatórios.

5 RESULTADOS E DISCUSSÕES

Este capítulo apresenta os resultados obtidos com o levantamento das heurísticas de privacidade encontradas na literatura e o resultado da inspeção realizada no Facebook e Instagram com base nessas heurísticas. Neste capítulo também é realizado uma análise qualitativa das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok.

Este trabalho contribui para a área de privacidade no sentido de trazer essas heurísticas, que podem ser aplicadas a qualquer outra rede social, além da análise do quanto as redes sociais avaliadas cumprem com as recomendações e princípios propostos na lei.

5.1 Heurísticas de Privacidade

Esta seção apresenta artigos que identificaram heurísticas de privacidade que influenciam as decisões de divulgação de dados pessoais dos indivíduos e que aumentam ou inibem a divulgação de informações.

5.1.1 Heurísticas de GAMBINO et al.

No estudo realizado por Gambino et al. (2016), os autores realizaram oito sessões de grupo focal com 41 participantes. Três grupos foram formados por estudantes universitários e cinco por não estudantes. Um conjunto semiestruturado de perguntas foi aplicado a cada grupo ao longo do estudo para avaliar o comportamento dos indivíduos em relação à privacidade, desde percepções e comportamentos amplos até ações específicas. Em geral, as perguntas abrangeram seis tópicos principais de interesse: privacidade e segurança, dispositivos móveis, comércio eletrônico, mensagens, computação em nuvem e mídias sociais.

Os autores desses experimentos identificaram quatro heurísticas denominadas *positivas* que foram consideradas eficazes para facilitar o engajamento dos usuários em contextos *online* ou móveis. São eles: *(1) Gatekeeping*: os usuários preferem um sistema que adote medidas claras para proteger suas informações, como usar autenticação de dois fatores[1] *(2) Rede de Segurança*: os usuários têm como premissa a confiança de que serviços de terceiros, como Visa, PayPal e Apple, garantirão a segurança de suas informações pessoais. *(3) Bolha*: Os usuários relataram uma maior sensação de segurança ao usar modos de navegação anônimos ou ao realizar transações na rede doméstica. *(4) Efemeridade*: Em plataformas como o *Snapchat*, os participantes ficam mais à vontade para trocar informações. Segundo os autores, quando a heurística é ativada, os usuários se sentem mais à vontade e abertos para compartilhar mais informações, pois não há registro permanente ou registro que possa ser acessado por outras pessoas.

Quatro heurísticas adicionais foram identificadas como *negativas*, em que os in-

[1] Adicionada uma segunda camada de verificação acionada para confirmar a identidade do usuário ao realizar login em algum serviço *online*.

divíduos desconfiam de um site ou restringem o compartilhamento de informações. *(1) Limite Difuso*: os usuários expressaram desconforto quando confrontados com evidências constantes de seu comportamento de navegação *online*. Um exemplo disso são as propagandas direcionadas ao indivíduo, causando a suspeita de que as informações sejam compartilhadas com terceiros sem o seu conhecimento ou consentimento. *(2) Intrusão*: associado ao inconveniente de receber *e-mails* ou notificações e anúncios não solicitados, o que leva o usuário a questionar a integridade do sistema que faz ou permite a solicitação. *(3) Incerteza*: referente ao sentimento de desconforto causado por uma situação desconhecida em que um indivíduo se sente inseguro devido à incapacidade de compreender o dispositivo ou site. Um exemplo disso é o ceticismo dos usuários em relação aos serviços em nuvem. *(4) Mobilidade*: são preocupações inerentes ao uso de produtos móveis, que podem estar associadas a preocupações com a Internet utilizada ou roubo de dispositivos.

5.1.2 Heurísticas de VINCENT et al.

No estudo realizado por Vincent et al. (2017), foram realizadas 23 entrevistas individuais semiestruturadas com usuários entre 18 e 25 anos. Os autores identificaram seis classes de heurísticas nas quais os usuários confiam durante as divulgações, são elas: *Proeminência*, *Rede*, *Confiabilidade*, *Acordo*, *Modalidade* e *Narrativa*.

A classe **Proeminência** permite observar que, em geral, se algo ganhou Proeminência, deve estar fazendo algo certo, enquanto a falta dele sugere o contrário. Portanto, esta classe compreende duas heurísticas, sendo elas: 1) *Reputação*: para a qual se considera que um serviço de prestígio não faria algo errado conscientemente, referindo-se a julgamentos de credibilidade sobre a legitimidade de uma organização. 2) *Reconhecimento*: em que a principal diferença é que tal Reputação se estende além da entidade original em direção às subsidiárias, similarmente definida por Gambino et al. (2016) como "Rede de Segurança".

A classe **Rede** é observada através da percepção da influência que a rede interpessoal de um indivíduo tem nas decisões de divulgação. É evidenciado por meio de heurísticas, como 1) *Endosso*: as recomendações de conhecidos são preferidas às autorecomendações; 2) *Bandwagon*: estende-se a recomendações de estranhos recebidas por fatores menos pessoais, como depoimentos agregados ou classificações por estrelas incorporadas na interface. 3) *Autoridade*: quando a confiança deriva de recomendações de autoridades oficiais ou especialistas. De acordo com Vincent et al. (2017), o comportamento de manada pode surgir sem a devida consideração das circunstâncias, com a expectativa de que outros descubram os riscos inerentes a uma decisão de divulgação de informações.

A classe **Confiabilidade** contém três heurísticas: 1) *Consistência*: baseada na confiança sobre o acordo entre fontes independentes, sendo observada quando fica evidente que um requisito não padronizado para registro é um requisito consistente de serviço simi-

lar; 2) *Consenso*: trata-se de um acordo padronizado e geral, por exemplo, para interagir em uma rede social, espera-se que o nome, *e-mail* e foto do perfil sejam informados; e 3) *Expectativa*: para o qual podem surgir conotações negativas em torno do *design* de interface deficiente, no qual há expectativa de profissionalismo. De acordo com Vincent et al. (2017), as três heurísticas estão ligadas à ideia de que se algo está quebrado, tem erros ou algo muda, isso pode levar os usuários a não divulgar informações.

A classe **Acordo** difere da classe *Confiabilidade*, pois se refere a crenças e entendimento ao invés de interface do processador. Nesta classe, duas heurísticas estão presentes: 1) *Autoconfirmação*: acionado quando algo se alinha com uma crença anterior, não exigindo uma norma para a solicitação de informações, desde que haja o entendimento de que a solicitação "aparece por boas razões". 2) *Intenção Persuasiva*: cujo princípio subjacente é que a manipulação percebida leva a julgamentos negativos. Gambino et al. (2016) chame isso de "*Intrusão*", como no caso em que o usuário tenta interagir com um site e aparecem pop-ups, por exemplo. Além disso, de acordo com Vincent et al. (2017), com a retirada da palavra "Persuasiva", a heurística ("Intenção") serviria a um propósito próximo ao elemento de integridade em Gambino et al. (2016).

A classe **Modalidade** inclui heurísticas: 1) *Coolness*: associado a novos recursos tecnológicos, ou sinos e assobios de tecnologias existentes, com avaliações positivas de credibilidade; e 2) *Novidade*: sutilmente diferente da heurística *Coolness*, sendo invocada pela experiência inicial do usuário com a tecnologia.

De acordo com o estudo, a classe **Narrativa** é simbolizada pela ausência de narrativa, ou seja, consideração dos riscos envolvidos com a divulgação excessiva (NORBERG; HORNE; HORNE, 2007). Quando confrontados com uma determinada decisão, os indivíduos podem optar por divulgar mais informações quando influenciados por essa classe. Existem duas heurísticas: 1) *Disponibilidade*: refere-se a um julgamento da probabilidade de um evento baseado na "facilidade com que instâncias relevantes vêm à mente". 2) *Coerência*: relacionado à capacidade de ver o resultado de uma decisão como uma consequência plausível. De acordo com Vincent et al. (2017), não é satisfatório esperar que as experiências negativas dos usuários incutam uma abordagem mais cautelosa e ponderada à divulgação. Em vez disso, pode ser possível informar os usuários sobre o risco de divulgação por meio de uma narrativa relacionável.

Uma sétima classe **Troca**, não heurística[1], também foi reconhecida que os respondentes estavam avaliando suas divulgações em termos de ganhos de utilidade comercial versus perdas. Segundo os autores, embora os usuários demonstrem esforços para divulgar informações de forma mais indutiva, após considerar um número suficiente de casos particulares, as variáveis subjacentes à decisão tomada geralmente permanecem baseadas em heurísticas.

[1]Tomada de decisão que combate qualquer viés de confirmação; prevendo o risco envolvido e agindo com cautela.

5.1.3 Heurísticas de SUNDAR et al.

No estudo realizado por Sundar et al. (2020) doze heurísticas derivadas da literatura de privacidade *online* foram selecionadas e estão organizadas em três contextos de privacidade: 1) *social*, refere-se a contextos que pressupõem a existência da influência de outros indivíduos sobre as decisões do usuário; 2) *pessoal*, referindo-se a situações que incidem sobre o indivíduo como entidade autônoma, em que os utilizadores procuram manter a sua privacidade ou divulgar informação para se protegerem, ampliarem ou melhorarem; e 3) *tecnológico ou ambiental*, refere-se a elementos do espaço físico.

No contexto ***social***, identificam-se seis heurísticas associadas a maiores intenções de divulgação, são elas: *(1) Autoridade*: a presença de um nome, marca ou organização conhecida num web site é suscetível de fazer com que os usuários se sintam seguros, tomando o atalho mental de que tudo o que eles fazem e revelam no site é seguro; *(2) Bandwagon*: se a maioria dos usuários de uma comunidade *online* mostra informações para um site, então a tendência é que o usuário também opte pela divulgação; *(3) Reciprocidade*: regra comum da comunicação interpessoal em que a auto-revelação íntima segue o princípio da reciprocidade - se o parceiro revela algo pessoal, a tendência é retribuir, revelando algo igualmente pessoal sobre si mesmo; *(4) Senso de Comunidade*: quando as pessoas se sentem parte de uma comunidade, elas podem confiar e depender umas das outras para apoio e, finalmente, compartilhar aspectos mais íntimos de suas vidas umas com as outras; *(5) Criação de Comunidade*: um fórum *online* robusto é o resultado da participação ativa dos usuários. O compartilhamento de informações pessoais pode contribuir para a construção da comunidade dessa maneira; *(6) Autoapresentação*: o objetivo de revelar informações pessoais *online* é melhorar o status social em ambientes sociais *online*.

No contexto ***pessoal***, identificam-se duas heurísticas associadas a maiores intenções de divulgação, são elas *(1) Controle*: proporcionar aos utilizadores a capacidade de controlar o ritmo e a natureza do conteúdo é uma forma de acionar a heurística de controle, resultando em uma percepção favorável da interface e de seu conteúdo; *(2) Gratificação instantânea*: os indivíduos são movidos por um "viés de otimismo", o que os faz responder prontamente a ofertas instantâneas *online* e subestimar os riscos de divulgar informações no processo.

Quatro heurísticas relacionadas à divulgação foram identificadas no contexto ***tecnológico ou ambiental***. Existem duas heurísticas relacionadas às intenções de divulgação *positivas*. *(1) Transparência*: ao explicar o que é e como as informações do usuário são usadas, as declarações de política de privacidade e a demonstração explícita de permissões podem impor credibilidade a um site, no qual o usuário tende a confiar devido à divulgação completa de suas políticas; *(2) Máquina*: acredita-se que as máquinas manipulariam a informação de acordo com as regras legais e não teriam fraquezas humanas como fofocas;

o autor discute interações com assistentes de voz como Siri, Cortana e Alexa. Além disso, duas heurísticas adicionais estão associadas às intenções de divulgação *negativas*. *(1) Publicidade*: os usuários expressam preocupações mais profundas com a privacidade quando estão em uma rede sem fio, com um sentimento de vulnerabilidade ao realizar transações usando redes públicas; *(2) Mobilidade*: os usuários, sempre que lembrados de que estão em um dispositivo móvel, tendem a acionar a heurística de mobilidade; evitando assim armazenar informações privadas.

Na Figura 10, heurísticas de privacidade que aumentam o comportamento de divulgação de informações são ilustradas. Ao contrário disso, Figure 11 revela heurísticas de privacidade que inibem a divulgação de informações. As Figuras 10 e 11 sintetizam as heurísticas de privacidade identificadas por Gambino et al. (2016), Vincent et al. (2017), Sundar et al. (2020).

5.1.4 Considerações Gerais Sobre as Heurísticas Identificadas

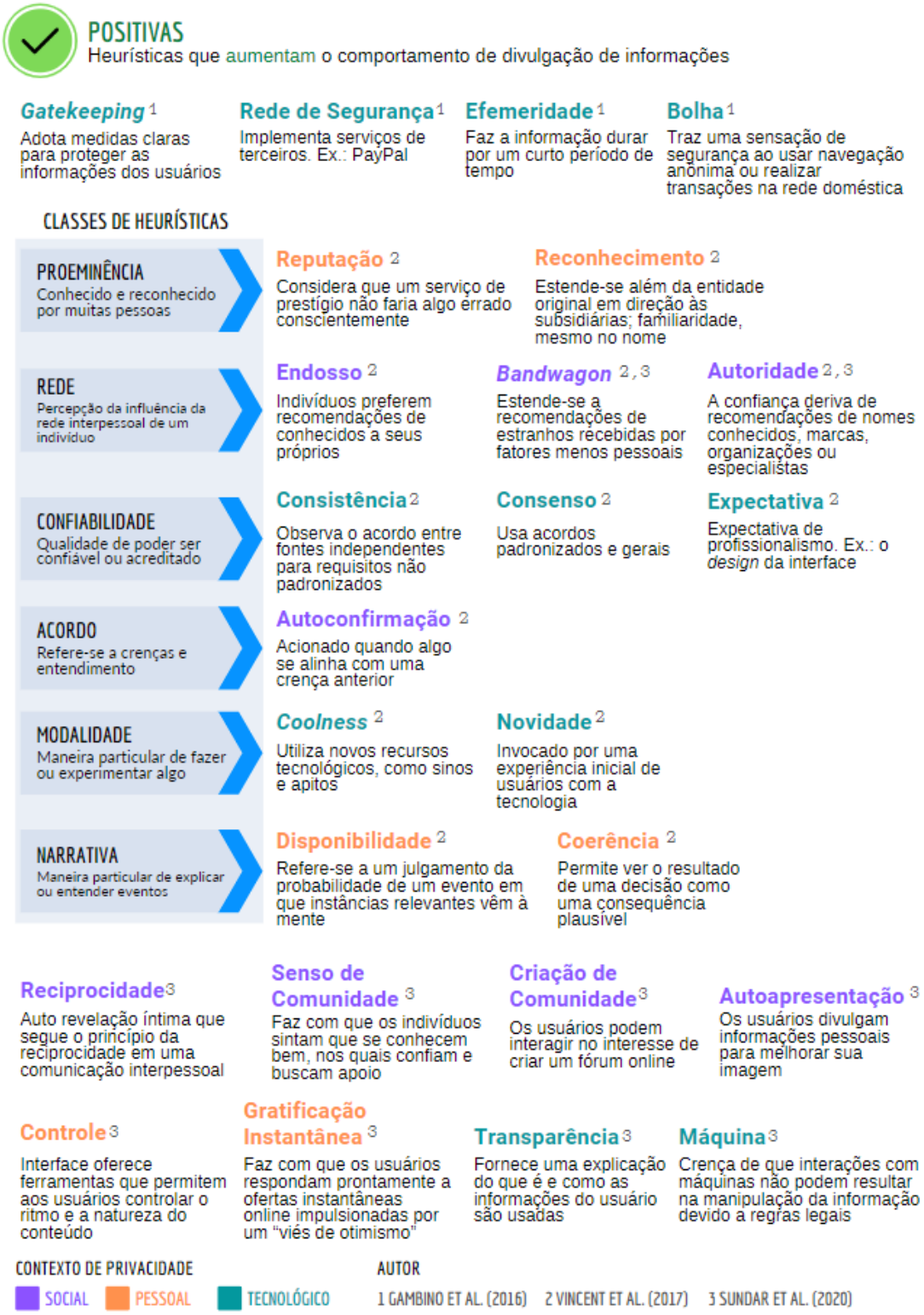
As conclusões alcançadas pelos autores citados Gambino et al. (2016), Vincent et al. (2017), Sundar et al. (2020) corroboram a relevância que as heurísticas de privacidade cognitiva desempenham no apoio à tomada de decisão dos usuários em relação a informações claras e precisas sobre os serviços *online* utilizados.

Wu et al. (2018) concluem que os usuários fornecem mais informações para itens moderados quando não têm conhecimento prévio. Em comparação, o modelo heurístico pode persuadir outros que não têm conhecimento prévio para apoiar sua tomada de decisão a divulgar mais informações. Essa questão também foi observada no trabalho de Gambino et al. (2016), que constataram que os indivíduos geralmente agem com pouco pensamento ou avaliação, mesmo mostrando surpresa diante de seus comportamentos.

No mesmo sentido, Vincent et al. (2017) afirmam que os usuários tendem a tomar decisões ruins e que os esforços regulatórios que buscam aumentar a autonomia do usuário informado são ineptos. Os autores reforçam que as heurísticas cognitivas são essenciais para entender os usuários que consentem em divulgar mais do que o pretendido (ou seja, paradoxo da privacidade). Além disso auxilia para entender os usuários que concordam em revelar mais do que sabem (ou seja, consentimento simples). Portanto, os autores sugerem que a chave para apoiar os usuários durante as decisões de divulgação pode ser empurrar os usuários por meio de dicas que favoreçam o acionamento de heurísticas de privacidade cognitiva de forma positiva.

Sundar et al. (2020) confirmam sua hipótese de que a crença dos usuários (ou grau de acessibilidade) em uma determinada heurística está significativamente associada às suas intenções de revelar informações privadas em um contexto de divulgação que apresenta uma sugestão delineada para acionar uma determinada heurística. Além disso, os autores observaram o papel significativo que as dicas de interface desempenharam em influenciar a decisão de um usuário de compartilhar informações privadas.

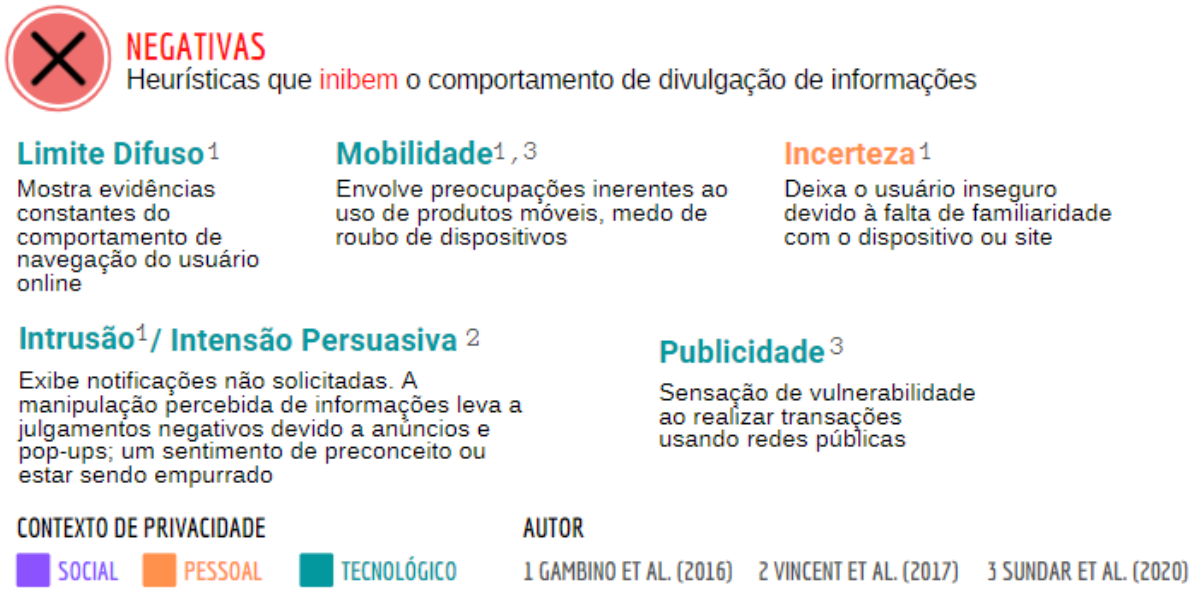
Figura 10 – Heurísticas de privacidade positivas que aumentam a divulgação de informações dos usuários



Fonte: Elaborada pela autora

Em relação às considerações dos autores mencionadas anteriormente, Anaraky et al. (2021) identificaram que os adultos mais jovens dependem mais da tomada de decisão

Figura 11 – Heurísticas de privacidade negativas que inibem a divulgação de informações dos usuários



Fonte: Elaborada pela autora

heurística, sendo mais propensos a mudar sua percepção da sensibilidade dos dados com base na confiança. Por outro lado, os idosos eram mais propensos a divulgar informações que consideravam valiosas, enquanto eram menos propensos a divulgar informações influenciadas por heurísticas.

5.2 Inspeção de Heurísticas de Privacidade em Redes Sociais

Esta seção apresenta o resultado da análise heurística realizada nas redes sociais Facebook e Instagram com base nas heurísticas levantadas que favorecem o aumento ou inibição da divulgação de informações.

Para a inspeção do Facebook e Instagram as funcionalidades consideradas foram derivadas dos desafios e tendências relatados por Mark Zuckerberg, sendo eles:

1. Mudança de pessoas das redes sociais tradicionais para mensagens privadas e a linguagem das histórias (*stories*);

2. Crescimento do vídeo entre as plataformas, prevendo-se que nos próximos dez anos as formas de interação sejam baseadas em grupos, ou "comunidades";

3. Preocupações relacionadas às "ameaças de segurança" dos usuários.

5.2.1 Inspeção de Heurísticas de Privacidade no Facebook

Dadas as heurísticas selecionadas, para o Facebook foi analisada a seção de *Marketplace*. Para o segundo desafio citado por Zuckerberg, foi inspecionado a forma de

interação disponível entre indivíduos em grupos, órgãos governamentais, figuras públicas, empresas de mídia ou marcas. Para o terceiro desafio, foi avaliada as opções disponíveis em "Configurações e privacidade".

5.2.1.1 Heurísticas que aumentam o comportamento de divulgação de informações (positivas)

Os itens a seguir expõem fatores observados durante a inspeção do Facebook que podem proporcionar uma influência positiva para que os usuários continuem interagindo e compartilhando conteúdo.

- ***Gatekeeping*:** é possível habilitar a autenticação de dois fatores para os casos em que o usuário utiliza o Facebook como forma de autenticação em outros aplicativos. Além disso, a possibilidade de configurar uma senha de uso único é fornecida para aplicativos que não suportam autenticação de dois fatores (exemplo: Xbox, Spotify).

- **Rede de Segurança:** na área Marketplace da rede social, é possível anunciar produtos para venda/aluguel, podendo visualizar anúncios de qualquer pessoa da rede. No entanto, o Facebook não permite adicionar um método de pagamento. Nesse caso, o espaço funciona apenas como propaganda, cabendo aos usuários negociar a compra e venda dos produtos publicados. Usando a ferramenta, os usuários podem pesquisar anúncios com base em sua localização atual em seus telefones.

- **Efemeridade:** uma das formas de publicação disponíveis é através de *stories* onde o usuário faz um post. De acordo com sua configuração definida, estará disponível por 24 horas para o "Público", "Amigos", "Personalizado" ou "Ocultar *story* de". Como o Facebook permite que o usuário controle para quem a postagem está disponível, é possível que os usuários concordem em divulgar informações sem compartilhá-las com todos na rede social.

- **Proeminência (Reputação e Reconhecimento):** apesar de o Facebook estar envolvido no escândalo Cambridge Analytica em 2018 – uma consultoria política que usou indevidamente dados de usuários para afetar eleições nos Estados Unidos – a empresa demonstrou um compromisso com gestão de questões sociais. Em 2021, a rede social completou 17 anos de existência, totalizando 2,9 bilhões de usuários ativos mensais e dominando o mercado de mídias sociais por uma década (Statista, 2021; ORTIZ-OSPINA, 2019). A Reputação e Reconhecimento do Facebook permite que os usuários continuem optando por usar a plataforma para se comunicar com outros indivíduos.

- **Confiabilidade (Consistência, Consenso e Expectativa):** A página Engineering at Meta (2017) expõe a abordagem de escala de entrega contínua adotada pela

plataforma, que divide o processo em três camadas: desenvolvimento, análise estática e testes. O ciclo de entrega constante permite que a experiência do usuário seja melhor e mais rápida. De acordo com a página Meta (2018), a equipe está trabalhando para revisar e expandir suas ferramentas para ajudar as pessoas a gerenciar a privacidade e entender suas escolhas em relação aos dados pessoais.

- **Modalidade (*Coolness* and Novidade):** a rede social mostra foco no cliente, proporcionando melhorias baseadas nos interesses de seus usuários. Um bom exemplo disso são as reações personalizadas às publicações. Em 2020, por exemplo, o Facebook lançou a reação "Força", Figura 12 (a) cujo objetivo era ajudar os usuários de redes sociais a expressar apoio uns aos outros durante a pandemia do coronavírus (COVID-19). Outro exemplo é quando alguém recebe um "parabéns" e pode clicar/tocar na palavra. A interface pode exibir uma animação de confetes, balões e estrelas, como evidenciado na Figura 12 (b). Este é um exemplo de mudanças cosméticas feitas na plataforma que criam o desejo de usar esses recursos durante a postagem.

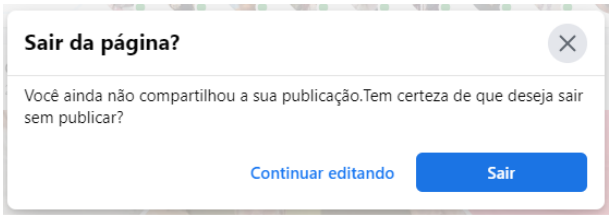
Figura 12 – (a) Reação "Força" adicionada pelo Facebook em indicação de conscientização com o distanciamento social imposto pela pandemia do COVID-19; (b) Efeito da palavra "parabéns" escrita em um *post* quando clicado/tocado

Fonte: Facebook

- **Narrativa (Disponibilidade e Coerência):** Ao utilizar a interface do Facebook, é possível perceber **disponibilidade** e **coerência** nas funcionalidades disponíveis. Por exemplo, ao realizar uma ação e não salvar, o usuário é solicitado a confirmar se deseja sair sem terminar, Figura 13.

- **Rede (Endosso, *Bandwagon*, Autoridade):** O Facebook proporciona interação entre os indivíduos, onde solicitam e fornecem recomendações a conhecidos ou não, podendo assim acionar as heurísticas de Endosso e Bandwagon, respectivamente.

Figura 13 – Confirmação de que deseja sair sem terminar a ação iniciada anteriormente



Fonte: Facebook

Em relação à heurística Autoridade, há um "selo de autenticidade" na rede social, destinado a páginas e perfis conhecidos e pesquisados, que valida como autênticas postagens feitas por órgãos governamentais, figuras públicas, empresas de mídia ou marcas.

- **Senso e Criação de Comunidades:** como mencionado anteriormente no Capítulo 4, projeta-se que nos próximos dez anos, as formas de interação sejam baseadas em grupos. Com isso em mente, o Facebook apresenta uma seção na barra de menu principal para acompanhar as atividades recentes dos "Grupos" do usuário.

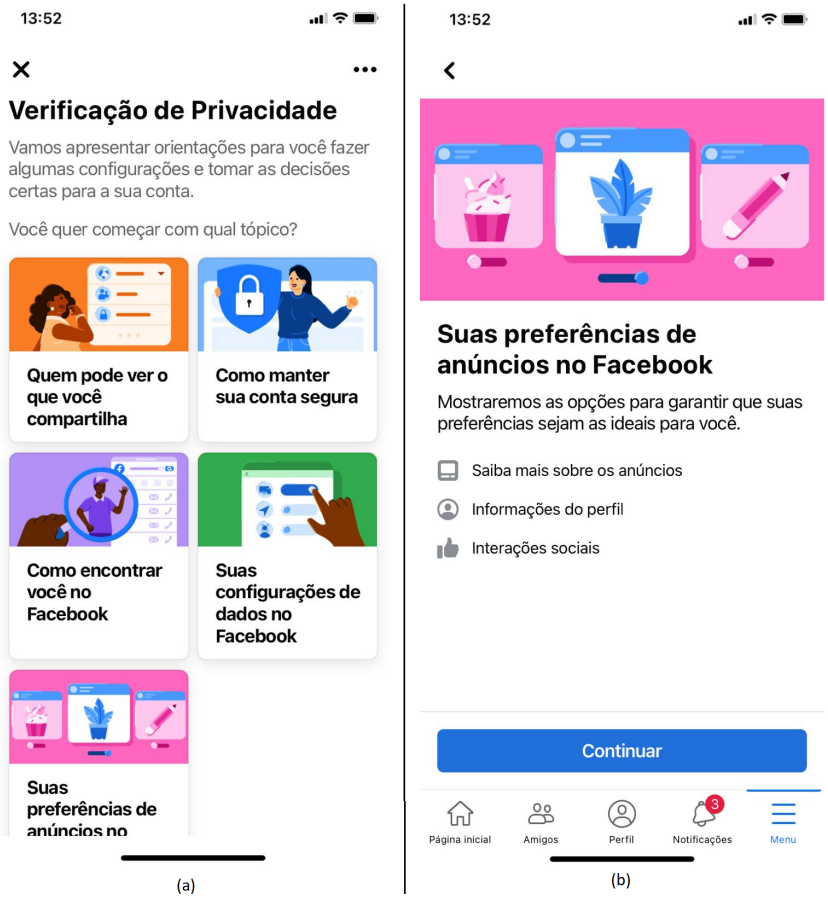
- **Gratificação instantânea:** heurística não identificada durante a inspeção da rede social.

- **Controle:** tanto no navegador quanto no acesso ao aplicativo móvel, a interface incentiva e dá dicas ao usuário sobre as etapas que podem ser tomadas para gerenciar os dados que desejam compartilhar e com quais indivíduos desejam que os mesmos fiquem visíveis. No nível de privacidade *individual*, o Facebook permite ao usuário os quatro estados fundamentais de interação com outras pessoas (solidão, intimidade, anonimato e reserva). Ao escolher o público com o qual o usuário deseja compartilhar determinadas informações, por exemplo, número de telefone, e-mail, data de nascimento e publicações, é possível definir como "Público", "Somente eu", " Amigos", "Amigos exceto conhecidos", "Personalizados", entre outros. Assim como a Efemeridade, o Facebook permite que o usuário controle para quem a postagem está disponível, ao fazê-lo, o usuário dá consentimento para divulgar informações sem compartilhá-las com todos na rede social. Além disso, (Meta, 2018) mostra que o Facebook assumiu o compromisso de simplificar o *design* de suas configurações de privacidade em um novo centro de controle e definiu o compromisso de notificar os usuários em seu feed para verificar sua configuração de privacidade, recursos observados durante a avaliação.

- **Transparência:** por conta de medidas regulatórias como GDPR e LGPD, o Facebook permite que os usuários estabeleçam regras quanto à coleta, armazenamento,

tratamento e compartilhamento de seus dados. A área de configurações e privacidade permite ao usuário visualizar as informações acessíveis (Figura 14 a).

Figura 14 – (a) Página de verificação de privacidade criada para orientar os usuários sobre como gerenciar as configurações de dados; (b) Página de preferências de anúncios sobre como os mesmos são selecionados com base nos dados.



Fonte: Facebook

5.2.1.2 Heurísticas que inibem o comportamento de divulgação de informações (negativas)

Durante a inspeção de uma publicação (*post*), inspecionamos a navegação na linha do tempo (*feed*) do Facebook. A ativação das heurísticas **Intrusão/Intenção Persuasiva** ocorreu devido ao aparecimento de anúncios patrocinados entre as postagens de conexões e grupos. Tal ocorrência, a princípio, pode causar algum desconforto ao usuário, levando-o a ser influenciado também pelas heurísticas de **Incerteza** e **Limite Difuso**. Por padrão, a configuração de anúncios da rede social é definida como "Permitido", o que é contrário ao princípio PbD de "Privacidade como configuração padrão", e essa configuração deve ser inicialmente definida como "Não permitido".

Ressalta-se que para aqueles usuários que buscam um maior nível de interatividade com a interface, o Facebook oferece no *post* a palavra "Patrocinado" como uma URL que direciona o usuário para uma página. Na página, os usuários são convidados a entender melhor como funciona a publicidade e como os dados do usuário são usados para exibir anúncios (Facebook, 2020). Da mesma forma, na área "Atalhos de privacidade", é possível verificar as preferências de anúncios (Figura 14 b).

5.2.2 Inspeção de Heurísticas de Privacidade no Instagram

Para o Instagram avaliou-se a linha do tempo (*feed*), a criação de nova publicação e postagem de stories, avaliou-se também a publicação de *Reels* e o perfil do usuário. Por fim, avaliou-se as opções disponíveis em "Configurações" e em específico na opção "Privacidade e segurança".

5.2.2.1 Heurísticas que aumentam o comportamento de divulgação de informações (positivas)

Os itens a seguir expõem fatores observados durante a inspeção do Instagram que podem proporcionar uma influência positiva para que os usuários continuem interagindo e compartilhando conteúdo.

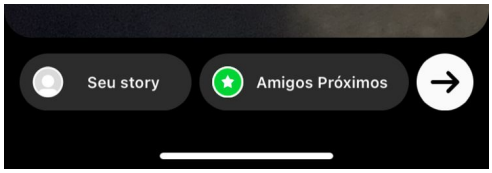
- ***Gatekeeping*:** no Instagram, assim como observado no Facebook, é possível ativar a autenticação de dois fatores. Podendo a autenticação ser via SMS ou App de autenticação (recurso disponível apenas para o aplicativo).

- **Rede de Segurança:** para países da África do Sul e em alguns países da Europa e América Latina está liberado o serviço Facebook Pay, o qual aceita o cadastro de cartão de Débito e Crédito (Visa ou Mastercard) ou a utilização do PayPal. Todavia, como o mesmo não se encontra disponível para o Brasil no momento da realização da inspeção, não foi possível observar a utilização deste recurso.

- **Efemeridade:** no Instagram também existe a publicação de fotos e vídeos no formato de stories. De acordo com a configuração do usuário, caso ele tenha definido a conta como privada o *story* publicado ficará disponível apenas para as pessoas que o usuário segue. Outra possibilidade é a de criar uma lista de "Aminos Próximos" e então compartilhar o *story* para os amigos adicionadas a lista (Figura 15).

- **Proeminência (Reputação e Reconhecimento):** Em 2022, com 92,5%, o Instagram foi considerado a rede social mais relevante para gerar novos negócios, seguida pelo Facebook (61,2%) e LinkedIn (37,7%) (Resultados Digitais, 2022). De 2021 para 2022 a rede social cresceu 17,9%, possuindo 1,4 bilhões de usuários ativos e figura como a 4ª rede social com mais usuários no mundo, atrás do Facebook, Youtube e WhatsApp (Resultados Digitais, 2022). A Reputação e Reconhecimento do

Figura 15 – Publicar *story* para lista de "Amigos Próximos"



Fonte: Instagram

Instagram permite que os usuários continuem optando por usar a plataforma para interagir com outros indivíduos e realizar ações de Marketing e Vendas.

- **Confiabilidade (Consistência, Consenso e Expectativa):** A Meta, Inc., assim como para o Facebook, realiza a abordagem de escala de entrega contínua para a plataforma do Instagram.

- **Modalidade (*Coolness* and Novidade):** Conforme a tendência observada por Zuckerberg para o crescimento do vídeo, em Agosto de 2020 o Instagram lançou o recurso de *Reels* em mais de 50 países. O *Reels* permite o usuário criar vídeos divertidos para compartilhar com os amigos ou qualquer pessoa no Instagram. Outro exemplo da presença da classe Modalidade no Instagram foi a criação em 2015 do recurso de *Boomerang* (minivídeo de alta qualidade que é reproduzido para frente e para trás). O lançamento dessas funcionalidades para a plataforma aumenta o engajamento dos usuários com a mesma.

- **Narrativa (Disponibilidade e Coerência):** Ao utilizar a interface do Instagram, também é possível perceber **disponibilidade** e **coerência** nas funcionalidades. Assim como observado no Facebook, no Instagram quando é realizada uma ação e opta-se para realizar outra ação antes de salvar, a plataforma solicita confirmação de que deseja sair e descartar a tarefa (Figura 16).

Figura 16 – Coerência ao utilizar uma funcionalidade e a interface solicitar confirmação se deseja descartar ação

Fonte: Instagram

- **Rede (Endosso, *Bandwagon*, Autoridade):** Por meio dos comentários e a marcação de usuários em comentários é possível que os usuários da rede social recomendem produtos anunciados na plataforma para seus amigos e até mesmo para estranhos. Em relação à heurística Autoridade, o Instagram trabalha com um selo de conta "Verificada", possibilitando que os usuários reconheçam contas oficiais de artistas, empresas, times esportivos e etc.

- **Senso e Criação de Comunidades:** heurística não identificada durante a inspeção da rede social.

- **Gratificação instantânea:** heurística não identificada durante a inspeção da rede social.

- **Controle:** O Instagram, conforme citado anteriormente, possibilita ao usuário definir sua conta como privada, dessa forma quando alguém opta por seguir a conta do usuário este deve ser aprovado antes de poder visualizar as fotos e vídeos publicadas. A plataforma também possibilita ao usuário controlar o status de sua atividade na rede social, controlar se é permitido que outros compartilhem seus stories, bem como moderar palavras que não podem ser usadas nos comentários. Outro recurso disponibilizado para o usuário é o de adicionar manualmente em seu perfil fotos que outros usuários postam com o mesmo e controlar quem pode mencionar sua conta do Instagram em postagens.

- **Transparência:** Devido a complexidade menor do Instagram as opções para controle da "privacidade e segurança" do usuário são menos abrangentes do que as opções observadas no Facebook. Todavia, nota-se que a área de "privacidade e segurança" permite ao usuário observar a transparência da plataforma com relação ao seu perfil e disseminação de suas publicações de fotos e vídeos.

5.2.2.2 Heurísticas que inibem o comportamento de divulgação de informações (negativas)

Durante a inspeção da linha do tempo (*feed*) do Instagram, ocorreu a ativação das heurísticas **Intrusão**/**Intenção Persuasiva** pelo mesmo motivo observado durante a inspeção da linha do tempo do Facebook – aparecimento de anúncios patrocinados entre as postagens de contas que o usuário segue. Dessa mesma forma, o usuário também pode ser influenciado também pelas heurísticas de **Incerteza** e **Limite Difuso**.

Todavia, assim como existe no Facebook, o usuário pode acessar a Central de Ajuda do Instagram e ler sobre como funcionam os anúncios na plataforma. Outra coisa que o usuário pode fazer é visualizar qual o critério para que um anúncio específico esteja sendo mostrado na linha do tempo.

5.2.3 Heurísticas não Avaliadas no Contexto de Inspeção das Redes Sociais

A heurística "Bolha" não foi avaliada durante a inspeção porque sua ativação estava associada ao modo de navegação anônima ou rede doméstica. As heurísticas "Autoconfirmação", "Reciprocidade" e "Autoapresentação" também não foram avaliadas por estarem associadas às crenças do usuário, comunicação interpessoal e vontade de auto divulgar sua imagem, respectivamente. A heurística "Máquina" não foi avaliada porque se refere à ideia de que máquinas manipulariam informações de acordo com regras legais. Por fim, as heurísticas de "Mobilidade" e "Publicidade" também não foram avaliadas, pois as características que inibem o comportamento de divulgação dos usuários estão diretamente relacionadas à vulnerabilidade quando conectados em redes públicas de Internet ou durante o uso de dispositivos móveis (propensos a roubos). O Quadro 4 apresenta o resultado agrupado das heurísticas de privacidade cognitiva que foram (ou não) observadas durante a inspeção das redes sociais Facebook e Instagram.

Quadro 4– Resultado da análise heurística nas redes sociais

	Classe[2]	**Heurísticas**	**Facebook**	**Instagram**
Positivas		*Gatekeeping*[1]	✓	✓
		Rede de Segurança[1]	✗	✗
		Bolha[1]	N/A	
		Efemeridade[1]	✓	✓
	Proeminência	Reputação[2]	✓	✓
		Reconhecimento[2]	✓	✓
	Confiabilidade	Consistência[2]	✓	✓
		Consenso[2]	✓	✓
		Expectativa[2]	✓	✓
	Acordo	Autoconfirmação[2]	N/A	
	Modalidade	*Coolness*[2]	✓	✓
		Novidade[2]	✓	✓
	Narrativa	Disponibilidade[2]	✓	✓
		Coerência[2]	✓	✓
	Rede	Endosso[2]	✓	✓
		Bandwagon[2 3 a]	✓	✓
		Autoridade[2 3 a]	✓	✓
		Reciprocidade[3 a]	N/A	
		Senso de Comunidade[3 a]	✓	✗
		Criação de Comunidade[3 a]	✓	✗
		Autoapresentação[3 a]	N/A	
		Gratificação Instantânea[3 b]	✗	✗
		Controle[3 b]	✓	✓
		Transparência[3 c]	✓	✓
		Máquina[3 c]	N/A	
Negativas	Acordo	Intrusão[1]/ Intenção Persuasiva[2]	✓	✓
		Limite Difuso[1]	✓	✓
		Incerteza[1]	✓	✓
		Mobilidade[1 3 c]	N/A	
		Publicidade[3 c]	N/A	

[1] Gambino et al. (2016) [2] Vincent et al. (2017) [3] Sundar et al. (2020)
[a] Contexto Social [b] Contexto Pessoal [c] Contexto tecnológico ou ambiental
Legenda: ✓- observada ✗- não observada N/A - não avaliada

5.2.4 Relação das Heurísticas com o PbD e as Leis LGPD e GDPR

De acordo com Oliveira, Mattedi e Seabra (2021), quando a experiência do usuário é positiva o suficiente isso pode influenciar os usuários a continuar usando a tecnologia. Além disso, o nível de complexidade de um sistema deve ser proporcional às expectativas do público-alvo. Como alternativa às heurísticas observadas, fatores culturais podem afetar a percepção de vantagens relativas, como questões éticas, de privacidade ou de gênero. Os fatores listados previamente também contribuem para a experiência do usuário e a decisão de divulgar informações pessoais. Com relação a algumas das heurísticas observadas contemplam-se princípios do *Privacy by Design* e princípios das leis LGPD e GDPR, sendo estes informados a seguir.

Conforme observado nas subseções 5.2.1.1 e 5.2.2.1, ambas as redes sociais apresentam a presença da heurística de ***Gatekeeping***, sendo esta um exemplo dos princípios do PbD "Segurança de ponta a ponta - garantindo proteção completa do ciclo de vida" e "Proativo não reativo". Para o princípio da LGPD fala-se de "Segurança" e para GDPR o princípio de "Integridade e confidencialidade". A presença do *Gatekeeping* no Facebook e Instagram favorece um controle mais seguro do acesso à conta do usuário. A **Efemeridade** observada nas redes sociais é um exemplo dos princípios do PbD "Respeito pela privacidade do usuário" e "Privacidade como configuração padrão". Para a LGPD fala-se do princípio da "Necessidade" e para o GDPR o princípio da "Limitação de armazenamento".

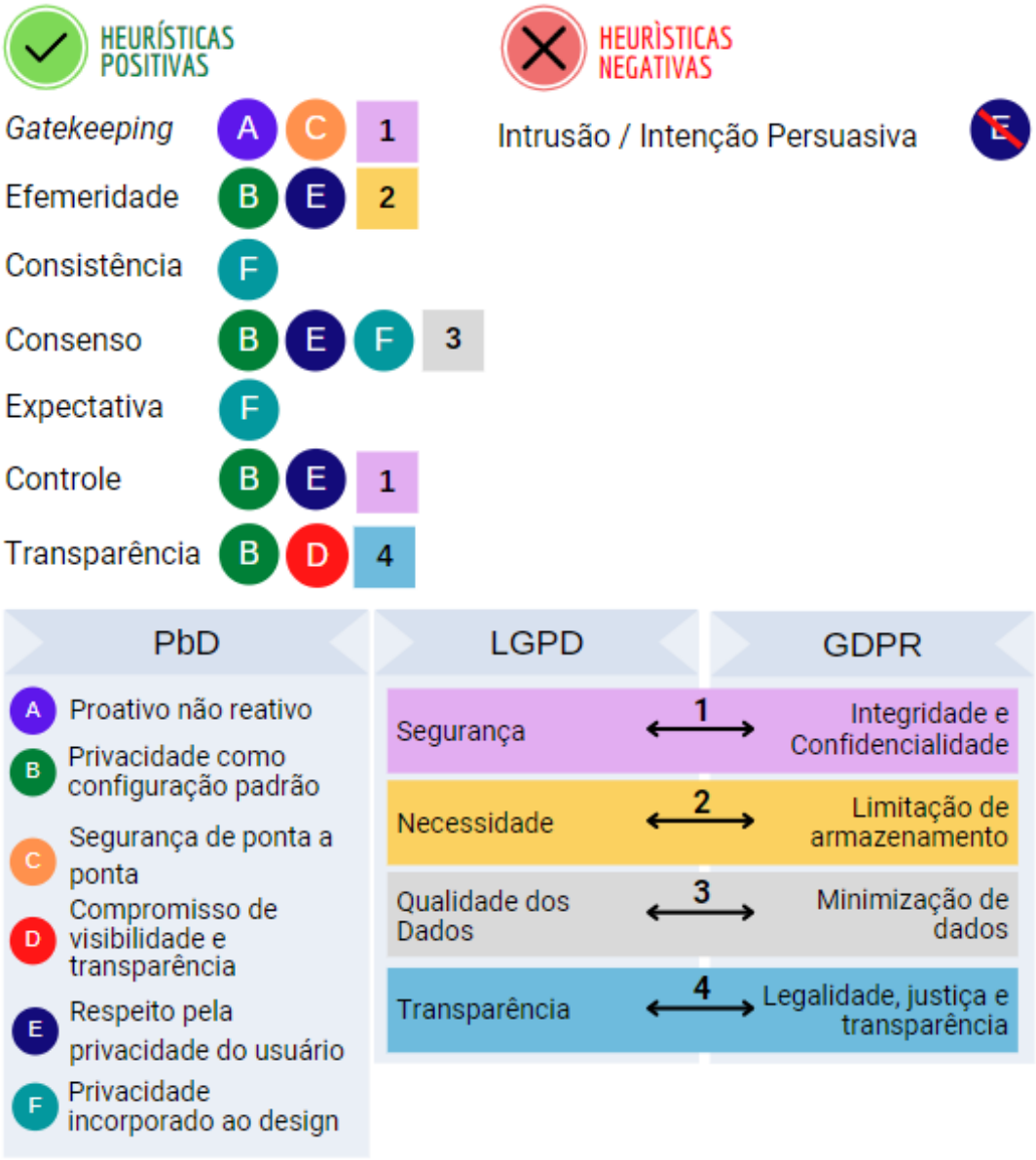
A Classe **Confiabilidade (Consistência, Consenso e Expectativa)** observada para ambas as redes sociais é um exemplo do princípio do PbD "Privacidade incorporada ao design". O Consenso heurístico também aplica os princípios PbD de "Respeito pela privacidade do usuário" e "Privacidade como configuração padrão". Em relação ao Consenso GDPR aplica-se o princípio da "minimização de dados" e para a LGPD o princípio da "qualidade dos dados". A heurística de **Controle** é um exemplo do princípio do PbD "Respeito pela privacidade do usuário" e "Privacidade como configuração padrão". Para o princípio LGPD fala-se de "Segurança" e para GDPR o princípio de "Integridade e confidencialidade". Por fim, a heurística de **Transparência** é um exemplo do princípio PbD "Compromisso com a visibilidade e transparência" e também "Privacidade como configuração padrão". Em relação à LGPD fala-se do princípio da "Transparência" e para o GDPR o princípio da "legalidade, justiça e transparência".

De acordo com os resultados da análise, o Facebook e Instagram demonstram estar preocupado em cumprir as leis GDPR e LGPD. A plataforma oferece ao usuário mecanismos para gerenciar suas configurações de privacidade. No entanto, o usuário deve decidir como gostaria de proteger sua privacidade e em que nível, considerando os quatro estados de privacidade pessoal (solidão, intimidade, anonimato e reserva) (WESTIN, 2003).

Ao examinar as heurísticas pesquisadas na literatura, observa-se os princípios do

Privacy by Design, que são um aliado no processo de adequação à legislação. O PbD figura como uma boa prática no processamento de dados pessoais e, conforme descrito na seção 2.1.3, abrange os princípios apresentados nas leis GDPR e LGPD. Além disso, ao avaliar a interface do Facebook e Instagram percebe-se que existem heurísticas de privacidade relacionadas aos princípios de PbD, LGPD e GDPR. A Figura 17 ilustra a relação entre as heurísticas e os princípios do PbD e os princípios descritos nas leis LGPD e GDPR.

Figura 17 – Relação entre as heurísticas e os princípios de *Privacy by Design* (PbD), Lei Geral de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR)



Fonte: Elaborada pela autora

A presença ou ausência de heurísticas relacionadas aos princípios propostos no *Privacy by Design* (PbD), na Lei Geral de Proteção de Dados (LGPD) e no *General*

Data Protection Regulation (GDPR) podem ter um impacto significativo nas questões de privacidade, dependendo da finalidade do princípio relacionado com a respectiva heurística. Quando as heurísticas não estão associadas a nenhum princípio, sua presença ou ausência pode afetar a decisão do usuário de divulgar informações. Além disso, como as configurações de privacidade do usuário são realizadas pode afetar o impacto percebido na privacidade com relação as informações divulgadas.

De acordo com Ferreyra, Meis e Heisel (2018), os usuários de Sites de Redes Sociais geralmente não são muito informados sobre os riscos de privacidade da interação *online*. Além disso, os usuários que consentem com a coleta e processamento de dados (ou seja, aqueles que aceitam as políticas de privacidade) geralmente não são informados sobre esses riscos antes de dar seu consentimento. A ausência de informações modula a gravidade percebida dos riscos de privacidade, beneficiando os provedores de serviços. Para desenvolver tecnologias preventivas, bem como para moldar políticas públicas que promovam a conscientização da privacidade nas redes sociais, a comunicação e o gerenciamento de riscos devem ser explorados.

5.3 Análise Qualitativa das Políticas de Privacidade de Redes Sociais

Nessa seção são apresentadas as observações referente a análise qualitativa das políticas de privacidade das redes sociais Facebook[1], Instagram[2], Twitter[3], LinkedIn[4] e TikTok[5]. No momento dessa análise, as políticas de privacidade das redes sociais tiveram sua última atualização no ano de 2022 e somente a política de privacidade do LinkedIn que teve sua última atualização em 2020.

A análise das políticas de privacidade das redes sociais possibilitou observar que as mesmas abrangem tópicos de mesma natureza, sendo eles:

I) Quais informações são coletadas;

II) Como as informações coletadas são usadas;

III) Como as informações são compartilhadas no produtos da empresa ou com parceiros, fornecedores, provedores de serviços e terceiros;

IV) Como o usuário pode gerenciar ou excluir suas informações;

V) Por quanto tempo as informações são mantidas;

VI) Como transferem as informações;

[1]Disponível em: <https://www.facebook.com/privacy/policy/>
[2]Disponível em: <https://privacycenter.instagram.com/policy/>
[3]Disponível em: <https://twitter.com/pt/privacy>
[4]Disponível em: <https://br.linkedin.com/legal/privacy-policy>
[5]Disponível em: <https://www.tiktok.com/legal/page/row/privacy-policy/pt-BR>

VII) Como respondem a solicitações legais, cumprem a legislação aplicável e previnem danos;

VIII) Como saber se a política de privacidade foi alterada;

IX) Como entrar em contato com a empresa;

X) Porque e como tratam as informações dos usuários.

Todavia, a ordem e a forma como tais tópicos são abordados divergem entre as políticas de privacidade avaliadas trazendo uma complexidade maior para automatizar a avaliação de políticas de privacidade. Dessa forma, dificultando que o próprio usuário da rede social realize uma Avaliação de Impacto de Privacidade (PIA), e obtenha maior entendimento sobre qual impacto a utilização de recursos disponíveis na rede social pode trazer a si próprio.

Com relação a análise dos requisitos de privacidade de um sistema baseado no método ProPAn (*Problem-based Privacy Analysis*) diante dos tópicos abordados nas políticas de privacidade é possível obter a informação de **como**, **em que quantidade**, **por quanto tempo** e **para qual propósito** os dados são coletados. Para a informação de **a quais declarações** os dados pessoais estão **disponíveis** em um domínio e **quais dados pessoais** disponíveis em um domínio **precisam ser vinculáveis** entre si, somente com a leitura da política de privacidade não é possível determinar. Sendo assim, necessário uma maior compreensão da plataforma da rede social.

A realização da distinção entre coleta de IPI obrigatória e voluntária pode ser feita analisando as informações fornecidas nos tópicos de "Quais informações são coletadas" e "Como as informações coletadas são usadas".

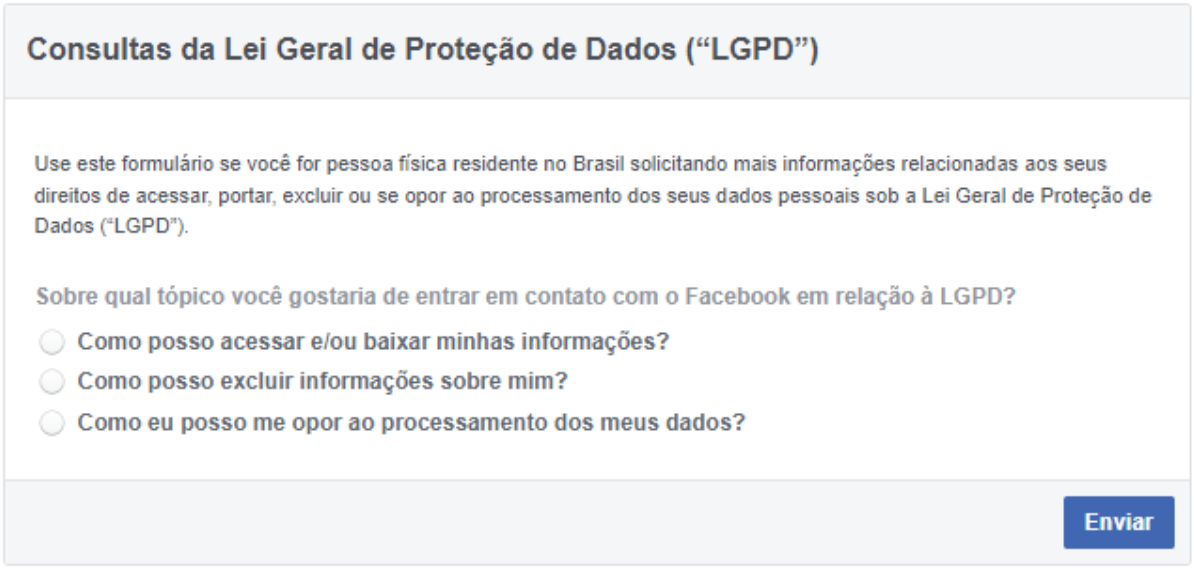
Com relação a conformidade da política de privacidade com a lei LGPD, observou-se que a política de privacidade da empresa Meta (produtos Facebook e Instagram) e a política de privacidade do TikTok reservam um seção para tratar particularidades específicas da jurisdição do Brasil. As redes sociais Twitter e LinkedIn não reservam uma seção específica para abordar sobre o Brasil, porém foi possível observar que no texto respondem as exigências contidas na lei sobre os direitos do titular de dados (Artigo 9º), sendo eles:

- Confirmação que os dados estão sendo processados;
- Acesso aos dados;
- Correção de dados incompletos, imprecisos e desatualizados;
- Solicitação para anonimização, bloqueio ou eliminação de dados desnecessários;
- Portabilidade de dados pessoais para terceiros;

- Objeção ao processamento de dados pessoais;
- Informações de entidades públicas e privadas com as quais compartilham-se dados;
- Informações sobre a possibilidade de recusar o fornecimento de dados pessoais e as respectivas consequências, quando aplicável; e
- Retirada do seu consentimento.

As Figuras 18 e 19 apresentam exemplos de formulários de contato disponibilizados pelas redes sociais Facebook e LinkedIn para tirar dúvidas e gerenciar informações pessoais da conta do usuário. Ao acessar a página de formulários fornecida pela plataforma o usuário pode enviar uma requisição para aprender como acessar e/ou baixar suas informações, excluir suas informações, opor ao processamento dos dados (revogar um consentimento prévio), transferir seus dados para outro controlador de dados, entre outros, conforme os direitos que o titular de dados possui de fazer uma requisição ao controlador a qualquer momento, descritos no Artigo 18º da LGPD.

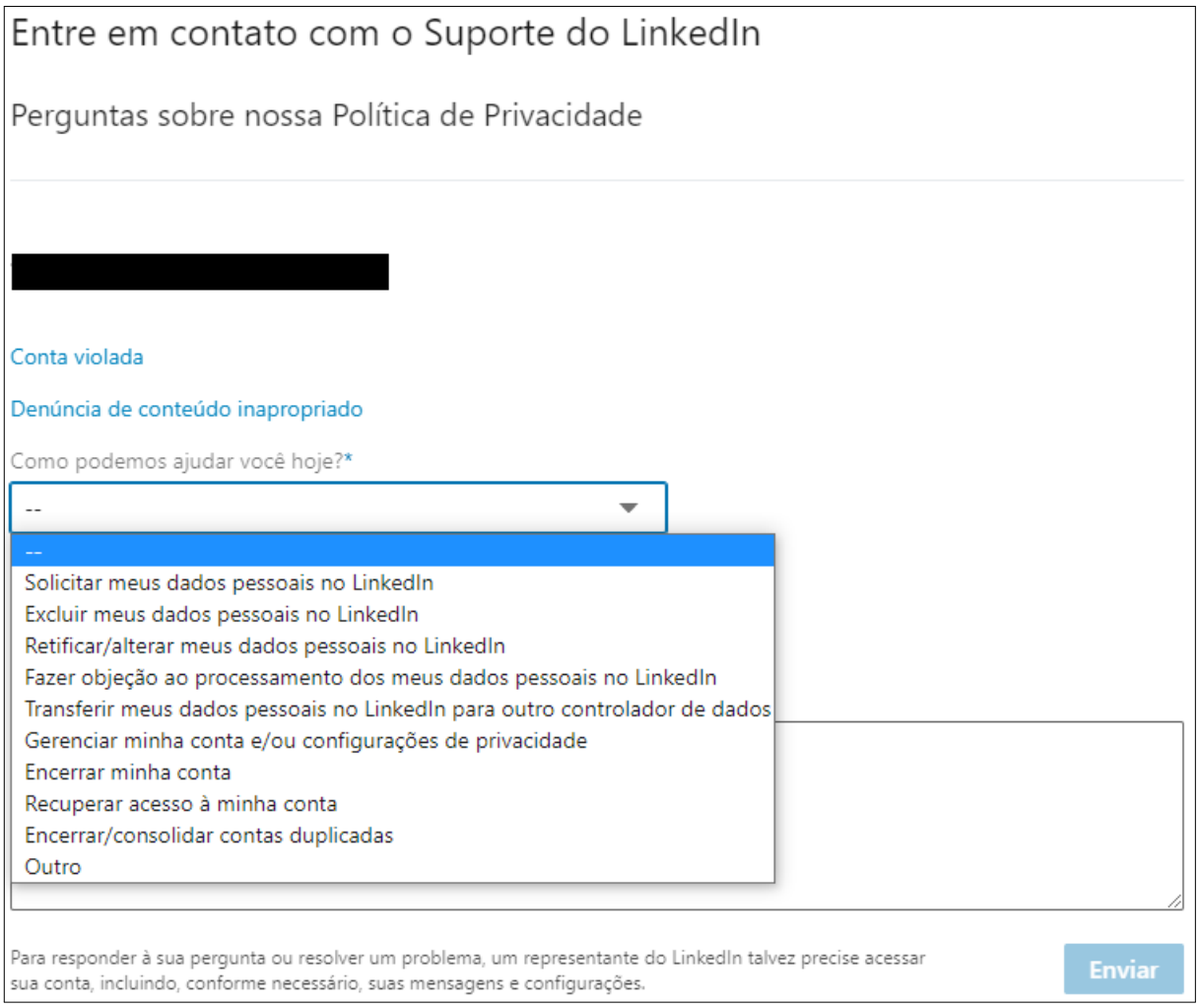
Figura 18 – Formulário do Facebook para solicitação de consultas sobre a lei LGPD



Fonte: Facebook

Referente as heurísticas cognitivas de privacidade estudadas nesta pesquisa, observa-se que nas políticas de privacidade das redes sociais pode-se evidenciar a presença das heurísticas de *Controle* e *Transparência*. Demais heurísticas somente foram observadas durante a inspeção da interface das redes sociais.

Figura 19 – Contato com o suporte do LinkedIn permitindo gerenciar informações pessoais conforme previso na LGPD



Fonte: LinkedIn

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Na última década, a privacidade do consumidor tornou-se uma questão prioritária para os formuladores de políticas, dadas as inúmeras ocorrências de vazamentos de informações pessoais que o tornaram um dos principais candidatos à legislação (NORBERG; HORNE; HORNE, 2007). Há uma preocupação com o consentimento explícito entre os subtemas abordados nas ações legislativas. Portanto, o usuário deve fornecer seu consentimento para o processamento de seus dados pessoais por meio de uma declaração ou ação afirmativa.

Com isso, este estudo investigou heurísticas cognitivas de privacidade, que influenciam os usuários quando eles têm apenas alguns segundos para decidir se devem clicar em uma URL ou um menu de opções ou caixas de seleção. A avaliação da privacidade por análise heurística mostrou que para tornar o sistema mais seguro e proteger a privacidade das pessoas, a empresa Meta (produtos Facebook e Instagram) disponibilizou aos seus usuários medidas em sua página de configurações de privacidade, identificando as principais características da proteção da privacidade dos dados dos indivíduos (Michel Protti, Chief Privacy Officer, Product, 2020). Ao analisar as heurísticas de "Transparência" e "Controle" nota-se que o Facebook e o Instagram permitem que os usuários controlem a coleta, armazenamento, tratamento e compartilhamento de dados em sua área de configurações de privacidade.

Ao inspecionar as heurísticas "Efemeridade" e "Controle", foi possível observar o princípio do PbD de "Respeito à privacidade do usuário" e "Privacidade como configuração padrão". Outro princípio do PbD reconhecido foi o "Compromisso com a visibilidade e transparência" considerando a heurística "Transparência". Além disso, observou-se o princípio do PbD de "Segurança de ponta a ponta - garantindo proteção completa do ciclo de vida" e "Proativo não reativo" observando a heurística "*Gatekeeping*". Ao examinar a classe de heurísticas "Confiabilidade", nota-se o princípio do PbD de "Privacidade incorporada ao *design*". Portanto, as plataformas das redes sociais estudadas incentivam o usuário a entender como seus dados são coletados, armazenados, tratados e compartilhados. Como resultado de tais aspectos percebidos, promove-se um alto nível de compartilhamento de informações entre os indivíduos e evidencia-se a conformidade com as leis GDPR e LGPD, pois o Facebook e o Instagram permitem que o usuário gerencie suas configurações de privacidade de acordo com os recursos da rede social.

Por outro lado, durante a investigação de heurísticas que inibem a divulgação de informações, notou-se que a configuração de anúncios na rede social do Facebook por padrão é definida como "Permitido". Sendo que a navegação na linha do tempo (*feed*) pode causar desconforto ao usuário, pois ele se sente confrontado com o aparecimento de anúncios vinculados aos seus interesses de navegação recentes. De acordo com o princípio do PbD de "Privacidade como configuração padrão", tal configuração deveria, por

padrão, ser definida como “Não permitido”. Para ambas as redes sociais, foram observados a ocorrência das heurísticas de “Intrusão”, “Limite Difuso” e “Incerteza”, as quais inibem o comportamento de divulgação de informações dos usuários. Tal percepção dessas heurísticas podem ir contra o princípio do PbD de “Respeito pela privacidade do usuário”.

Dessa forma, este estudo tem como principal contribuição a identificação de heurísticas específicas orientadas à privacidade que podem ajudar a comunidade de *design* e os engenheiros de *software* a projetar e desenvolver sistemas que apresentem pistas, sugestões e oportunidades para promover uma computação mais segura e confiável – desenvolvendo sistemas norteados na proteção de privacidade, com foco na preservação dos dados pessoais de um indivíduo ao longo do ciclo de vida da informação. No entanto, é essencial que *designers* e engenheiros de *software* usem essas heurísticas de forma ética e evitem enganar os usuários para revelar dados confidenciais que possam comprometer sua privacidade (GAMBINO et al., 2016).

Neste estudo, percebeu-se que as dicas de interface desempenham um papel crítico no desencadeamento de regras mentais, ditando comportamentos de disseminação. Compreender o número e a diversidade de sugestões (heurísticas) a que os usuários estão suscetíveis permite a criação de diretrizes explícitas para informá-los, alertá-los e educá-los, avançando o conhecimento nessa área. Apesar disso, parece que não foi desenvolvido nenhum conjunto de heurísticas operacionais que possam operacionalizar os sete princípios do PbD e os princípios descritos nas leis GDPR e LGPD.

Durante a análise qualitativa das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok, nota-se que as mesmas abordam os mesmos tópicos. Todavia, não há um padrão em como o conteúdo desses tópicos serão descritos, o que dificulta a realização de uma análise automática das políticas de privacidade. Durante a análise, pode-se averiguar que as políticas de privacidade tratam questões exigidas pelas legislações vigentes de privacidade, o que indica que as mesmas estão preocupadas em estar em conformidade com as regras estabelecidas.

Com relação aos objetivos específicos propostos para este estudo, o objetivo de “Realizar uma revisão sistemática da literatura para identificar quais são as metodologias propostas e como é realizada a elaboração de uma *Avaliação de Impacto de Privacidade*” foi explicitado no Capítulo 3. O objetivo de “Realizar uma análise qualitativa das políticas de privacidade das redes sociais Facebook, Instagram, Twitter, LinkedIn e TikTok conforme metodologia identificada para elaboração de uma PIA” foi apresentado na Seção 5.3. O objetivo de “Realizar um levantamento das heurísticas cognitivas de privacidade que influenciam as decisões dos indivíduos de proteger ou renunciar à sua privacidade” foi disposto na Seção 5.1. Para o objetivo de “Avaliar o possível impacto à privacidade do usuário de acordo com as heurísticas cognitivas de privacidade observadas durante a análise das redes sociais Facebook e Instagram” o mesmo foi discutido na Seção 5.2. Por fim, o objetivo de “Realizar a análise da relação das heurísticas cognitivas de privacidade com

os princípios do *Privacy by Design* e os princípios das leis LGPD e GDPR" foi evidenciado na Subseção 5.2.4.

Como sugestões para trabalhos futuros, com relação a análise heurística propõe-se realizar a inspeção das redes sociais Twitter, LinkedIn e TikTok. Podendo assim avaliar as similaridades e diferenças na forma como tais redes sociais abordam as heurísticas de privacidade estudadas. Além disso, propõe-se realizar um estudo com usuários de serviços *online* para formalizar um conjunto de heurísticas de privacidade que operacionalizem os sete princípios de *Privacy by Design* e os princípios das leis GDPR e LGPD, permitindo que os controladores de dados demonstrem transparência na coleta, armazenamento, tratamento e compartilhamento de dados pessoais. Como conseguinte, sugere-se também o estudo da percepção dos usuários sobre privacidade em diferentes culturas. Com relação as políticas de privacidade, sugere-se a aplicação de um algoritmo de análise de tópicos (exemplo: LDA) como uma forma de facilitar a avaliação de tais políticas pelos usuários de redes sociais. Por fim, propõe-se a atualização e extensão do trabalho de identificação das definições de privacidade apresentadas na Figura 1 e a continuação das revisões sistemáticas de literatura para identificar metodologias para elaboração de Avaliação de Impacto de Privacidade (PIA) e heurísticas de privacidade que influenciam na divulgação de informações.

REFERÊNCIAS

ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science*, American Association for the Advancement of Science, v. 347, n. 6221, p. 509–514, 2015. ISSN 0036-8075. Disponível em: <https://science.sciencemag.org/content/347/6221/509>. 19, 22, 42

Agência Brasil. *Especialista recomenda prazo de adaptação à Lei de Proteção de Dados*. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-07/especialista-recomenda-prazo-de-adaptacao-lei-de-protecao-de-dados?amp>. Acesso em: 12 de Julho de 2020. 46, 65

AHMADIAN, A. S. et al. Supporting privacy impact assessment by model-based privacy analysis. In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2018. (SAC '18), p. 1467–1474. ISBN 9781450351911. Disponível em: <https://doi.org/10.1145/3167132.3167288>. 21, 23, 54, 56, 58, 59, 60, 61

AL-FEDAGHI, S.; JERAGH, A. A flow-based model to assess privacy impact. *Journal of Information Technology Impact*, v. 11, n. 2, p. 101–120, 2011. 31

AL-MOMANI, A. et al. A privacy-aware v-model for software development. In: *2019 IEEE Security and Privacy Workshops (SPW)*. San Francisco, CA, USA, USA: IEEE, 2019. p. 100–104. 54, 57, 58, 60, 61

ALLEN, A. *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press, 2011. (Oxford Scholarship Online: Philosophy). ISBN 9780195141375. 26, 28

ANARAKY, R. G. et al. To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2021. p. 1–14. ISBN 9781450380966. Disponível em: <https://doi.org/10.1145/3411764.3445204>. 74

BADEN, R. et al. Persona: An online social network with user-defined privacy. In: *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication*. New York, NY, USA: Association for Computing Machinery, 2009. (SIGCOMM '09), p. 135–146. ISBN 9781605585949. Disponível em: <https://doi.org/10.1145/1592568.1592585>. 20

BIEKER, F. et al. A process for data protection impact assessment under the european general data protection regulation. In: SCHIFFNER, S. et al. (Ed.). *Privacy Technologies and Policy*. Cham: Springer International Publishing, 2016. p. 21–37. ISBN 978-3-319-44760-5. 54, 56, 58, 59, 60, 61

BIRNHACK, M.; TOCH, E.; HADAR, I. Privacy mindset, technological mindset. *SSRN Electronic Journal*, n. June, p. 1–71, 2014. 23

CAVOUKIAN, A. *The 7 Foundational Principles*. Information & Privacy Commissioner, 2009. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 17 de Junho de 2019. 34, 35, 36

CHASSANG, G. The impact of the eu general data protection regulation on scientific research. *Ecancermedicalscience*, ecancer, v. 11, n. 709, p. 1–13, 2017. Disponível em: <https://doi.org/10.3332/ecancer.2017.709>. 19

CLARKE, R. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Xamax Consultancy, 1997. Revisões Set. 1999, Dez. 2005, Ago. 2006, Oct. 2013 e Jul. 2016. Disponível em: <http://www.rogerclarke.com/DV/Intro.html>. Acesso em: 12 de Julho de 2020. 26, 27, 28, 29, 30

CLARKE, R. Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, v. 25, n. 2, p. 123 – 135, 2009. ISSN 0267-3649. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0267364909000302>. 23

DAYALU, P.; PUNNAGAI, M. GDPR: A privacy regime. *International Journal of Trend in Scientific Research and Development*, Volume-3, p. 713–716, 06 2019. 44

DENNEDY, M.; FOX, J.; FINNERAN, T. *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. 1. ed. Berkeley, CA: Apress, 2014. 1-362 p. Disponível em: <https://doi.org/10.1007/978-1-4302-6356-2>. 33

EDWARDS, L.; VEALE, M. Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"? *IEEE Security Privacy*, v. 16, n. 3, p. 46–54, may 2018. 21, 44

Engineering at Meta. *Rapid release at massive scale*. 2017. Disponível em: <https://engineering.fb.com/web/rapid-release-at-massive-scale/>. Acesso em: 17 de Junho de 2020. 76

ENSERINK, M.; CHIN, G. The end of privacy. *Science*, American Association for the Advancement of Science, v. 347, n. 6221, p. 490–491, 2015. ISSN 0036-8075. Disponível em: <https://science.sciencemag.org/content/347/6221/490>. 19

ESTIVILL-CASTRO, V.; NETTLETON, D. F. Privacy tips: Would it be ever possible to empower online social-network users to control the confidentiality of their data? In: *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*. New York, NY, USA: Association for Computing Machinery, 2015. (ASONAM '15), p. 1449–1456. ISBN 9781450338547. Disponível em: <https://doi.org/10.1145/2808797.2809279>. 20

European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>. Acesso em: 20 de Outubro de 2019. 20, 21, 32, 34

Facebook. *Sobre os Anúncios do Facebook*. 2020. Disponível em: <https://www.facebook.com/ads/about/>. Acesso em: 24 de Junho de 2020. 80

FERREYRA, N. E. D.; MEIS, R.; HEISEL, M. At your own risk: Shaping privacy heuristics for online self-disclosure. In: *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. [S.l.: s.n.], 2018. p. 1–10. 86

FINN, R. L.; WRIGHT, D.; FRIEDEWALD, M. Seven types of privacy. In: _____. *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013. p. 3–32. ISBN 978-94-007-5170-5. Disponível em: <https://doi.org/10.1007/978-94-007-5170-5_1>. 26, 29, 30

GAMBINO, A. et al. User disbelief in privacy paradox: Heuristics that determine disclosure. In: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2016. (CHI EA '16), p. 2837–2843. ISBN 9781450340823. Disponível em: <https://doi.org/10.1145/2851581.2892413>. 16, 20, 65, 69, 70, 71, 73, 83, 92

GDPR EU. *Richie Koch - What is the LGPD? Brazil's version of the GDPR*. 2020. Disponível em: <https://gdpr.eu/gdpr-vs-lgpd/>. Acesso em: 10 de Junho de 2020. 45, 46

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Editora Atlas S.A., 2002. ISBN 8522431698. 63

HADAR, I. et al. Privacy by designers: Software developers' privacy mindset. In: *Proceedings of the 40th International Conference on Software Engineering*. New York, NY, USA: Association for Computing Machinery, 2018. (ICSE '18), p. 396. ISBN 9781450356381. Disponível em: <https://doi.org/10.1145/3180155.3182531>. 23

HANSEN, M.; JENSEN, M.; ROST, M. Protection goals for privacy engineering. In: *2015 IEEE Security and Privacy Workshops*. Colmar, France: IEEE, 2015. p. 159–166. 39, 40

HARBIRD, R. et al. Privacy Impact Assessment with PRAIS. In: *8th Privacy Enhancing Technologies Symposium (PETS 2008)*. Leuven, Belgium: UCL Department of Computer Science, 2008. Disponível em: <http://www0.cs.ucl.ac.uk/staff/r.harbird/prais/>. 54, 55, 57, 59, 61

HAZEYAMA, A. et al. Literature survey on technologies for developing privacy-aware software. In: *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*. Beijing, China: IEEE, 2016. p. 86–91. 34

HIMMEL, J. et al. Privacy points as a method to support Privacy Impact Assessments. In: *Proceedings of the 2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal Aspects of Data PRivacy and SEcurity*. USA: IEEE Computer Society, 2015. (TELERISE '15), p. 50–53. ISBN 9781467370974. Disponível em: <https://doi.org/10.1109/TELERISE.2015.17>. 54, 55, 57, 59, 60, 61

IAPP. *What does privacy mean?* Portsmouth, NH - USA: International Association of Privacy Professionals, 2020. Disponível em: <https://iapp.org/about/what-is-privacy/>. Acesso em: 08 de Julho de 2020. 40

ICMP Consultoria em TI. *O que é a Lei Geral de Proteção de Dados (LGPD)*. 2020. Disponível em: <https://www.icmpconsultoria.com.br/post/o-que-e-a-lgpd>. Acesso em: 12 de Julho de 2020. 46

ISO/IEC. *ISO/IEC 29100:2011 Information technology – Security techniques – Privacy Framework*. Technical report, International Organization for Standardization and International Electrotechnical Commission, 2011. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en>. Acesso em: 08 de Julho de 2020. 34, 37

ISO/IEC. *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Technical report, International Organization for Standardization and International Electrotechnical Commission, 2018. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Acesso em: 08 de Julho de 2020. 39

KHO, N. D. *GDPR for Content Design, Development, and Deployment*. 2018. Disponível em: <http://www.econtentmag.com/Articles/Editorial/Feature/GDPR-for-Content-Design-Development-and-Deployment-126107.htm>. Acesso em: 17 de Junho de 2019. 44

KITCHENHAM, B. et al. Systematic literature reviews in software engineering – a systematic literature review. *Information and Software Technology*, v. 51, n. 1, p. 7–15, 2009. ISSN 0950-5849. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0950584908001390>. 49

KOKOLAKIS, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, v. 64, p. 122–134, 2017. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404815001017>. 42

KOOPS, B.-J. et al. A typology of privacy. *University of Pennsylvania Journal of International Law (forthcoming)*, v. 38, 12 2016. 25, 26, 27, 28, 29, 30

KROENER, I.; WRIGHT, D. A strategy for operationalizing privacy by design. *The Information Society*, Routledge, v. 30, n. 5, p. 355–365, 2014. 35

Lei Nº 13.709. *Lei Nº 13.709, De 14 De Agosto De 2018*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 de Outubro de 2019. 21, 31, 32, 34, 35, 43, 44

Lei Nº 13.853. *Lei Nº 13.853, De 8 De Julho De 2019*. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 20 de Outubro de 2019. 32

LGPD Brasil. *Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/18*. 2019. Disponível em: <https://www.lgpdbrasil.com.br/>. Acesso em: 20 de Outubro de 2019. 20, 43, 46

MARTIN, Y.; KUNG, A. Methods and tools for GDPR compliance through privacy and data protection engineering. In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. London, UK: IEEE, 2018. p. 108–111. 23, 62

MEIS, R. *Problem-based Privacy Analysis (ProPAn) – A Computer-aided Privacy Requirements Engineering Method*. 12 2018. Tese (Doutorado) — Universität Duisburg-Essen. 25, 34, 36, 37, 38, 39, 66

MEIS, R.; HEISEL, M. Systematic identification of information flows from requirements to support privacy impact assessments. In: *2015 10th International Joint Conference on Software Technologies (ICSOFT)*. Colmar, France: IEEE, 2015. v. 2, p. 1–10. 54, 55, 57, 59, 60, 61

Meta. *Facebook apresenta novas opções para proteger dados e privacidade em conformidade com a GDPR*. 2018. Disponível em: <https://pt-br.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr>. Acesso em: 13 de Junho de 2022. 77, 78

Meta. *Founder's Letter, 2021*. 2021. Disponível em: <https://about.fb.com/news/2021/10/founders-letter/>. Acesso em: 19 de Dezembro de 2021. 65

Michel Protti, Chief Privacy Officer, Product. *Fighting Platform Abuse, Simplifying Privacy in Groups, and Protecting Information While Sharing Data*. 2020. Disponível em: <https://about.fb.com/news/2020/06/privacy-improvements/>. Acesso em: 24 de Junho de 2020. 91

NISTIR 8062. *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. U.S. Department of Commerce, 2017. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>. Acesso em: 08 de Julho de 2020. 33, 40, 41

NORBERG, P.; HORNE, D.; HORNE, D. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, v. 41, p. 100–126, 03 2007. 42, 71, 91

NOTARIO, N. et al. PRIPARE: integrating privacy best practices into a privacy engineering methodology. In: *2015 IEEE Security and Privacy Workshops*. San Jose, CA, USA: IEEE, 2015. p. 151–158. 54, 55, 58, 59, 60, 61

OECD. *OECD Privacy Guidelines*. 2020. Disponível em: <https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>. Acesso em: 13 de Janeiro de 2020. 34, 35

OETZEL, M. C.; SPIEKERMANN, S. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, Taylor & Francis, v. 23, n. 2, p. 126–150, 2014. 23, 54, 55, 57, 59, 61

OLIVEIRA, M.; MATTEDI, A.; SEABRA, R. Usability evaluation model of an application with emphasis on collaborative security: an approach from social dimensions. *Journal of the Brazilian Computer Society*, Springer Open, v. 27:3, p. 1–32, 2021. Disponível em: <https://doi.org/10.1186/s13173-021-00108-8>. 42, 84

ORTIZ-OSPINA, E. *Our World In Data - The rise of social media*. 2019. Accessed 24 June 2020. Disponível em: <https://ourworldindata.org/rise-of-social-media>. Acesso em: 24 de Junho de 2020. 76

Resultados Digitais. *Pesquisa indica recursos mais relevantes de mídias sociais + 95 estatísticas de redes em 2022*. 2022. Disponível em: <https://resultadosdigitais.com.br/marketing/estatisticas-redes-sociais/#:~:text=Estat%C3%ADsticas%20do%20Instagram,n%C3%BAmero%20cresceu%2017%2C9%25.> Acesso em: 22 de Setembro de 2022. 80

REUBEN, J. et al. Privacy impact assessment template for provenance. In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*. Salzburg, Austria: IEEE, 2016. p. 653–660. 54, 56, 58, 59, 60, 61

RODRIGUES, A. A.; VALENTIM, N. M. C.; CONTE, T. Privacy evaluation of online social network stories feature: An empirical study with pdm. In: *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2017. (IHC 2017), p. 1–10. ISBN 9781450363778. Disponível em: <https://doi.org/10.1145/3160504.3160528>. 20

SOLOVE, D. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, p. 477–560, 2006. 29, 30

Statista. *Facebook - Statistics & Facts*. 2021. Disponível em: <https://www.statista.com/topics/751/facebook/>. 76

SUNDAR, S. S. et al. Online privacy heuristics that predict information disclosure. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2020. (CHI '20), p. 1–12. ISBN 9781450367080. Disponível em: <https://doi.org/10.1145/3313831.3376854>. 16, 20, 65, 72, 73, 83

US Federal Trade Commission. *Privacy online: A report to congress*. Federal Trade Commission, 1998. Disponível em: <https://www.ftc.gov/reports/privacy-online-report-congress>. Acesso em: 20 de Julho de 2020. 33, 34, 35

VINCENT, J. M. et al. The cognitive heuristics behind disclosure decisions. In: *Social Informatics. SocInfo 2017*. Oxford, United Kingdom: Springer, 2017. v. 10539, p. 591–607. ISBN 978-3-319-67216-8. Disponível em: <https://eprints.soton.ac.uk/414781/>. 16, 20, 65, 70, 71, 73, 83

WANG, Y.; LIU, J. An attribute-based statistic model for privacy impact assessment. *2016 International Conference on Collaboration Technologies and Systems*, Faculty Research & Publications, p. 619–621, 2016. 54, 56, 58, 59, 60

WANG, Y.; NEPALI, R. K. Privacy impact assessment for online social networks. In: *2015 International Conference on Collaboration Technologies and Systems (CTS)*. Atlanta, GA, USA: IEEE, 2015. p. 370–375. 54, 56, 58, 59, 60

WESTIN, A. F. *Privacy and Freedom*. New York: Ig Publishing, 1967. ISBN 9781935439974. 25, 26

WESTIN, A. F. Social and political dimensions of privacy. *Journal of Social Issues*, v. 59, n. 2, p. 431–453, 2003. Disponível em: <https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/1540-4560.00072>. 25, 26, 84

WRIGHT, D. Should privacy impact assessments be mandatory? *Commun. ACM*, Association for Computing Machinery, New York, NY, USA, v. 54, n. 8, p. 121–131, ago. 2011. ISSN 0001-0782. Disponível em: <https://doi.org/10.1145/1978542.1978568>. 22, 32, 62

WRIGHT, D. Making Privacy Impact Assessment more effective. *The Information Society*, Routledge, USA, v. 29, n. 5, p. 307–315, 10 2013. ISSN 0197-2243. Disponível em: <https://doi.org/10.1080/01972243.2013.825687>. 54, 55, 60, 62

WRIGHT, D.; FINN, R.; RODRIGUES, R. A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research*, v. 9, n. 1, p. 160–180, 2013. 62

WU, H. et al. A heuristic model for supporting users' decision-making in privacy disclosure for recommendation. *Security and Communication Networks*, v. 2018, p. 1–13, 02 2018. 20, 73

WU, P. The privacy paradox in the context of online social networking: A self-identity perspective: Journal of the association for information science and technology. *Journal of the Association for Information Science and Technology*, v. 70, 11 2018. 42

WUYTS, K. et al. Effective and efficient privacy threat modeling through domain refinements. In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2018. (SAC '18), p. 1175–1178. ISBN 9781450351911. Disponível em: <https://doi.org/10.1145/3167132.3167414>. 54, 57, 58, 60

YOUNG, A.; QUAN-HAASE, A. Privacy protection strategies on facebook. *Information*, v. 16, 05 2013. 42