Extensões BPMN para Conformidade com a LGPD e GDPR: Um Panorama do Estado da Arte

Geraldo Gabriel Crelier dos Santos[1 [0009−0008−4394−7444]], Henrique Prado de Sá Sousa[1 [0000−0003−2150−8113]], Eduardo Kinder Almentero[2 [0000−0002−5664−1080]], and Tadeu Moreira de Classe[1 [0000−0001−9849−5133]]

[1] Universidade Federal do Estado do Rio de Janeiro (UNIRIO), Brasil
{geraldo.santos,hsousa,tadeu.classe}@uniriotec.br
[2] Universidade Federal Rural do Rio de Janeiro (UFRRJ), Brasil
almentero@ufrrj.br

Resumo A entrada em vigor das regulamentações sobre proteção de dados, em destaque o GDPR (*General Data Protection Regulation*) na Europa e a LGPD (Lei Geral de Proteção de Dados) no Brasil, criaram demanda por técnicas de modelagem capazes de representar requisitos de privacidade em processos de negócio. Embora o BPMN seja padrão *de facto* para modelagem de processos, seus elementos nativos carecem de suporte explícito para proteção de dados pessoais. Este artigo apresenta um Mapeamento Sistemático da Literatura (MSL) que investiga se e como a BPMN tem sido estendida para suportar conformidade com privacidade no contexto do GDPR e da LGPD. Após análise de 18 estudos selecionados, os resultados indicam crescimento do tema a partir de 2018, com o *framework* PE-BPMN como linha de pesquisa mais proeminente, e revelam contribuições em anotação visual, extensões ontológicas, verificação semi-automatizada e detecção de conflitos entre requisitos de privacidade. Destaca-se que apenas um estudo aborda diretamente a LGPD, evidenciando lacuna significativa no contexto brasileiro.

Keywords: BPMN, Privacy, LGPD, GDPR, Requirements Engineering, Privacy-by-Design, Business Process Modeling

1 Introdução

O crescimento exponencial da digitalização de processos organizacionais nas últimas décadas consolidou a *Business Process Model and Notation* (BPMN) como o padrão de fato para a modelagem de processos de negócio em Sistemas de Informação (SI). Desenvolvida pelo *Object Management Group* (OMG), a BPMN oferece uma linguagem gráfica padronizada e expressiva, capaz de representar fluxos de controle, colaborações interorganizacionais, coreografias de serviços e subprocessos em diferentes níveis de abstração [8]. Sua adoção massiva, tanto na academia quanto na indústria, decorre não apenas da riqueza semântica de sua notação, mas também de seu alinhamento com iniciativas de modelagem

Proceedings of the 29th Workshop on Requirements Engineering (WER2026),
August 11-13, 2026, La Plata, Argentina.
https://doi.org/10.29327/1884517.29-21

orientada a serviços e transformação digital, tornando-a um instrumento central no ciclo de vida do desenvolvimento de sistemas, desde o levantamento de requisitos até a execução e monitoramento facilmente compreensível de processos automatizados entre *stakeholders* técnicos ou não[10].

Em paralelo ao amadurecimento das práticas de BPM, o cenário regulatório global passou por transformações profundas no que diz respeito à proteção de dados pessoais. A aprovação do Regulamento Geral de Proteção de Dados da União Europeia (GDPR - *General Data Protection Regulation*, EU 2016/679)[19], em vigor desde maio de 2018, estabeleceu um novo paradigma jurídico-técnico fundado nos princípios de minimização de dados, finalidade, responsabilização (*accountability*) e privacidade desde a concepção (*Privacy-by-Design*) [5]. No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), em vigor desde 2020, incorporou princípios análogos, exigindo das organizações que tratem dados pessoais de titulares brasileiros a adoção de medidas técnicas e organizacionais compatíveis com a legislação [13]. Essas regulamentações não apenas impõem obrigações jurídicas, mas também demandam uma reconfiguração profunda da forma como os processos de negócio são projetados, documentados e auditados, elevando a conformidade regulatória à condição de requisito não funcional crítico no desenvolvimento de sistemas de informação [1].

Embora o BPMN seja amplamente utilizado para modelar processos que tratam dados pessoais, a especificação nativa da notação carece de mecanismos explícitos para representar requisitos de privacidade e proteção de dados [17]. Elementos como a identificação de bases legais para o tratamento de dados (consentimento, legítimo interesse, obrigação legal), a categorização de dados pessoais sensíveis, as obrigações de minimização e retenção, os fluxos de transferência internacional de dados e os direitos dos titulares, como o direito ao esquecimento e a portabilidade, não possuem representação formal na notação BPMN 2.0.2. Essa lacuna semântica impõe uma tensão estrutural entre duas dimensões críticas do desenvolvimento de sistemas: de um lado, a necessidade de modelar processos de negócio com precisão e clareza; de outro, a exigência legal e ética de garantir a conformidade com regulamentações de proteção de dados desde as fases iniciais do projeto. Como consequência, os analistas e arquitetos de processos são forçados a recorrer a anotações informais, documentos externos ou abordagens *ad hoc* para representar obrigações de privacidade, comprometendo a rastreabilidade, a auditabilidade e a verificabilidade da conformidade regulatória ao longo do ciclo de vida do processo [1].

A comunidade científica tem respondido a esse desafio com a proposição de extensões, metamodelos, perfis e mecanismos de anotação para a BPMN, com o objetivo de incorporar semânticas de privacidade e proteção de dados diretamente na notação de processos. Contudo, a produção acadêmica nessa área apresenta características de fragmentação que dificultam a consolidação de conhecimento e a adoção prática: As propostas existentes adotam abordagens heterogêneas, desde extensões sintáticas formais para apoiar simulações de processos de negócio [20], passando por mecanismos de coloração visual, como em [21]. Até

mesmo ontologias de domínio acopladas a ferramentas CASE e agentes de IA [3] são desenvolvidas de forma independente, sem convergência para um padrão amplamente aceito, e frequentemente focam em aspectos parciais da conformidade, como o GDPR isoladamente, sem considerar regulamentações nacionais como a LGPD. Ademais, a sobreposição entre requisitos de privacidade e requisitos de segurança da informação gera ambiguidades conceituais que comprometem a precisão das soluções propostas [14]. Essa dispersão do estado da arte justifica a necessidade urgente de um estudo de mapeamento sistemático que consolide, classifique e avalie criticamente as abordagens existentes.

Diante desse contexto, o presente artigo tem como objetivo realizar um Mapeamento Sistemático da Literatura (MSL) sobre extensões e adaptações da BPMN voltadas ao suporte de conformidade com privacidade e proteção de dados pessoais, com ênfase nos requisitos estabelecidos pelo GDPR e pela LGPD. Especificamente, objetiva-se: (i) identificar e catalogar as contribuições que propõem extensões explícitas à notação BPMN para a representação de requisitos de privacidade; (ii) caracterizar as abordagens adotadas em termos de mecanismos de extensão, ferramentas de suporte, técnicas de verificação e regulamentações contempladas; (iii) avaliar a distribuição temporal, geográfica e metodológica da produção científica no tema; e (iv) identificar lacunas de pesquisa, em especial no que concerne à LGPD e ao contexto brasileiro. O estudo segue o protocolo metodológico de Kitchenham e Charters [15], reconhecido como referência em revisões sistemáticas da literatura em Engenharia de Software, garantindo reprodutibilidade, rigor na seleção de estudos e transparência na avaliação de elegibilidade.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta o referencial teórico sobre BPMN e regulamentações de privacidade; a Seção 3 descreve o protocolo metodológico do MSL; a Seção 4 apresenta o Esquema de Classificação dos estudos e resultados; a Seção 5 apresenta a análise dos estudos incluídos, implicações dos achados e as ameaças à validade; e a Seção 6 apresenta as conclusões e direcionamentos para trabalhos futuros.

2 Fundamentação Teórica

A compreensão do estado da arte sobre as extensões da notação *Business Process Model and Notation* (BPMN) para conformidade com a proteção de dados exige a articulação de três pilares fundamentais: a modelagem de processos de negócio, o paradigma de *Privacy by Design* (PbD) e os marcos regulatórios contemporâneos, representados pelo *General Data Protection Regulation* (GDPR) e pela Lei Geral de Proteção de Dados (LGPD).

2.1 Modelagem de Processos com BPMN e sua Extensibilidade

A gestão de processos de negócio (*Business Process Management* - BPM) consolidou-se como uma disciplina essencial para a transparência organizacional. Dentro deste ecossistema, a notação BPMN 2.0 emergiu como o padrão de

fato, provendo uma linguagem comum entre analistas de negócio e desenvolvedores de sistemas [10].

Contudo, a notação padrão foca primordialmente na lógica de controle e no fluxo de mensagens, carecendo de semântica nativa para expressar requisitos não-funcionais complexos, como a privacidade. Conforme evidenciado por Agostinelli et al. (2026), a integração de restrições de privacidade diretamente nos modelos de processo é crucial para evitar violações de dados (*data breaches*). A arquitetura da BPMN permite essa integração por meio de mecanismos de extensibilidade, que podem ocorrer via: **Extensão do Metamodelo:** Alterações nas classes e atributos estruturais da linguagem; **Perfis BPMN (Profiles):** Adaptação via estereótipos e valores etiquetados (*tagged* values); e **Anotações Visuais:** Introdução de marcadores gráficos sem alteração da lógica subjacente. Essa flexibilidade é o que permite a criação de variantes como a *Privacy-enhanced* BPMN (PE-BPMN), proposta por Pullonen [17], focada na análise de fluxos de informações privadas e salvaguardas técnicas.

2.2 Marcos Regulatórios: GDPR e LGPD

A proteção de dados pessoais transicionou de uma abordagem passiva para um modelo de responsabilidade proativa (accountability). A GDPR (Regulamento UE 2016/679)[19] estabeleceu precedentes globais que influenciaram diretamente a LGPD brasileira (Lei nº 13.709/2018)[9]. Ambas as normas exigem que as organizações não apenas protejam os dados, mas que demonstrem conformidade em todo o ciclo de vida do tratamento. Conceitos-chave extraídos da literatura selecionada [4][18] apontam que a conformidade exige o mapeamento sistemático de: **Consentimento:** A base legal para o processamento de dados; **Minimização de Dados:** A coleta estritamente necessária para a finalidade pretendida; **Direitos do Titular:** Mecanismos para acesso, retificação e o "direito ao esquecimento"; **Segurança (Integridade e Confidencialidade):** Medidas técnicas para prevenir acessos não autorizados.

2.3 *Privacy by Design* e Engenharia de Requisitos de Privacidade

A integração entre legislação e técnica materializa-se no conceito de *Privacy by Design* (PbD). O PbD preconiza que a privacidade deve ser incorporada de forma intrínseca e por padrão no desenvolvimento de sistemas. Na engenharia de software, isso se traduz na captura de requisitos de privacidade ainda na fase de modelagem de processos [12].

A literatura aponta desafios significativos nessa integração. Ramadan et al. [18] destacam que requisitos de segurança e minimização de dados podem ser inerentemente conflitantes, exigindo *frameworks* (como o proposto no método LGPD4BP) para detectar e resolver tais inconsistências de forma semiautomatizada. Além disso, a utilização de ontologias [6] e modelos de verificação formal [8] surge como uma tendência para garantir que os modelos BPMN estendidos sejam semanticamente consistentes com as disposições legais da GDPR/LGPD.

Método de Pesquisa

A condução deste estudo segue o protocolo de Mapeamento Sistemático da Literatura (MSL) por meio da classificação e análise de frequência de publicações [16], cujo rigor metodológico baseia-se nas diretrizes de Kitchenham e Charters (2007) [15], dividindo-se em três fases principais: planejamento, condução e documentação dos resultados. Todo o conteúdo deste mapeamento encontra-se armazenado no repositório Zenodo: https://doi.org/10.5281/zenodo.18830846

O objetivo primordial deste MSL é identificar como a literatura técnica integra a notação BPMN aos requisitos de privacidade da LGPD e GDPR. Para tanto, formularam-se as seguintes questões de pesquisa, conforme detalhadas abaixo:

QP1: Quais são as principais abordagens e métodos utilizados para integrar requisitos de privacidade (LGPD/GDPR) à notação BPMN? Esta questão busca avaliar as propostas de modelagem vinculadas às normas legais.

QP2: Como a frequência de publicações sobre extensões de BPMN para privacidade tem evoluído ao longo do tempo? Visa identificar a maturidade do campo e a liderança regional (ex: influência da GDPR na Europa vs. LGPD no Brasil).

A Questão de Pesquisa 1 (QP1) é composta pelas duas subquestões abaixo:

SQ1.1: Quais tipos de extensões ou adaptações à notação BPMN são propostos? (Foco na natureza técnica: metamodelos, perfis, anotações).

SQ1.2: Quais aspectos da LGPD e/ou GDPR são cobertos pelas propostas? (Foco em conceitos como Consentimento, Anonimização e Direitos do Titular).

A Questão de Pesquisa 2 (QP2) por sua vez, é composta pela subquestão abaixo:

SQ2.1: Qual é o nível de maturidade das propostas? (Avaliação em particular das propostas levantadas).

A estratégia de busca foi desenhada para maximizar a abrangência dentro do escopo de Engenharia de Software e Sistemas de Informação. A string de busca foi construída utilizando operadores booleanos (OR, AND) unindo três eixos: Notação (BPMN), Domínio (Privacidade/Proteção de Dados) e Contribuição Técnica (Extensão/Metamodelo/Requisitos).

A *string* final aplicada foi a seguinte:

(TITLE-ABS-KEY ("BPMN"OR "Business Process Model"OR "Business Process Modeling") AND ("Privacy"OR "Data Protection"OR "LGPD"OR "GDPR"OR "Privacy-by-design"OR "Data Regulation") AND ("Extension"OR "Metamodel"OR "Profile"OR "Annotation"OR "DSL"OR "Model-driven"OR "Requirements Engineering"))*

Para garantir que apenas estudos com rigor técnico e relevância temática fossem analisados, ou seja, com o universo do BPMN em conjunto com as regulamentações de proteção de dados, seja a GDPR ou a LGPD, aplicaram-se critérios rigorosos de seleção em que o Critério de Inclusão esteja satisfeito e que

nenhum Critério de Exclusão esteja atingido para que um estudo seja considerado elegível para seleção:

Como Critério de Inclusão (IC) segue o **IC1 (Correspondencia às questões de Pesquisa):** Estudos que respondam ao menos uma das questões de pesquisa. Como Critérios de Exclusão (EC)são aplicados os seguintes: **EC1 (Obsolescência Temporal):** Estudos publicados antes de 2016 (ano de aprovação da GDPR); **EC2 (Indisponibilidade):** Estudos com acesso indisponível na íntegra; **EC3 (relevância acadêmica insuficiente):** Estudos com menos de 4 páginas; **EC4 (incompatibilidade à pesquisa):** Estudos que não respondam ao menos uma das questões de pesquisa; **EC5 (Estudos não científicos):** Estudos que sejam prefácio, livros, capítulo de livros, resumos, pôsteres, painel, palestras, keynotes, tutoriais, editoriais ou demonstrações.

A busca foi realizada nos bancos de dados SCOPUS, IEEE, ACM Digital Library, Engeneering Ville Compedex, ISE Web of Science e Google Scholar seguindo o fluxo PRISMA, garantindo transparência desde a identificação inicial até a seleção final dos estudos via leitura do inteiro teor e revisão qualitativa por análise temática, resultando na inclusão do total de 18 estudos para este Mapeamento Sistemático da Literatura, consoante a Figura 1:

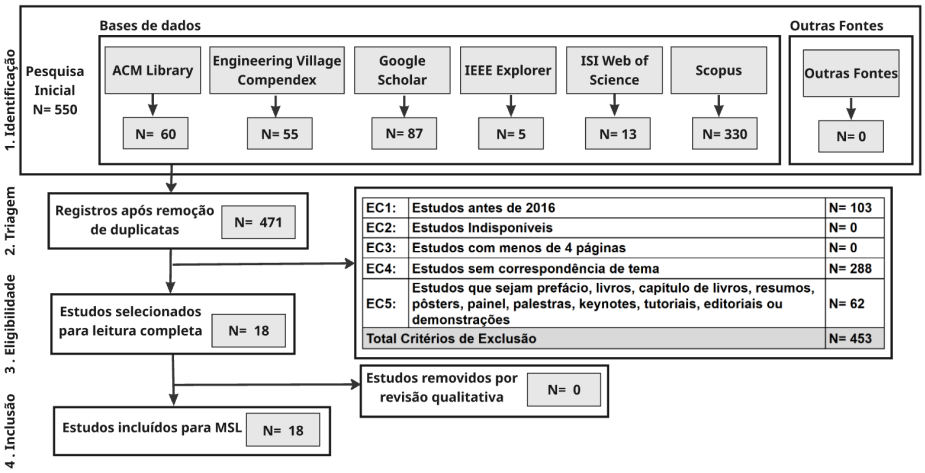

Figura 1. Fluxo Prisma utilizado neste estudo

A fase de extração foi guiada pelo processo de *Keywording* proposto por Petersen et al. (2008)[16], no qual os conceitos-chave de cada artigo são mapeados para categorias pré-definidas. O esquema de classificação adotado fundamenta-se nas seguintes cinco facetas: **1. Natureza da Extensão -** Classifica a intervenção técnica (Metamodelo, Perfil UML, Anotação Visual, DSL ou *Framework*); **2. Cobertura de Requisitos -** Mapeia quais "dores"regulatórias são tratadas

(Consentimento, Direitos do Titular, Minimização, etc.); **3. Tipo de Pesquisa -** Baseado na taxonomia de Wieringa et al. (2006)[21], classifica os estudos em Pesquisa de Avaliação, Validação, Proposta de Solução ou Artigo Conceitual; **4. Tipo de Validação -** Identifica o rigor da prova de conceito (Estudo de Caso, Experimento ou Exemplo Ilustrativo) e; **5. Contexto Legal -** Identifica se o foco é GDPR, LGPD ou uma abordagem agnóstica.

Esquema de Classificação: A fase de classificação é o processo pelo qual os estudos primários são agrupados em facetas que representam as dimensões de interesse da pesquisa. Adotou-se o método de *Keywording* proposto por Petersen et al. (2008)[16], que consiste em: (i) leitura dos resumos para identificar conceitos centrais, (ii) combinação de palavras-chave para criar categorias e (iii) refinamento das categorias mediante a leitura do texto completo.

O esquema resultante foi estruturado em categorias fundamentais, desenhadas para responder às questões de pesquisa (QPs) estabelecidas no protocolo. Cabe informar que alguns estudos não estavam disponíveis para análise, devido a dificuldade de acionar os autores durante o prazo do estudo.

Natureza da Extensão e Contribuição Técnica: Esta categoria classifica o artefato técnico proposto pelo estudo, permitindo mensurar o rigor da modificação na notação BPMN. As categorias são: **1. Perfil BPMN:** Adaptações que utilizam mecanismos de extensão da BPMN, como estereótipos e *tagged values*; **2. Anotações Visuais:** Propostas que introduzem marcadores gráficos ou ícones sem alterar a semântica de execução do modelo; **3. Linguagem Específica de Domínio (DSL):** Criação de variações textuais ou gráficas baseadas no BPMN para propósitos específicos; **4. Extensão de Metamodelo:** Estudos que alteram a estrutura lógica (classes e atributos) do padrão BPMN 2.0 e; **5. *Framework*/Processo:** Estudos que propõem métodos de uso da notação sem alterar seus elementos nativos.

Cobertura de Requisitos de Privacidade: Esta categoria mapeia a aderência das propostas aos pilares da LGPD e GDPR. A classificação considera se o estudo provê mecanismos para a **Gestão de Consentimento:** Autorização expressa do titular. **Anonimização/Pseudonimização:** Técnicas de descaracterização de dados pessoais. **Direitos do Titular:** Implementação de fluxos para acesso, retificação ou exclusão de dados. **Retenção e Descarte:** Definição de ciclos de vida e prazos de guarda de dados. **Segurança da Informação:** Garantia de integridade e confidencialidade no fluxo do processo. Para avaliar a maturidade científica da área, utilizou-se a taxonomia de Wieringa et al. (2006)[21], conforme recomendado por Petersen[16]

4 Resultados e Mapeamento

Esta seção apresenta a síntese dos dados extraídos dos estudos selecionados, correlacionando-os com as Questões de Pesquisa (QPs). A análise permite visualizar não apenas a frequência das publicações, mas a maturidade técnica das soluções que buscam integrar a notação BPMN aos requisitos de privacidade (Tabela 1 e Tabela 2).

Tabela 1. Natureza da Extensão / Cobertura (LGPD/GDPR)

Estudo	Categoria 1: Natureza da Extensão					Categoria 2: Cobertura LGPD/GDPR				
	Perfil BPMN	Anotação Visual	DSL	Metamodelo	Framework	Consentimento	Anonimização	Direitos Titular	Retenção	Segurança
01	Sim	Não	Não	Não	Sim	Sim	Não	Sim	Sim	Sim
02	Sim	Não	Não	Não	Sim	Sim	Não	Sim	Sim	Sim
03	Sim	Não	Sim	Não	Sim	Sim	Não	Não	Não	Não
04	Sim	Não	Não	Não	Sim	Sim	Não	Sim	Sim	Sim
05	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
06	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
07	Sim	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim
08	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Sim
10	Sim	Não	Não	Não	Sim	Não	Não	Não	Sim	Sim
11	Sim	Não	Não	Não	Sim	Não	Não	Não	Sim	Sim
12	Sim	Não	Não	Não	Sim	Sim	Não	Sim	Sim	Sim
13	Não	Não	Não	Não	Não	Sim	Sim	Sim	Sim	Sim
14	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
17	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim
18	Sim	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim
20	Sim	Não	Sim	Não	Sim	Não	Sim	Não	Não	Sim
22	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Não	Sim
23	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim

Tabela 2. Tipos de Pesquisa/ Validação/ Contexto Geográfico-Legal

Estudo	Categoria 3: Tipo de Pesquisa				Categoria 4: Tipo de Validação				Categoria 5: Contexto		
	Avaliação	Validação	Proposta de Solução	Conceitual	Estudo de Caso	Experimento	Exemplo Ilustrativo	Nenhuma	Brasil (LGPD)	Europa (GDPR)	Global/Agnóstico
01	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não	Sim	Sim
02	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Sim
03	Sim	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Não
04	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Não
05	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Não
06	Não	Sim	Sim	Sim	Não	Não	Sim	Não	Não	Sim	Sim
07	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não	Sim	Não
08	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Não
10	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Sim
11	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Sim
12	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Sim
13	Sim	Sim	Não	Sim	Não	Não	Não	Sim	Não	Sim	Não
14	Sim	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Não
17	Não	Sim	Sim	Sim	Sim	Não	Sim	Não	Não	Sim	Não
18	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não	Sim	Sim
20	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não	Sim	Sim
22	Não	Sim	Não	Não	Não	Não	Sim	Não	Não	Sim	Sim
23	Não	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não	Sim	Sim

A análise cronológica dos estudos (2018-2026) revela um interesse crescente e sustentado após a plena vigência do GDPR em 2018. Observa-se que a litera-

tura amadureceu de discussões conceituais iniciais para propostas de *frameworks* complexos. Embora o contexto europeu (GDPR) tenha sido o precursor, com contribuições seminais de Pullonen et al. (2019)[17] e Agostinelli et al. (2019)[2], nota-se um avanço significativo na literatura brasileira com o método LGPD4BP [4], focado nas especificidades da LGPD. Em Irina,et al. (2024)[13] o estudo mapeia as intervenções do GDPR nas quatro fases do ciclo de vida BPM: **Concepção:** Integração de normas by design em modelos gráficos. **Configuração:** Implementação de políticas em sistemas BPMS e interfaces técnicas. **Execução:** Monitoramento ativo para garantir que instâncias sigam as restrições de privacidade. **Análise:** Uso de Mineração de Processos (Process Mining) e logs para auditar e avaliar a conformidade a posteriori. O estudo chama a atenção para a necessidade de analisar com maior profundidade o impacto da regulamentação sobre a engenharia de requisitos e a infraestrutura impactada pelo GDPR aplicada aos processos, bem como as respectivas questões de fluxo e armazenamento de dados.

Frameworks e Processos: Estudos como Agostinelli et al. (2026)[1] e Capodieci et al. (2025)[10] focam em metodologias de uso de padrões de design (design patterns) para conformidade, sem necessariamente alterar o metamodelo da OMG. Nos estudos de Windrich et al. [22] [23], destacam-se as aplicações tanto do método de cores Padrão Semáforo bem como a regra do Pior Cenário para o armazenamento de dados, por meio da tradução de requisitos complexos do GDPR em gatilhos visuais intuitivos.

Extensões de Metamodelo e PE-BPMN: A proposta de *Privacy-enhanced BPMN* (PE-BPMN) de Pullonen et al. (2019)[17] destaca-se como uma das contribuições mais rigorosas, introduzindo semântica para análise de fluxos de informação e tecnologias de aumento de privacidade (*Privacy Enhancing Technologies* - PETs).

Abordagens baseadas em Ontologias: O trabalho de Bartolini et al. (2019)[6] introduz uma camada semântica via ontologias, permitindo que o modelo BPMN seja verificado contra as provisões legais de forma computacional.

Quanto a cobertura de requisitos regulatórios da LGPD/GDPR, ao analisar quais são efetivamente abordados, observa-se uma cobertura heterogênea em destaque, **Segurança (Integridade/Confidencialidade):** Presente em quase 90% dos estudos, sendo o requisito mais consolidado; **Consentimento e Direitos do Titular:** Abordados majoritariamente em propostas mais recentes por exemplo, a LGPD4BP, refletindo a necessidade de modelar pontos de interação direta com o titular do dado; **Minimização de Dados:** Identificada como uma lacuna técnica em muitos estudos, mas central no trabalho de Ramadan et al. (2020)[18], que propõe a detecção de conflitos entre segurança e minimização de dados através de anti-padrões e; **Retenção e Descarte:** Ainda subrepresentados na modelagem gráfica, aparecendo frequentemente apenas como anotações textuais ou metadados de framework. Utilizando a taxonomia de Wieringa et al. (2006)[21], os resultados indicam que a área encontra-se em fase de Pesquisa de Validação (42%) e Proposta de Solução (33%). A maioria dos estudos utiliza exemplos ilustrativos[11] para demonstrar a viabilidade das extensões.

No entanto, há uma escassez de estudos de caso em ambientes organizacionais reais de larga escala, o que aponta para uma oportunidade de pesquisas futuras que validem a eficácia dessas notações sob a ótica de modeladores de processos reais. A análise cruzada revela que estudos focados na LGPD tendem a ser mais prescritivos (manuais e métodos de avaliação como o LGPD4BP)[4], enquanto estudos focados no GDPR têm explorado caminhos mais formais, como a verificação baseada em modelos (*model-based verification*) proposta por Belluccini et al. (2025)[7], utilizando linguagens formais como mCRL2 para provar a conformidade de processos colaborativos.

5 Discussão

Um dos achados mais significativos deste mapeamento é a predominância de extensões voltadas à segurança técnica (integridade e confidencialidade) em detrimento de princípios de privacidade mais abstratos. Conforme discutido por Ramadan et al. (2020)[18], existe um conflito inerente entre os requisitos de segurança e a minimização de dados. Enquanto a segurança muitas vezes exige logs detalhados e autenticação forte (gerando mais dados), a minimização exige a redução da coleta ao estritamente necessário. Outro ponto levantado no estudo secundário de Irina[13] chama a atenção para trabalhos futuros nos temas de transferências de dados a terceiros.

A literatura analisada sugere que o uso de antipadrões, como proposto no *framework* de detecção de conflitos de Ramadan et al.[18], é uma das abordagens mais promissoras para resolver esse impasse na fase de design. Contudo, a integração desses mecanismos em ferramentas CASE (*Computer-Aided Software Engineering*) comerciais ainda é incipiente.

Também observamos uma diferença qualitativa na maturidade regulatória entre a GDPR e a LGPD, dependendo do contexto legal. As pesquisas focadas no GDPR [17][7] tendem a explorar a verificação formal e a semântica profunda, tratando a privacidade como um problema de fluxo de informação verificável matematicamente.

Em contrapartida, as pesquisas voltadas à LGPD, como o método LGPD4BP [4], apresentam uma orientação mais metodológica e prescritiva, focada em auxiliar analistas a avaliar a conformidade de modelos existentes através de checklists e catálogos de requisitos. Essa tendência indica que, no Brasil, o foco da pesquisa em Sistemas de Informação ainda está na transição da conformidade legal para a técnica, enquanto na Europa a pesquisa já se move para a automação da verificação de conformidade.

5.1 Resposta às Questões de Pesquisa

As evidências coletadas permitiram responder de forma conclusiva às questões norteadoras deste estudo: A análise sistemática dos estudos selecionados permitiu consolidar a resposta à QP1. Esta resposta é fundamentada na convergência dos achados técnicos (SQ1.1) e regulatórios (SQ1.2):

Resposta à SQ1.1 (Natureza das Extensões e Adaptações): A literatura técnica revela a real iniciativa de desenvolvimento de mecanismos para adaptar o BPMN à privacidade. Identificou-se uma predominância de *Frameworks* Metodológicos (ex. LGPD4BP e propostas de Agostinelli et al.[2]), presentes em aproximadamente 70% da amostra, que guiam a aplicação de padrões sem alterar o núcleo da notação. Complementarmente, abordagens de alto rigor semântico utilizam Extensões de Metamodelo e Linguagens Específicas de Domínio (DSL), como o método PE-BPMN, para permitir análises formais de fluxos de dados e tecnologias de aumento de privacidade (PETs). O uso de Perfis BPMN (*Profiles*) e Anotações Visuais também é comum para prover suporte gráfico de baixo acoplamento.

Resposta à SQ1.2 (Cobertura de Requisitos da LGPD/GDPR): A cobertura dos requisitos regulatórios é heterogênea entre os estudos. A Segurança da Informação (integridade e confidencialidade) é o pilar mais consolidado, sendo abordado por quase a totalidade das extensões analisadas. A Gestão de Consentimento e os Direitos do Titular (acesso e retificação) ganharam protagonismo em *frameworks* mais recentes, refletindo a necessidade de modelar interações diretas com o titular. Contudo, identificou-se uma lacuna em requisitos como Retenção e Descarte de Dados e Anonimização, que muitas vezes são tratados de forma periférica ou apenas como metadados, sem uma representação visual padronizada no fluxo do processo.

Síntese Final da QP1: Em suma, a literatura propõe a integração BPMN/Privacidade através de um ecossistema híbrido de modelagem. A integração não ocorre apenas no nível sintático (novos ícones), mas sim através de uma camada de Engenharia de Requisitos, onde o BPMN atua como o artefato central para unir a conformidade jurídica à implementação técnica. A síntese dos resultados indica que a tendência atual é a transição de simples anotações visuais para *frameworks* que suportam a verificação automatizada de conformidade e a aplicação de design patterns orientados à privacidade, operacionalizando o princípio de *Privacy by Design* desde a concepção dos processos organizacionais. No entanto, observou-se que a integração ainda é parcial: requisitos de segurança e consentimento são bem atendidos, enquanto a retenção de dados e o direito à portabilidade permanecem sub-representados na modelagem gráfica.

Resposta à QP2 Evolução e maturidade dos estudos ao longo do tempo: Confirmou-se uma correlação direta entre o marco regulatório e a produção científica. O pico de publicações iniciou-se em 2019, logo após a vigência plena do GDPR. Geograficamente a Europa lidera as propostas de verificação formal, enquanto o Brasil apresenta um aparente crescimento com métodos focados na avaliação de conformidade sob a égide da LGPD. Em resposta a subquestão SQ2.1, a frequência de publicações evoluiu de uma preocupação genérica com segurança para uma especialização em conformidade regulatória (compliance by design), consolidando-se como um campo de pesquisa robusto e tecnicamente orientado na comunidade de BPM[13].

5.2 Lacunas Identificadas e Oportunidades de Pesquisa

A análise sistemática revelou três lacunas principais que representam oportunidades para trabalhos futuros: **Modelagem de Direitos do Titular:** Embora o consentimento seja abordado, fluxos complexos como a portabilidade de dados e o direito à explicação em decisões automatizadas (conforme exigido pela LGPD/GDPR) raramente possuem representação gráfica padronizada em BPMN. **Ciclo de Vida: Retenção e Descarte:** A "morte"do dado é negligenciada. Faltam extensões que modelem de forma clara o acionamento de subprocessos de descarte após o término da finalidade de tratamento. **Avaliação em Larga Escala:** A predominância de "Exemplos Ilustrativos"aponta que as extensões propostas precisam ser testadas em ecossistemas de software reais, onde a complexidade dos processos pode tornar as extensões visuais poluídas e de difícil manutenção.

5.3 Ameaças à Validade

Seguindo as diretrizes de Petersen et al. (2008)[16] e Kitchenham e Charters (2007)[15], foram considerados os seguintes fatores que poderiam comprometer o rigor deste MSL: **Validade de Construto:** Para mitigar a seleção inadequada de termos, a *string* de busca foi testada iterativamente. No entanto, termos específicos de extensões proprietárias podem não ter sido capturados. **Validade Externa (Generalização):** O foco em BPMN excluiu outras notações como CMMN ou DMN. Assim, os resultados são generalizáveis apenas para o domínio de modelagem de processos e não para toda a modelagem de negócios. **Confiabilidade (*Reliability*):** O processo de extração foi guiado por uma planilha padronizada. Para minimizar viés subjetivo, os critérios de inclusão e exclusão foram validados por pares (orientador e pesquisador).

6 Conclusão

Este Mapeamento Sistemático da Literatura (MSL) investigou o estado da arte das integrações entre a notação BPMN e os requisitos das regulamentações de proteção de dados pessoais, especificamente o GDPR e a LGPD. Através da análise rigorosa de estudos publicados entre 2016 e 2026, foi possível estruturar o campo e identificar as principais tendências e desafios técnicos.

A principal contribuição deste MSL é o fornecimento de um esquema de classificação que categoriza as extensões BPMN por sua natureza técnica e cobertura legal. Para pesquisadores este trabalho mapeia as lacunas ontológicas da área; para profissionais (DPOs e analistas de processos), oferece um catálogo de soluções existentes para implementar a *Privacy by Design* em fluxos de negócio. Destaca-se ainda, a identificação do conflito entre "Segurança"e "Minimização de Dados"como um ponto crítico de decisão que exige maior suporte de ferramentas automatizadas. Embora o protocolo de Kitchenham e Charters (2007)[15] tenha sido rigorosamente seguido, a rápida evolução das leis de proteção de dados em

outras jurisdições pode limitar a generalização destes achados para além do eixo Europa-Brasil.

A modelagem de processos via BPMN demonstrou ser uma linguagem capaz de absorver a complexidade regulatória, mas sua eficácia plena depende de uma padronização mais profunda que une a visão jurídica à semântica técnica da Engenharia de Software. Em trabalhos futuros, planejamos o desenvolvimento de extensões visuais específicas para o ciclo de vida do dado e a integração com Inteligência Artificial, explorando como modelos BPMN podem capturar requisitos de transparência e explicabilidade em processos de decisão automatizada. Pretende-se aplicar essa proposta para validação em cenários reais.

Referências

1. Agostinelli, S., De Luzi, F., Maggi, F. M., Marrella, A., and Volpi, A. (2026). *Design patterns for GDPR-aware process modeling in BPMN.* Information Systems, 137, 102646. Elsevier.
2. Agostinelli, S., Maggi, F.M., Marrella, A., Sapio, F. (2019). *Achieving GDPR compliance of BPMN process models.* Lecture Notes in Business Information Processing, 350, pages 10–22. Springer.
3. Amantea, I.A., Robaldo, L., Sulis, E., Governatori, G., & Boella, G. (2022). Business Process Modelling in Healthcare and Compliance Management: A Logical Framework. FLAP, 9, 1131-1154.
4. Araújo, E., Vilela, J., Silva, C., Alves, C. (2021). *Are My Business Process Models Compliant with LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes.* ACM International Conference, pages 21–30. ACM.
5. Bakhtina, M., Matulevicius, R. & Seeba, M. (2023). Tool-supported method for privacy analysis of a business process model.. J. Inf. Secur. Appl., 76, 103525.
6. Bartolini, C., Calabro, A., Marchetti, E. (2019). *Enhancing Business Process Modelling with Data Protection Compliance: An Ontology-based Proposal.* International Conference on Information Systems Security and Privacy, pages 421–428.
7. Belluccini, S., De Nicola, R., Dumas, M., ... Re, B., Tiezzi, F. (2025). *Model-based verification of data protection mechanisms in collaborative business processes*, Software and Systems Modeling, pages 489–521. SSM.
8. Belluccini, S., De Nicola, R., Dumas, M., ... Re, B., Tiezzi, F. (2020). *Verification of privacy-enhanced collaborations.* Proceedings 2020 IEEE ACM 8th International Conference on Formal Methods in Software Engineering Formalise, pages 141–152.
9. BRASIL. (2018) Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais* Disponível em: www.planalto.gov.br. Acesso em: 26 jan. 2026.
10. Capodieci, A., Mainetti, L., Lisi, S., Matino, S., Ugirashebuja, M. (2025). *Enhancing privacy awareness through a novel BPMN based methodology*, Multimedia Tools and Applications, 84(20), pp. 23163–23185. Springer.
11. Capodieci, A., De Carolis, M., Lisi, S., ... Paiano, R., Ugirashebuj, M. (2023). *BPMN-Enabled Data Protection and GDPR Compliance.* Ceur Workshop Proceedings, page 3408. CEUR-WS.org.
12. Capodieci, A., & Mainetti, L. (2019). *Business process awareness to support GDPR compliance.* Proceedings of the 9th International Conference on Information Systems and Technologies.

13. Irina, R., Rebecca, D., & Sothiya, J. (2024). *Conformité au RGPD dans les Pratiques de Gestion des Processus Métier : Revue Systématique de la Littérature.* Revue ouverte d'ingénierie des systèmes d'information.
14. Kiesel, J., & Grünewald, E. (2024). *Extending Business Process Management for Regulatory Transparency.* International Conference on Business Process Management.
15. Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering.*
16. Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008, June). *Systematic mapping studies in software engineering. In 12th international conference on evaluation and assessment in software engineering (EASE).* BCS Learning & Development.
17. Pullonen, P., Matulevičius, R., and Toots, A. (2019). *Privacy-enhanced BPMN: enabling privacy assessments in business processes. Software and Systems Modeling,*, pages 3235–3264. SSM.
18. Ramadan, Q., Strüber, D., Salnitri, M., ... Riediger, V., Staab, S. (2020). *A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization, and fairness requirements.* Software and Systems Modeling, 21(5), pages 1191–1227. SSM.
19. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *Regulamento Geral sobre a Proteção de Dados (GDPR).* Jornal Oficial da União Europeia, Bruxelas, 4 maio 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 13 fev. 2026.
20. Varela-Vaca, Á.J., Gómez-López, M.T., Morales Zamora, Y., M. Gasca, R. (2025). *Business process models and simulation to enable GDPR compliance* International Journal of Information Security, 24(1), page 41. Springer.
21. Wieringa, R., Maiden, N.A., Mead, N.R., & Rolland, C. (2005). Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements Engineering, 11, 102-107.
22. Windrich, Melanie & Hilge, Paul & Speck, Andreas & Gruschka, Nils. (2026). *Labeling of Data Protection Properties in Business Process Models.* 10.1007/978-3-032-04878-3_12.
23. Windrich, M., Speck, A., & Gruschka, N. (2021). *Representing Data Protection Aspects in Process Models by Coloring.* Annual Privacy Forum.