Uma abordagem baseada no Catálogo de Requisitos Não Funcionais para conformidade à LGPD

Henrique Prado de Sá Sousa[1], Eduardo Kinder Almentero[2], Tadeu Moreira de Classe[1], Rodrigo Juliao dos Santos[2], and Julio Cesar Sampaio do Prado Leite[4]

[1] Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, Brasil
[2] Universidade Federal Rural do Rio de Janeiro, Seropédica, Brasil
[3] Ordem dos Advogados do Brasil do Rio de Janeiro, Rio de Janeiro, Brasil
[4] Universidade Federal da Bahia, Salvador, Brasil
hsousa@uniriotec.br, ekalmentero@gmail.com,
tadeu.classe@uniriotec.br, juliao.job@gmail.com,
julioleite@ufba.br

Abstract. A Lei Geral de Proteção de Dados (LGPD) foi criada para garantir que direitos fundamentais, como a privacidade, fossem respeitados por organizações que realizam tratamento de dados. O texto da Lei define uma série de restrições que devem ser consideradas por pessoas ou organizações que realizam o tratamento de dados, inclusive nos meios digitais. Quando o tratamento é realizado através de sistemas computacionais, estas restrições têm impacto no software que realiza o tratamento, uma vez que este é o responsável por implementar as ações relacionadas ao tratamento dos dados. Em outras palavras, o software deve cumprir requisitos específicos para implementar as restrições estabelecidas pela Lei. Entretanto, a LGPD é alvo de muitas discussões e há uma série de dúvidas relacionadas a sua implementação. Para auxiliar o entendimento da Lei, e, consequentemente, sua implementação, apresentamos uma análise sob a ótica da engenharia de requisitos, orientado pela construção de catálogos de requisitos não funcionais, que são mencionados de forma recorrente no texto da Lei.

Keywords: LGPD, RNF, Requisitos de Qualidade, Catálogo de Requisitos Não-Funcionais (RNFs), Requisitos legais.

1. Introdução

Segundo o artigo 5º, inciso X, da Constituição Federal, “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. Uma vez que nas últimas décadas muitos dados pessoais migraram do ambiente físico para o virtual, o debate sobre privacidade no âmbito de sistemas computacionais (software) se tornou crítico. Neste contexto, surgiram diversos regulamentos e leis, como a GDPR [14] e a LGPD [13], buscando definir critérios para a garantia do direito à privacidade no uso de dados pessoais, seja no ambiente físico como no ambiente virtual.

Sob a perspectiva social, a legislação sobre este tema é muito relevante, considerando os inúmeros casos de vazamento de informações pessoais e prejuízos múltiplos

Proceedings of the 26th Workshop on Requirements Engineering (WER23), August 15-17, 2023, Porto Alegre, RS, Brazil.
DOI: 10.29327/1298356.26-8

sofridos por pessoas comuns devido ao uso indevido de suas informações [28]. Esses eventos se intensificaram quando a internet passou a ser comumente utilizada com objetivos diversos. A presença de software nos dispositivos pessoais, como celulares, relógios e dispositivos inteligentes, permitiu o acesso a informações que, muitas vezes, os usuários não sabem que são coletadas [27].

As organizações se beneficiam dessas coletas para formar perfis visando oferecer seus produtos e serviços de forma personalizada. A informação sobre as pessoas possui grande valor de comércio, sendo inclusive analisadas em profusão para gerar dados relevantes para decisões estratégicas [25]. Não obstante, a coleta, venda/compartilhamento dessas informações pode ser lucrativa, no entanto, há de questionar a legalidade dessas transações [26].

O benefício do controle de informações se mostrou unilateral, com o agravante de ter um prejuízo potencial aos consumidores, consolidando o cenário que denota relevância substancial da LGPD.

No entanto, após a vigência desta lei, as condições de uso de informações de terceiros foram profundamente alteradas, e as organizações (daqui em diante podem ser referenciadas apenas como "**controlador(as/es)**" dos dados, conforme a LGPD) passaram a ter grande responsabilidade legal. A manipulação inadequada de dados pessoais pode ser configurada como crime, passível de multas e outras penalidades. Adicionalmente, o controlador se encontra responsável pelos riscos de eventos diversos (de segurança, por exemplo) e seus desdobramentos.

Por exemplo, o Art. 42º da LGPD dispõem sobre a responsabilidade penal do controlador: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

Como agravante, em disputas judiciais, considerando a organização controladora como a parte ré, caberá a ela o dever de gerar provas que demonstre a sua conformidade legal, exercendo o direito ao contraditório. Porém há outras áreas do Direito que reforçam essa possibilidade.

Por exemplo, no Código de Processo Civil (CPC), o Art. 373. (...) §1º, no item II define que o ônus da prova incumbe: "ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor". O direito do titular dos dados é amparado pela LGPD no Art.17 que define: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei". O mesmo artigo 373 permite ao magistrado decidir de forma fundamentada sobre o ônus da prova à parte que possui melhor condição de produção de prova.

Outro exemplo semelhante, presente no Código de Defesa do Consumidor (CDC), no Art. 6º, item VIII, é um direito básico do consumidor: "a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências".

A própria LGPD apresenta um caso de ônus da prova, no § 2º do Art. 8º: "Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei". E, similar ao Art. 373 do CPC, o Art. 42 § 2º, define que: O juiz,

no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Diante de tantas exigências legais, as organizações controladoras enfrentam o desafio de ajustar a sua estrutura para adequar-se às leis. Adicionalmente, quando se observa os casos em que há presença de tecnologias no processo de tratamento de dados, há especialistas da área de TI que também apresentam suas dificuldades no entendimento de como implementar a LGPD. Isso se apresenta especialmente porque esta lei foi definida em grande parte através da referência a quesitos qualitativos, gerando dúvidas no momento da definição de operacionalizações em sistemas de software [7, 22, 24].

Considerando a necessidade de se compreender melhor a LGPD em termos de seus requisitos não funcionais (RNF), bem como a necessidade das organizações em apresentar provas de aderência com a lei, neste artigo, propomos o uso de Catálogo de Requisitos Não Funcionais (CRNF) como um recurso para a modelagem do conhecimento sobre os requisitos qualitativos da LGPD, registro do conhecimento sobre operacionalizações dos NRF e documentação dos respectivos relacionamentos de contribuição das ações definidas pelas organizações para incrementar o grau dos RNFs.

Este artigo está dividido da seguinte forma: a seção 1 é a presente introdução; na seção 2 é apresentada a fundamentação teórica que inclui os assuntos NFR *Framework*, Catálogos de RNF, e uma busca simplificada realizada na literatura para identificar trabalhos relacionados com o tema deste artigo; na sessão 3 apresentamos a proposta de uso dos catálogos de RNFs para apoiar a LGPD; na sessão 4 são apresentadas as conclusões.

2. Fundamentação teórica

2.1 NFR *Framework*

Os requisitos de software são especificados a partir do conhecimento adquirido sobre o domínio, através de processos de elicitação de requisitos [16]. Durante a elicitação, as fontes de informação de conhecimento devem ser mapeadas. No caso em questão, o texto da Lei nº 13.709/2018 é a principal fonte de conhecimento. Através do entendimento do texto da Lei, são identificados requisitos descritos em nível abstrato devido às descrições apresentadas sob a perspectiva do domínio abordado, ou seja, ainda distante de uma descrição contendo aspectos técnicos do software. Essa parte é descrita na literatura da engenharia de requisitos como "*early requirements*". Posteriormente, na fase de "*late requirements*" [8], com foco restrito aos aspectos técnicos, surgem os requisitos de software devidamente especificados.

O NFR *Framework* [10] apresenta uma proposta para a modelagem de requisitos de qualidade que parte de um nível abstrato e, através de sucessivos refinamentos e correlações, é possível alcançar o nível em que se mapeiam possíveis operacionalizações para as qualidades, mantendo um rastro explícito entre os elementos.

O modelo proposto pelo NFR *Framework* para registrar estes conhecimentos é o *Softgoal Interdependecy Graph* (SIG). Ele possui como uma de suas características a

representação dos RNFs como "*softgoals*" (metas flexíveis), os quais representam objetivos que não possuem uma definição clara e/ou critérios bem definidos de satisfação [10]. Essa natureza qualitativa é a principal característica de um RNF.

O NFR *Framework* define que uma meta flexível não pode ser considerada "satisfeita" já que não há entendimento universal sobre a sua satisfação, e propõem o termo "satisfatório" (termo original *satisficed*, definido originalmente em [3]) para expressar que, sob determinada perspectiva, aquela meta flexível foi atingida "a contento".

Portanto não há efetivamente ações que, quando implementadas, garantam de forma definitiva a realização de uma meta flexível. No entanto, as ações são capazes de alterar o seu "grau", para mais ou para menos, uma vez que podem ser favoráveis ou desfavoráveis, agregando ou desagregando valor à determinada qualidade.

As características qualitativas são apontadas como uma das dificuldades existentes na hora de se especificar, implementar e avaliar uma meta flexível [7, 22]. Isso ocorre porque a definição e avaliação de determinada meta flexível está restrita ao ponto de vista do avaliador que irá mensurar a meta de acordo com premissas pessoais. Além disso, uma meta flexível pode impactar outras metas flexíveis, e operacionalizações podem causar efeitos indesejados.

O SIG auxilia no mapeamento dessas informações, e auxilia a análise detalhada das interdependências e operacionalizações. No entanto, a estrutura de um Catálogo de RNFs adiciona novos recursos ao SIG que orientam melhor a definição de operacionalizações e organização do conhecimento.

2.2 Catálogo de RNFs

O uso de catálogos com o intuito de registrar e consultar conhecimento adquirido em experiências anteriores está presente no NFR *Framework*. Neste trabalho, utilizamos uma versão de catálogo composto pelo SIG, e acrescido do uso dos padrões de RNF proposto por [2]. Os padrões utilizados são o Padrão de Questão (ver Fig. **5**), que representa o detalhamento dos RNFs em termos de perguntas que orientam a definição de operacionalizações; e o Padrão de Alternativa (Figura 6), que descreve os diferentes meios de satisfazer a contento as metas flexíveis e seus efeitos colaterais.

Esses três elementos compõem o catálogo que se organiza no formato *Goal-Question-Operationalization* (GQO), gerando o modelo conforme ilustra a Figura 1.

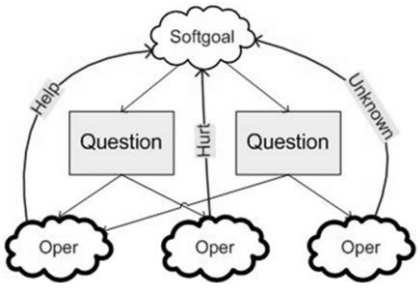

Fig. 1. Padrão GQO [1]

Catálogos contendo operacionalizações podem ser ferramentas muito úteis na construção e avaliação de sistemas relativos a um determinado softgoal, bem como no esclarecimento possíveis sinergias e conflitos entre eles. Ao representar conhecimento usando uma estrutura padronizada, os padrões facilitam a localização, entendimento e seleção de operacionalizações em um determinado domínio.

Alguns exemplos de catálogos SIG de softgoals RNF são: segurança, precisão, desempenho [9], usabilidade [10], acessibilidade [11] e privacidade [12]

2.3 Consulta à Literatura

Este trabalho se restringe a análise da LGPD sob uma ótica da engenharia de requisitos, mais especificamente sob o assunto de requisitos não funcionais e uso de catálogos. Neste primeiro passo do trabalho, a intenção foi identificar artigos que abordem o tópico de requisitos não funcionais na LGPD. Para isso, definimos a seguinte *string* de busca, em inglês: *LGPD AND (non functional OR NFR OR quality)*; e em português: *LGPD AND (não funcional OR RNF OR qualidade)*.

A pesquisa foi aplicada nas bases SOL, IEEE, ACM, *Science Direct*, bem como no *google scholar*, especificando as publicações com origem no WER[1]. Foram consideradas as bases de anais de eventos, periódicos e livros, nos idiomas português e inglês. Não foi definido um período específico das publicações. Após as buscas, selecionamos apenas os artigos que apresentassem as palavras-chave no *abstract*. No caso do WER encontramos mais alguns artigos relevantes utilizando a busca interna do sítio *WERpapers* com *a string* LGPD. O resultado é apresentado na Tabela 1.

Tabela 1. Artigos resultantes da busca

ACM	**[24]**	*Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal*	EN
	-	*Nenhum*	PT
Science Direct	**x**	*Developmental outcomes of young deaf children and the self-perceived parental role of their hearing mothers*	EN
	-	*Nenhum*	PT
SOL	**-**	*Nenhum*	EN
	[17]	LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados	PT
	[18]	*Information Security and LGPD Applied in Software Development*	PT
	[19]	Sigilo médico-paciente sobre criptografia ponta-a-ponta	PT
	[20]	*A Blockchain-Based Architecture for Auditing Compliance with Data Protection Regulations*	PT
	[21]	*The Brazilian Data at Risk in the Age of AI?*	PT
IEEE	**-**	*Nenhum*	EN
	-	*Nenhum*	PT
WER	**[7]**	Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso.	PT

[1] https://scholar.google.com/scholar?as_q=&as_publication=wer

	[8]	Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil	PT
	[9]	Um *survey* com especialistas como validação de elementos para composição de uma ontologia para Sistemas AAL (*Ambient Assisted Living*)	PT
	[10]	Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário	PT
	-	*Nenhum*	EN

O artigo "*Developmental outcomes of young deaf children and the self-perceived parental role of their hearing mothers*" foi excluído. O termo LGPD se refere a "*Low Global Psychomotor Development*".

Em [24] foi realizado um mapeamento sistemático da literatura (MSL) para identificar trabalhos que indicassem a existência de checklists de avaliação da aderência de sistemas computacionais à LGPD brasileira. O trabalho gerou um novo *checklist* contendo 52 itens provenientes da análise de atributos extraídos da Lei LGPD, do MSL, e de uma revisão informal de artigos de áreas complementares à computação.

Em [17], foi feito um estudo de técnicas que envolve a criptografia visando apoiar quesitos de segurança demandados pela LGPD. O trabalho discute o potencial de uso das técnicas de Anonimização, Pseudonimização, Privacidade Diferencial, *Fully Homomorphic Encryption*, *Property Preserving Encryption* e *Oblivious Random Access Memory*; conclui que, apesar destas técnicas possuírem vulnerabilidades, ainda podem ser consideradas como boas alternativas para aumentar o grau de privacidade, mantendo aderência com a Lei.

O artigo [18] se atém ao mapeamento de 42 práticas de segurança da informação para implementação em software, definidas e aplicadas pelo centro de tecnologia da IPM Sistemas Ltda, que é uma empresa operadora de informações que atua para manter aderência com a LGPD. As práticas foram classificadas em três grupos: técnico, culturais ou pessoais e jurídicas. Padrões e políticas de segurança também são referenciados.

Em [19] é proposto o uso do algoritmo *Diffie-Hellman* para apoiar o sigilo de dados utilizados na relação médico/paciente, em conjunto com uma API que permite aos pacientes o controle do acesso às suas informações. Em [20] é proposto o uso de *blockchain* como um recuso que permita auditar as operações de tratamento realizadas sobre dados pessoais. Este é um trabalho em andamento. Em [21], a aquisição da parte do governo brasileiro de um sistema de reconhecimento biométrico é discutida em termos de segurança. Os autores apresentam 10 preocupações sobre a adoção desta tecnologia, sendo uma delas, a aderência à LGPD.

O artigo [4] traz uma observação de interesse num questionário aplicado a pessoas atuando em sistema de assistência a idosos (*Ambient Assisted Living*) sobre requisitos. Foi fornecido um conjunto de requisitos, baseado numa taxonomia anteriormente publicada, onde não estava explicitada a questão privacidade. Nesse contexto, 27% dos respondentes apontaram, corretamente, a falta do requisito privacidade.

Alves e Neves [5] apontam que a implementação do requisito privacidade, tomando por base a LGPD é um desafio para os profissionais de TI. Através da aplicação de questionários numa amostra de profissionais de TI, os autores ressaltaram uma série de questões que apresentavam dificuldade. Com base nessa amostra, os autores fizeram uma primeira tentativa de criar um meta-padrão de maneira a facilitar a identificação e

a operacionalização do requisito legal. Essa meta padrão tem os seguintes atributos: ID e Nome do Padrão, Conformidade Legal (trecho da lei), Descrição legal, Objetivo de Privacidade, Ativos (dados onde se aplica), Vulnerabilidades (possíveis problemas de não proteção do dado), Solução, Consequências (informar ao usuário que o problema e tratado pelo sistema).

Em [6] se apresenta uma lista de operacionalizações para apresentação da política de privacidade de um software. A lista visa facilitar a iteração do usuário para a compreensão da política de privacidade em questão. Os elementos da lista são: "(i) Destacar informações sensíveis relacionadas ao compartilhamento de dados do usuário, (ii) Oferecer um menu de navegação guiado a tópicos ou subtópicos ou uma funcionalidade de busca alternativa, (iii) Definir uma composição hierárquica entre título, subtítulo e texto, (iv) Apresentar o significado de Políticas de Privacidade, (v) Definir seções com tópicos de títulos simples, (vi) Oferecer uma alternativa de entendimento da política por meio de mídia, (vii) Permitir interação de forma simples e fácil ao usuário sobre o assunto, (viii) Definir ícones que representam um tópico, (ix) Destacar termos que precisem de um *hiperlink* para direcionar o usuário para detalhes sobre o termo".

O artigo [7] propôs uma taxonomia de privacidade baseada na LGPD e na ISO/IEC 29100. A formação dessa proposta utilizou três etapas: identificação dos requisitos de privacidade, classificação desses requisitos, e refinamento dos requisitos. No total, foram identificados 169 requisitos que foram classificados em: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Apesar dos artigos abordarem o tema LGPD, nenhum trabalho propõem o uso de catálogos de requisitos não funcionais com os objetivos expostos neste trabalho. O tema privacidade é bastante estudado com foco na LGPD, porém **existem diversos outros RNFs presentes na legislação**.

3. Catálogo de RNFs da LGPD

Nesta seção iremos apresentar a abordagem de construção de um catálogo de requisitos não funcionais com base nas características e estrutura estabelecida na LGPD. Nossa proposta é baseada no trabalho sobre definições de padrões RNF de Supakkul et al. [2] e inclui a definição dos padrões Questão e Alternativa. A seguir apresentamos as atividades envolvidas na elaboração do catálogo sob a perspectiva de cada um destes padrões (Figura 2).

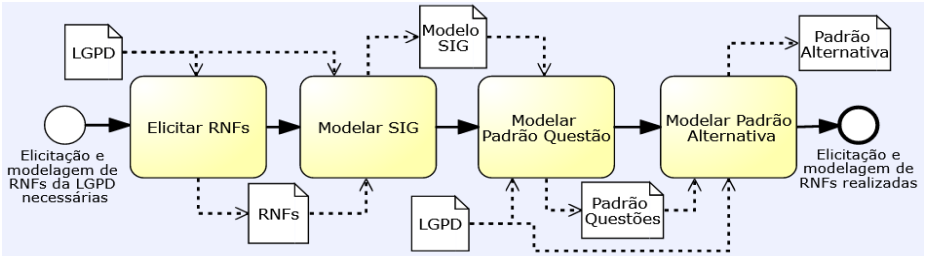

Fig. 2. Processo de construção do catálogo de RNFs da LGPD

3.1 Elicitar RNFs na LGPD

Os RNFs foram mapeados da LGPD através da interpretação textual e busca por palavras chaves [1] as quais naturalmente remetem a conceitos qualitativos e RNFs conhecidos. Ao realizarmos uma leitura preliminar buscando identificar os tipos de requisitos existentes na Lei, observamos a presença de metas-flexíveis em diferentes níveis de abstração. Alguns RNFs não devem ser implementados por software porque estão em nível abstrato de decisão. Um exemplo deste caso é a boa-fé, que, segundo a LGPD, deve ser observada no tratamento de dados pessoais. Este é um conceito ético, relacionado à conduta de acordo com os valores morais da sociedade. Esses casos podem ser operacionalizados de forma mais adequada, por exemplo, através da definição de regras, políticas e normas no nível organizacional.

Por existir grande número de RNFs na Lei, decidimos exemplificar a construção do catálogo utilizando os RNFs vinculados ao Art. 6 que enumera um conjunto de "requisitos (chamado de "princípios") para as atividades de tratamento de dados pessoais.

3.2 Modelar SIG

Para a modelagem dos requisitos não funcionais identificados na LGPD, propomos uma visão hierárquica, utilizando os mecanismos de decomposição por tipo e tópico do NFR *Framework*, conforme SIG apresentado na Figura 3.

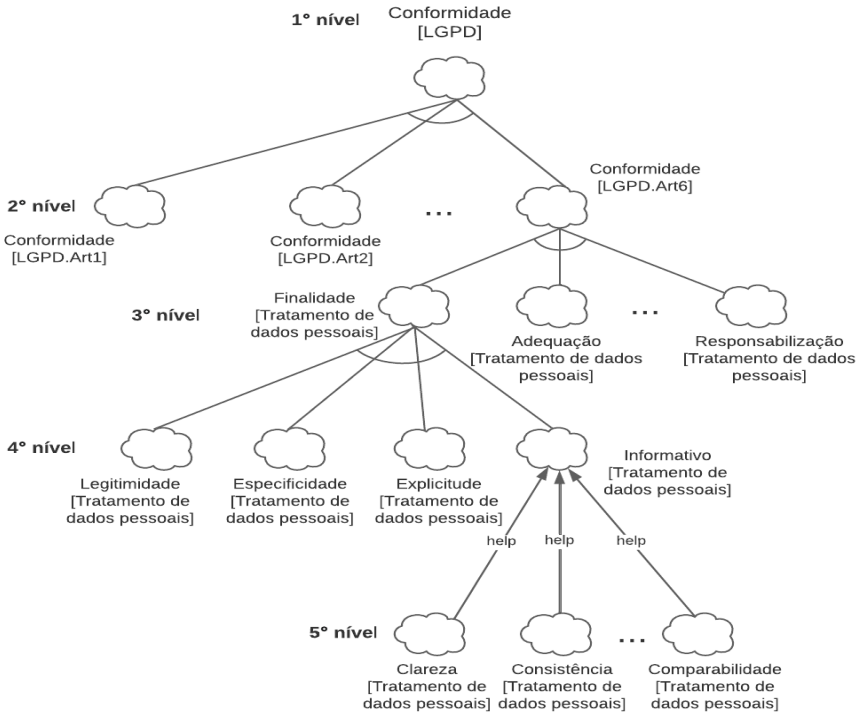

Fig. 3. Esboço de SIG da LGPD

Nesta representação, o primeiro nível é definido como a qualidade de estar em conformidade (tipo) com a LGPD (tópico). Para chegar ao segundo nível, refinamos o tópico LGPD de acordo com os artigos definidos no corpo da lei. Foi utilizada um refinamento do tipo "AND" indicando que a conformidade com todos os artigos é necessária para a conformidade com a lei. O primeiro e segundo nível exibem uma abordagem genérica, que pode ser aplicada para representação de leis em geral e, apesar de ser simples, permite a rastreabilidade com todos os elementos definidos nos níveis inferiores para cada artigo da lei. Assim, de uma perspectiva mais ampla, podemos avaliar o atendimento de cada artigo e, consequentemente, a conformidade com a lei.

O refinamento do SIG (Figura 3) a partir do terceiro nível exige a análise do texto da lei. Para exemplificar a abordagem proposta neste trabalho, selecionamos o artigo 6° da LGPD, o qual define um conjunto de princípios que devem ser seguidos para o tratamento dos dados pessoais. Neste caso, o refinamento realizado foi tanto por tipo (tais como: finalidade e adequação) quanto por tópico (tratamento de dados pessoais) para refletir precisamente a característica e o objeto a que se aplica. Também utilizamos a decomposição do tipo "AND", uma vez que o texto da lei indica que todas as características são necessárias.

Por fim, no quinto nível do SIG, demonstramos como outros catálogos podem ser reutilizados para enriquecer a estrutura existente e auxiliar no entendimento. Neste caso, identificamos que a qualidade "informativo" já havia sido considerada e detalhada no Catálogo de Transparência de Software (CTS) [9]. O CTS apresenta o refinamento de "informativo" através de relacionamento de colaboração do tipo "*help*", indicando que a satisfação das qualidades do nível inferior contribui de forma positiva para a satisfação da qualidade do nível superior. De acordo com o CTS, "clareza", "consistência", "integridade", "corretude", "acurácia", "atualidade", "completeza" e "comparabilidade" podem contribuir para a qualidade informativo. Incorporamos este detalhamento no SIG da LGPD por entender que a característica de proporcionar informação, definida no texto da LGPD, se assemelha a definição de "informativo" do CTS.

De maneira geral, podemos dividir o SIG da LGPD (Figura 4) em três partes: (1) estrutura genérica da lei (1° e 2º níveis), (2) análise de características presentes no texto da lei (3º e 4º níveis) e (3) refinamento com viés de implementação (5º nível).

Fig. 4. Interação entre as partes do SIG da LGPD

A segunda e terceiras partes são resultado de um processo de análise sujeito a interpretação por um, ou um grupo de indivíduos. Neste trabalho, identificamos, à princípio, dois níveis compondo a segunda e um nível na terceira parte, contudo, outro grupo de indivíduos pode chegar a um detalhamento diferente, dependendo de sua interpretação. Por isso sugerimos um processo de construção similar à elaboração do CTS, o qual permite que um grupo de pessoas construa estruturas similares através de um conjunto de atividades orientadas a busca de um consenso.

O resultado desta 1ª etapa é a estrutura de SIG, apresentada da Figura 3, que compreende o padrão objetivos, conforme definido por [2]. Esta estrutura é utilizada como insumo para a 2ª etapa, que compreende a definição do padrão alternativa, a qual será definida a seguir.

3.3 Modelar Padrão Questão

No padrão questão, os objetivos definidos no último nível do SIG, são detalhados através de categorias e questões. Para exemplificar este processo, detalhamos o RNF clareza utilizando esta abordagem (Figura 5).

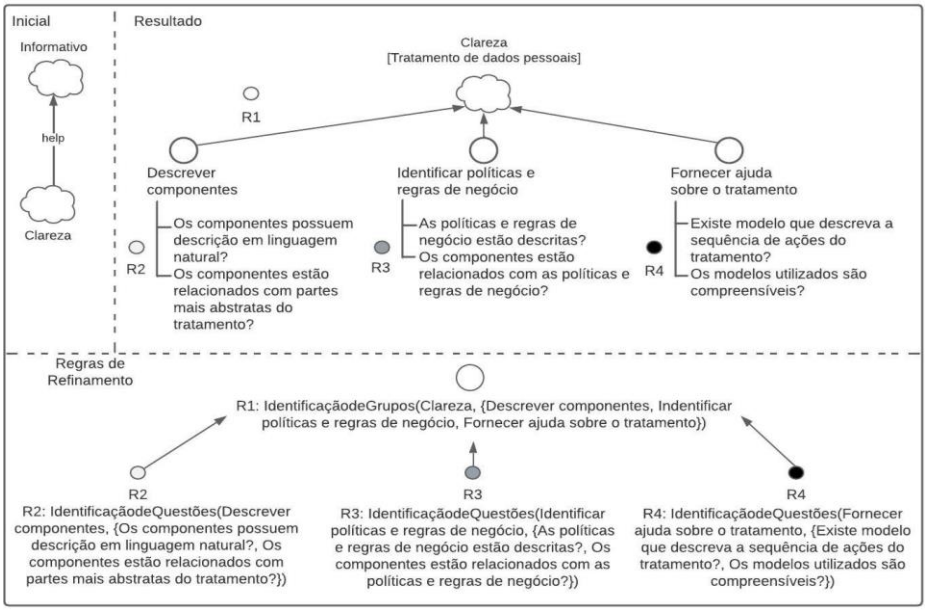

Fig. 5. Padrão Questão do softgoal clareza, instanciado para "Tratamento de dados pessoais" [2]

Como mencionado anteriormente, o refinamento do NFR "informativo" foi baseado no trabalho realizado para definição do CTS. Desta forma, baseamos a construção do nosso padrão questão na mesma estrutura, realizando adaptações em decorrência do tópico, que, no CTS era "software" e, neste caso, é "tratamento de dados pessoais". O CTS define clareza como "capacidade de ser nítido e compreensível".

Para proporcionar este detalhamento identificamos três categorias: "descrever componentes", identificar políticas e regras de negócio" e "fornecer ajuda sobre o tratamento". Estas características seguem o raciocínio de que, para ser claro, as partes de um processo precisam ser detalhadas. Além disto, como o tratamento ocorre em um contexto organizacional, estas partes precisam ser relacionadas à organização através de seus processos de negócio. Por fim, a ajuda é um recurso essencial para tornar estas partes, e o todo, mais fáceis de entender.

Seguindo a proposta de [2], as perguntas são definidas para auxiliar na orientação do alcance das metas subentendidas pelas categorias. Assim, a resposta à pergunta "os componentes possuem descrição em linguagem natural?" é um elemento, juntamente com a resposta às demais questões da categoria, que deve ser considerado para determinar se a descrição dos componentes foi satisfatoriamente realizada.

Ressaltamos que as estruturas apresentadas neste trabalho foram elaboradas apenas para demonstrar a abordagem proposta. O processo de montagem dessas estruturas tem níveis diferentes de sistematização, como observado acima sobre a construção do CTS.

3.4 Modelar Padrão Alternativa

A última etapa da abordagem de catálogo consiste no padrão Alternativa (Figura 6). Como o próprio nome diz, este padrão permite a definição das alternativas identificadas para a satisfação à contento das qualidades definidas no padrão objetivo (SIG).

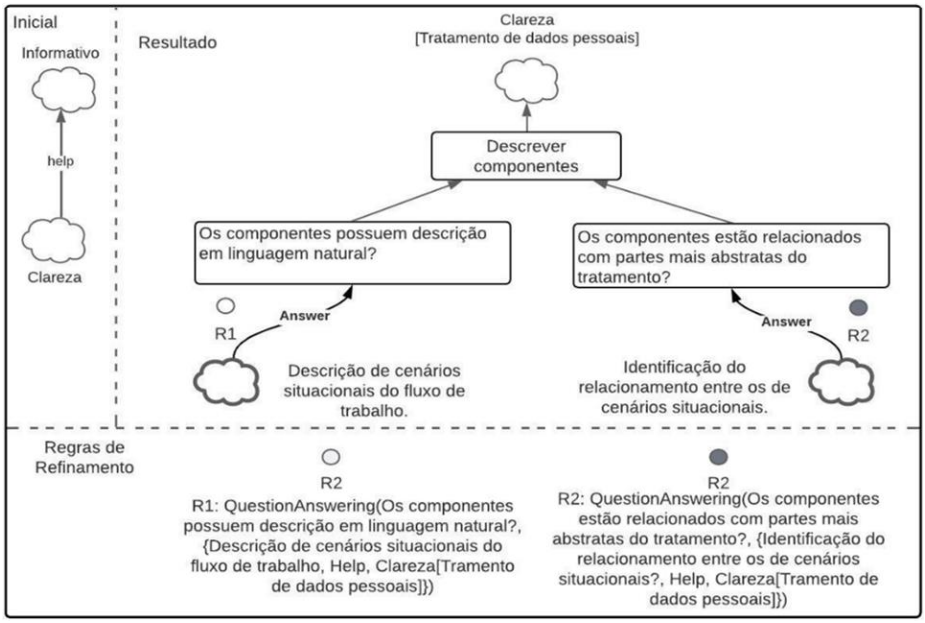

Fig. 6. Padrão Alternativa do softgoal clareza, instanciado para "Tratamento de dados pessoais"

As operacionalizações são explicitadas como respostas às perguntas do padrão questão. Para exemplificar esta ideia, apresentamos um exemplo relacionado a categoria "descrever componentes" do RNF "clareza". Neste caso, a "descrição de cenários situacionais do fluxo de trabalho" é uma possível resposta às perguntas "os componentes possuem descrição em linguagem natural" que, por sua vez, está associada a categoria "descrever componentes".

Desta forma, concluímos o ciclo proposto por [2] e conseguimos relacionar alternativas de operacionalização aos diferentes níveis de decomposição, proporcionados pelos padrões objetivo, questão e alternativas.

Para exemplificar, podemos seguir o rastro criado através dos exemplos utilizados neste trabalho. Desta forma, podemos argumentar que a operacionalização "descrição de cenários situacionais do fluxo de trabalho" contribui para "clareza", que, por sua vez, contribui para "informativo" (relacionamento *help*), o qual é necessário para satisfazer a contento a "finalidade" (relacionamento *AND*), que é necessária para a conformidade com o artigo 6º da LGPD (relacionamento *AND*), parte das condições necessárias para adequação à lei (relacionamento *AND*).

4. Conclusão

Neste trabalho apresentamos uma proposta de elaboração de um catálogo de RNF para auxiliar organizações a alcançarem a conformidade com a LGPD, que estabelece uma série de restrições para o tratamento de dados pessoais. Este tipo de legislação tem impacto direto na área de TI das organizações, mais especificamente em seus sistemas de informação, uma vez que o tratamento é, em grande parte dos casos, realizado através de sistemas computacionais.

A proposta baseia-se em um catálogo de qualidades (RNFs) com alto nível de abstração, possibilitando a compreensão e definição de ações a partir da perspectiva de operacionalizações. Durante a elaboração do catálogo um rastro é mantido, possibilitando que a avalie se todos os elementos de uma lei foram considerados e, de forma análoga, demonstre que ações foram tomadas para alcançá-los.

O rastro entre metas flexíveis e operacionalizações registrado no catálogo é importante para demonstrar que determinada organização agiu em busca de implementar a LGPD, bem como se orientou por artefatos técnicos, demonstrando o vínculo de suas operacionalizações e os artigos da lei através do catálogo. Além dos aspectos técnicos, cremos que esta documentação, bem construída, possa ser usada para demonstrar a boa-fé, nos casos de defesa previsto no Art. 52 §1º.

Este trabalho é relevante em um contexto em que a sociedade demanda ações governamentais para coibir o mal uso da tecnologia pelas organizações e o Estado responde através da criação de um arcabouço legal. A LGPD é uma das leis mais relevantes, contudo, há outras, como o Marco Civil da Internet e, mais recentemente, a discussão sobre a PL das *Fake News*.

Apesar da LGPD ter como principal objetivo a privacidade, ao realizar a análise de seu texto é possível verificar a existência de diversas características, que são discutidas em níveis de abstração distintos e que, em alguns casos, possuem um viés mais próximo do funcional. Isto contribui sobremaneira para a complexidade para elaboração de uma proposta objetiva e única para as organizações lidarem com este tipo de regulação.

Cabe às organizações encontrarem as ferramentas adequadas para atender os requisitos estipulados por leis, a fim de mitigar os riscos associados a punições. O próprio texto da LGPD deixa claro que além de atentar às restrições impostas, é obrigação das organizações demonstrar que estas estão sendo obedecidas.

Antes de iniciar este trabalho, já havíamos percebido que não seria fácil atender às restrições impostas pela lei e demonstrar como isso é realizado. Todavia, durante a construção do catálogo proposto, essa complexidade e o esforço necessário para

alcançar estes objetivos ficaram evidentes. Apresentamos um exemplo que considera apenas uma fração do que a Lei impõe, e o fizemos considerando o reuso de outros catálogos relacionados. Ainda assim, o esforço foi considerável e, provavelmente, caso fosse apresentado em um contexto organizacional, não seria um consenso entre os envolvidos

A busca por um consenso na definição do catálogo não é uma tarefa simples. As leis são complexas e podem levar a interpretações divergentes e até conflituosas, partindo do ponto de vista dos diferentes leitores. Portanto, sempre haverá o risco de que a interpretação daqueles que estão julgando a conformidade com a lei seja distinto dos que orientaram o processo de dentro da organização.

Em trabalhos futuros, cremos ser possível a definição de um modelo para guiar a implementação da LGPD. Em [1] observou-se uma forte correlação entre a estrutura do CTS e o MPS.BR, a qual pode ser replicada no presente caso, apoiando a construção de um modelo evolutivo para o caso da LGPD. Cremos que a proposta apresentada neste artigo também possa ser explorada na análise de outras leis [23]. Por exemplo, GDPR não fez parte do escopo deste trabalho, no entanto, trata-se de uma lei de assunto similar, o qual deverá ser avaliada no futuro. Por fim, a viabilidade de uso efetivo do artefato "catálogo de RNF" como um recurso jurídico será aprofundada.

Referências

1. Sousa, H. P.S., Leal, A. L. de C., & Leite, J. C. S. do P. (2015). Alinhamento de operacionalizações entre Transparência e MPS.BR. *ISys - Brazilian Journal of Information Systems*, *8*(4), 109–141. https://doi.org/10.5753/isys.2015.296
2. Supakkul, S., Hill, T., Chung, L., Tun, T.T., Leite, J.C.S.P. "*An NFR Pattern Approach to Dealing with NFRs*", IEEE *International Conference* on *Requirements Engineering*, pp. 179-188, ISBN: 978-0-7695-4162-4, 2010.
3. Simon, H.A. *The Sciences of the Artificial*, 3rd ed. The MIT Press, Cambridge, MA, 1977.
4. Gomes, T.; Alencar, F. Um *survey* com especialistas como validação de elementos para composição de uma ontologia para Sistemas AAL (*Ambient Assisted Living*). WER, 2022.
5. Alves, C., Neves, M.. "Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso." WER. 2021. http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER21/WER_2021_paper_31.pdf
6. Santana, E., Vilela, J., Peixoto, M. "Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário." WER 2022 http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_15.pdf
7. Ferrao, S.E.R, and Dias, E.. "Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil." WER 2022 http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_14.pdf
8. Dubois, E.; Yu, E.; Petit, M.. "*From early to late formal requirements: a process-control case study*." *International Workshop on Software Specification and Design*, 1998.
9. Catálogo de Transparência de Software. Disponível em http://transparencia.inf.puc-rio.br/wiki/index.php/Cat%C3%A1logo_Transpar%C3%AAncia. Acesso em maio de 2023.
10. Chung L., Nixon B. A., YU E., Mylopoulos J., *Non-Functional Requirements in Software Engineering*. Kluwer Academic Publishers, Lamsweerde A. *Requirements Engineering: From System Goals to UML Models to Software Specifications*. Wiley; 2009.

11. Cysneiros, L. M., Werneck, V. M., Kushniruk, A.: *Reusable knowledge for satisficing usability requirements*. IEEE *International Conference on Requirements Engineering*, (2005).
12. Oliveira, R., et al. "*Eliciting accessibility requirements an approach based on the NFR framework*." *Proceedings of Annual ACM Symposium on Applied Computing*. 2016.
13. Zinovatna, O., Cysneiros, L. M.: *Reusing knowledge on delivering privacy and transparency together*. In: IEEE *Fifth International Workshop on Requirements Patterns*, 2015.
14. Lei nº 13.709, LGPD, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
15. Regulation (EU) 2016/679, GDPR, https://eur-lex.europa.eu/eli/reg/2016/679/oj.
16. De Abreu, L. F.; Barbosa, G. A. R.; Silva, I. S.; Santos, N. S. Caracterização dos Processos para Elicitação de Requisitos de Software: Uma revisão sistemática da literatura. *In*: Simpósio Brasileiro De Sistemas De Informação (SBSI), Florianópolis. Porto Alegre: SBC, 2016. p. 192-199. DOI: https://doi.org/10.5753/sbsi.2016.5962.
17. Lamblet, I.S; A. S. Sanglard, J.; Lazarin, N. M. Sigilo médico-paciente sobre criptografia ponta-a-ponta. *In*: Escola Regional De Redes De Computadores (ERRC), Evento Online. Porto Alegre: SBC, 2020. p. 161-167. DOI: https://doi.org/10.5753/errc.2020.15206.
18. Sousa, T.R.; Coutinho, M.; Coutinho, L.; Albuquerque, R. LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados. *In*: Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais (SBSEG), Petrópolis. Porto Alegre: SBC, 2020. p. 55-68. DOI: https://doi.org/10.5753/sbseg.2020.19227.
19. Nardelli, C. Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. *In*: Escola Regional De Engenharia De Software (ERES), 2021, Evento Online. Porto Alegre: SBC, 2021. p. 169-178. DOI: https://doi.org/10.5753/eres.2021.18462.
20. De Castro, M.M; Pereira, M.B.; DE Castro, M.F. Uma Arquitetura Baseada em Blockchain para Auditoria de Conformidade com Regulamentos de Proteção de Dados. *In*: Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG), Santa Maria. Porto Alegre: SBC, 2022. p. 390-395. DOI: https://doi.org/10.5753/sbseg.2022.225347.
21. Teixeira, R. F. da S.; Januzi, R. B.; Faria, F. A.. *The Brazilian Data at Risk in the Age of AI?*. Encontro Nacional De Inteligência Artificial E Computacional (ENIAC), Campinas/SP. Porto Alegre: SBC, 2022. p. 413-424. DOI: //doi.org/10.5753/eniac.2022.227520.
22. Cunha, Herbet, et al. "*The challenges of representing transparency as patterns*", 3rd International Workshop on Requirements Patterns (RePa). IEEE, 2013.
23. Priscila, E., Cappelli, C., Leite, J.C.S.P. "*Eliciting concepts from the Brazilian access law using a combined approach*." ACM Symposium on Applied Computing. 2014.
24. Mendes, J.; Viana, D.; Rivero, L.. *Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal*. *In*: Simpósio Brasileiro De Engenharia De Software (SBES), Joinville. Porto Alegre: SBC, 2021.
25. Schinaider, A. D., Fagundes, P. M., Schinaider, A. D. Comportamento do consumidor educacional: seu perfil e o processo de decisão de compra. *Future Studies Research Journal: Trends and Strategies* 8.2 (2016): 144-164.
26. Finkelstein, M. E., Finkelstein, C.. "Privacidade e lei geral de proteção de dados pessoais." *Revista de Direito Brasileira* 23.9 (2020): 284-301.
27. Maple, C. "*Security and privacy in the internet of things*." *Journal of cyber policy* 2.2 (2017): 155-184.
28. Gominho, L. B. F, Severiano, G. C. "Direito a privacidade na internet: a lei geral de proteção de dados pessoais." *Revista Jurídica Facesf* 3.2 (2021): 7-20.