

LGPD e Requisitos de Software: Desafios e Oportunidades de Pesquisa

Lucas Vieira de Moura¹, Emanuel Coutinho¹

¹Programa de Pós-Graduação em Computação (PCOMP)
Universidade Federal do Ceará (UFC) – Quixadá – CE – Brasil

lucasmoura07@alu.ufc.br, emanuel.coutinho@ufc.br

Abstract. *Software requirements, whether functional or non-functional, are essential elements of Software Engineering, and present in the daily life of systems development projects. Elicitation and specification activities often involve development teams, clients, and access to data from institutions or companies. The LGPD appears as a way to protect data and individuals' fundamental freedom and privacy rights. In this context, this work aims to present challenges and research opportunities for requirements and the LGPD, so that individuals have the protection of their data already incorporated into the software development process.*

Resumo. *Requisitos de software, sejam funcionais ou não funcionais, são elementos essenciais da Engenharia de Software, e presentes no cotidiano dos projetos de desenvolvimento de sistemas. As atividades de elicitação e especificação muitas vezes envolvem equipe de desenvolvimento, clientes, e acesso a dados de instituições ou empresas. A LGPD surge como uma forma de proteger os dados e direitos fundamentais de liberdade e de privacidade dos indivíduos. Nesse contexto, esse trabalho visa apresentar desafios e oportunidades de pesquisa para requisitos e a LGPD, de forma que os indivíduos tenham a proteção de seus dados já incorporados no processo de desenvolvimento de software.*

1. Introdução

Com o uso crescente de aplicativos digitais, violações de dados ocorrem todos os dias, causando diversos problemas para empresas e usuários. Além disso, o uso indevido de dados dos usuários pode implicar em penalidades quando violados ou usados em desacordo com a legislação. Nesse sentido, projetistas e desenvolvedores de aplicações devem cumprir normas que garantam a privacidade dos usuários e a forma como seus dados são utilizados, o que no Brasil é previsto pela Lei Geral de Proteção de Dados (LGPD) [Rocha et al. 2023]. No Brasil, as organizações de desenvolvimento de software, públicas ou privadas, que processam dados pessoais dos usuários devem cumprir um grande número de regulamentos e garantir que os requisitos de negócios e sistemas estejam em conformidade legal, ou seja, implementam a LGPD em todos os seus sistemas de software [Canedo et al. 2020].

A atual sociedade vive numa era onde tecnologias inteligentes de captação e monitoramento de dados em tempo real são utilizadas, e o desenvolvimento de software precisa garantir a privacidade e proteção dos dados pessoais [Saraiva and Soares 2023a].

Sistemas e serviços de software contemporâneos exigem uma conectividade entre indivíduos e entidades corporativas, sejam elas públicas ou privadas, que resultam em atividades de coletar, processar ou divulgar regularmente grandes volumes de dados [Alves and Neves 2021]. Além disso, ao considerar o aumento na coleta, partilha e tratamento de dados pessoais em soluções tecnológicas cada vez mais inteligentes, torna-se imperativo proteger os titulares dos dados [Saraiva and Soares 2023b].

A LGPD [Brasil 2018] apresenta diretrizes para contextos relacionados a transações de dados e fatores importantes para garantir a privacidade dos dados dos usuários [Castro et al. 2022]. Ela visa garantir os direitos individuais e promover o desenvolvimento tecnológico através de regras claras, transparentes e abrangentes para o uso adequado de dados pessoais. Em um contexto institucional complexo, onde uma variedade de aplicações e sistemas coexistem, dados são constantemente obtidos e gerados, refletindo a dinâmica contínua das operações. Além disso, uma significativa dificuldade na adaptação à LGPD é enfrentada, seja devido aos esforços e custos adicionais envolvidos, seja pela falta de familiaridade com a LGPD e suas práticas de implementação.

A Engenharia de Requisitos (ER) é uma etapa fundamental e indispensável no processo de desenvolvimento de software. Isso porque seu objetivo principal é garantir que as necessidades e expectativas dos usuários finais sejam compreendidas e atendidas de forma efetiva [Kotonya and Sommerville 1998]. ER é geralmente ensinada como parte do currículo de cursos de computação. Segundo Mohan e Chenoweth (2011), os cursos geralmente abordam temáticas como a elicitação de requisitos, análise, especificação, validação e gerenciamento de requisitos. Além disso, os alunos geralmente são expostos a ferramentas e técnicas para documentação e modelagem de requisitos. Conforme mencionado por Osada et al. (2007), a abordagem tradicional para ensinar requisitos de software ainda depende fortemente da UML.

Nesse sentido, a LGPD se torna um aspecto a ser considerado dentro do processo de desenvolvimento de aplicações e sistemas, pois envolve a necessidade de funcionalidades estarem aderentes a seus princípios. Isso implica em uma forte relação com requisitos de software. Desse modo, por exemplo, os profissionais de desenvolvimento de software devem aprimorar seu aprendizado em relação a técnicas que garantam a privacidade e o cumprimento dos princípios da LGPD, o que pode ser alcançado por meio da utilização de um guia [Rocha et al. 2023].

De uma maneira mais ampla, em muitos contextos profissionais, tem-se observado uma crescente demanda pela adequação das instituições à LGPD, um requisito que ainda não se tornou comum [Ferreira et al. 2022]. Isso inclui a necessidade de modelagem de processos que estejam em conformidade com os princípios da LGPD [Araújo et al. 2021]. Adicionalmente, existe uma preocupação evidente em desenvolver metodologias ou abordagens que possam auxiliar os profissionais na implementação eficaz da LGPD [Castro et al. 2022, Rocha et al. 2023].

2. Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo [Brasil 2018]. A Lei discorre sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica

de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

A LGPD menciona que a disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Ela também se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

3. Desafio Proposto

Essa pesquisa traz a seguinte questão norteadora: “*Como os Requisitos de Software podem estar alinhados com a LGPD durante o processo de desenvolvimento de software?*”. E por Requisitos de Software, podemos ainda dividir em Requisitos Funcionais (RF) e Requisitos Não Funcionais (RNF). Então o desafio segue na linha de pesquisar LGPD, Requisitos de Software e suas implicações.

4. Contexto

Alguns dos itens a seguir são contextos ou situações que este desafio pode ser considerado.

Capacitação: O conhecimento em LGPD é necessário para que RF e RNF estejam alinhados a seus princípios. Conhecer os princípios da LGPD é algo essencial para que os requisitos estejam adequados e possam ser validados. Além disso, não apenas na vida profissional, é importante também capacitar alunos de cursos de graduação sobre os conceitos e aplicações da LGPD, garantindo uma base sólida de conhecimento a respeito do tema desde a formação.

Elicitação de RF e RNF: A elicitação de requisitos é uma atividade inicial do desenvolvimento de software, e muitas vezes envolve clientes, usuários e profissionais de sistemas e aplicações. A capacidade de se extrair requisitos muitas vezes depende da experiência de quem está conduzindo a elicitação e do conhecimento dos usuários sobre seus próprios processos de negócio, e adicionar elementos da LGPD para que esses requisitos sejam incorporados já no início do processo é algo essencial.

Especificação de RF e RNF: Uma vez requisitos elicitados, a atividade de especificar se inicia. Os modelos, textos e diagramas gerados nesse momento devem refletir aspectos da LGPD dentro do sistema, do ambiente, e devem ser entendidos pelos desenvolvedores. Neves Camêlo e Alves (2023) propuseram um catálogo de padrões de privacidade que serve para guiar a especificação de requisitos de privacidade em conformidade aos princípios da LGPD, como forma de apoiar a especificação.

Implementação de RF e RNF: Não apenas nas atividades de elicitar e especificar, mas

na etapa de implementação também há desafios. Além do conhecimento para o desenvolvimento em si de algo aderente a LGPD, há um acréscimo na carga de trabalho. Alves e Neves (2021) relataram equipes com pessoal bastante limitado para atender novas demandas, e uma dificuldade de interpretar e operacionalizar a LGPD no contexto dos sistemas e serviços prestados. Sá Sousa et al. (2023) sugeriram como trabalho futuro a definição de um modelo para guiar a implementação da LGPD.

Alinhamento sobre a coleta e uso dos dados: Consiste em uma maior interação entre as partes interessadas, planejando e deixando claras questões de segurança, privacidade e uso dos dados desde a fase inicial da Engenharia de Software. Adicionalmente, detalhar as coletas de dados e a finalidade para que estes serão utilizados, tal qual buscar prever e prevenir possíveis riscos a privacidade e integridade desses dados. O alinhamento dessas discussões às diretrizes da LGPD pode mitigar possíveis falhas de projeto, poupando tempo e custos financeiros por falta de conformidade com a LGPD.

Impacto econômico da não conformidade de RF e RNF com a LGPD: Cada vez mais sistemas serão cobrados por estarem alinhados com a LGPD. A não conformidade pode implicar em multas e sanções, necessidades de ajustes tanto em código quanto em infraestrutura. Todos esses aspectos requerem um esforço e tempo, e isso possui um custo financeiro associado.

Validação de requisitos quanto ao alinhamento com a LGPD: Esse desafio implica em processos de desenvolvimento, de qualidade, de testes. A validação dos requisitos já ocorre na própria especificação, com casos de testes, validação com especialistas em LGPD, e estende-se para as demais fases do processo de desenvolvimento de software.

Conscientização do uso de dados: A coleta de dados deve estar associada a uma necessidade ou finalidade específica, bem definida, deve ser clara e estar em conformidade com as diretrizes vigentes na legislação. Devido a conformidade com a LGPD, incorporada desde a fase de requisitos, a mudança do pensamento, dos hábitos de desenvolvimento eventualmente ocorrerá. Entretanto, essa mudança de cultura possui um preço, tanto comportamental, com resistências, e também do ponto de vista gerencial, com maiores esforços, prazos e custos.

5. Avaliação do Progresso

Alguns dos itens a seguir são possíveis formas de se visualizar, acompanhar e avaliar o desafio proposto.

Gestão dos recursos: Implementar e saber se os RF e RNF estão válidos, e em conformidade com a LGPD não é uma tarefa fácil. As formas de adequação aos princípios da LGPD requerem um esforço extra, requerem conhecimento sobre as diversas formas de estarem em conformidade e sobre a própria LGPD. Em caso de não conformidade, causas devem ser identificadas, por exemplo requisitos alinhados com a LGPD não especificados ou especificados incorretamente. A implementação de mais requisitos implica em mais custos financeiros, e possivelmente não incorporados nas estimativas iniciais.

Medição da qualidade dos RF e RNF: A incorporação da LGPD nos requisitos implicaria na sua inclusão dentro dos processos de desenvolvimento de software. Qualidade e testes naturalmente avaliam requisitos, e normalmente usam métricas para esse fim. Os profissionais envolvidos em testes e qualidade, normalmente analistas e projetistas de

testes, testadores e *Quality Assurance*, também devem estar atentos às novas diretrizes a serem consideradas devido a LGPD, além da necessidade de capacitação.

Avaliação da adequação dos RF e RNF a LGPD: A conformidade dos RF e RNF a LGPD pode variar em níveis. Um sistema ou ambiente pode estar totalmente aderente, parcialmente aderente, ou não aderente a LGPD. Isso pode levantar também questões éticas, pois o quanto (qual o grau) um sistema deveria estar aderente a LGPD é algo a ser considerado, além da relação custo benefício dessa aderência. Menegazzi e Silva (2023) propuseram um guia para alcançar a conformidade de sistemas de software com a LGPD por meio de Requisitos de Negócio e Requisitos de Solução, onde esse guia pode ser aplicado em sistemas que já estão em modo de produção - ou seja, que já estão sendo utilizados por seus usuários.

Produtos gerados de pesquisas: A interdisciplinaridade que este tema pode trazer às diversas áreas do conhecimento é uma oportunidade enorme para a geração de diversos produtos científicos. Por produtos científicos pode-se considerar artigos científicos relacionados a LGPD e Requisitos de Software, divulgação de resultados em eventos, produtos técnicos, como aplicações, e metodologias para aplicação em projetos e empresas. Adicionalmente, projetos de pesquisa que envolvam instituições diferentes são muito oportunos.

6. Considerações Finais

Esta pesquisa visa trazer para discussão elementos da Engenharia de Software, especificamente Requisitos Funcionais e Não Funcionais, sob a ótica da LGPD. Como contribuição para a sociedade, aplicações e sistemas podem estar mais alinhados com as diretrizes da LGPD, possibilitando um tratamento dos dados das pessoas de forma mais ética e segura, proporcionando benefícios tanto para os usuários, quanto para as organizações envolvidas.

Referências

- Alves, C. and Neves, M. (2021). Especificação de requisitos de privacidade em conformidade com a lgpd: Resultados de um estudo de caso. In *WER21 - Workshop em Engenharia de Requisitos*.
- Araújo, E., Vilela, J., Silva, C., and Alves, C. (2021). Are my business process models compliant with lgpd? the lgp4bp method to evaluate and to model lgp aware business processes. In *XVII Brazilian Symposium on Information Systems - SBSI (2021)*.
- Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd).
- Canedo, E. D., Calazans, A. T. S., Masson, E. T. S., Costa, P. H. T., and Lima, F. (2020). Perceptions of ict practitioners regarding software privacy. *Entropy*, 22(4).
- Castro, E., Silva, G. R. S., and Canedo, E. D. (2022). Ensuring privacy in the application of the brazilian general data protection law (lgpd). In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, SAC '22*.
- de Sá Sousa, H. P., Almentero, E. K., de Classe, T. M., dos Santos, R. J., and Leite, J. C. (2023). Uma abordagem baseada no catálogo de requisitos não funcionais para conformidade à lgpd. In *WER23 - Workshop em Engenharia de Requisitos*.

- Ferreira, L., Okano, M. T., Aguiar, F., De Castro Lobo dos Santos, H., and Ursini, E. L. (2022). A panorama of the implementation of the general law for the protection of personal data (lgpd) in brazil: an exploratory survey. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0723–0729.
- Kotonya, G. and Sommerville, I. (1998). *Requirements engineering: processes and techniques*. Wiley Publishing.
- Menegazzi, D. and Silva, C. (2023). Conformidade com a lgpd por meio de requisitos de negócio e requisitos de solução. In *WER23 - Workshop em Engenharia de Requisitos*.
- Mohan, S. and Chenoweth, S. (2011). Teaching requirements engineering to undergraduate students. In *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education, SIGCSE '11*, page 141–146, New York, NY, USA. Association for Computing Machinery.
- Neves Camêlo, M. and Alves, C. (2023). G-priv: A guide to support lgpd compliant specification of privacy requirements. *iSys - Brazilian Journal of Information Systems*, 16(1):2:1 – 2.
- Osada, A., Ozawa, D., Kaiya, H., and Kaijiri, K. (2007). The role of domain knowledge representation in requirements elicitation. In *25th IASTED International Multi-Conference Software Engineering*, pages 84–92. Citeseer.
- Rocha, L. D., Silva, G. R. S., and Dias Canedo, E. (2023). Privacy compliance in software development: A guide to implementing the lgpd principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC '23*, page 1352–1361.
- Saraiva, J. and Soares, S. (2023a). Adoption of the lgpd inventory in the user stories and bdd scenarios creation. In *Proceedings of the XXXVII Brazilian Symposium on Software Engineering, SBES '23*, page 416–421.
- Saraiva, J. and Soares, S. (2023b). Privacy and security documents for agile software engineering: An experiment of lgpd inventory adoption. In *2023 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*.