Desafios do Tratamento de Dados da LGPD em Aplicações Web

Lucas Moura[1], **Emanuel Coutinho**[1], **Leonardo Moreira**[2], **Inaldo Costa**[3]

[1]Universidade Federal do Ceará (UFC) – Quixadá – CE – Brasil

[2]Universidade Federal do Ceará (UFC) – Fortaleza – CE – Brasil

[3]Instituto Tecnológico de Aeronáutica (ITA) – São José dos Campos – SP – Brasil

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

leoomoreira@virtual.ufc.br,inaldo@ita.br

Abstract. *Currently, there is a massive data production and use, which may include personal data. In this context, regulations on privacy and protection of personal data have been proposed, such as General Data Protection Regulation (GDPR) and General Data Protection Law (LGPD). With the increasing use of digital applications, data breaches happen every day. Additionally, misuse of user data may result in penalties when breached. The objective of this research is to discuss aspects of the LGPD, specifically the data processing item, from the viewpoint of web applications. Some discussions and challenges are discussed, always considering the influence that LGPD data processing would bring.*

Resumo. *Atualmente há uma produção e utilização massiva de dados, os quais podem incluir dados pessoais. Nesse contexto, regulamentos sobre privacidade e proteção de dados pessoais vêm sendo propostos, como a General Data Protection Regulation (GDPR) e a Lei Geral de Proteção de Dados (LGPD). Com o uso crescente de aplicativos digitais, violações de dados acontecem todos os dias. Além disso, o uso indevido dos dados dos usuários pode implicar em penalidades quando violado. O objetivo desta pesquisa é discutir aspectos da LGPD, especificamente o item de tratamento de dados, sob o ponto de vista de aplicações web. Algumas discussões e desafios são discutidos, sempre considerando a influência que o tratamento de dados da LGPD traria.*

1. Introdução

Em mundo embasado em tecnologia, coleta e processamento massivo de dados (incluindo os pessoais), com uso de inteligência artificial, a Cibersegurança é um fator crítico [Espinha Gasiba et al. 2023]. Considerando que esses dados podem fazer parte da identidade e autodeterminação dos sujeitos, regulamentos sobre privacidade e proteção de dados pessoais vêm sendo propostos mundo afora, como é o caso da *General Data Protection Regulation* (GDPR) na Europa [Parliament 2016] e a Lei Geral de Proteção de Dados (LGPD) no Brasil [Brasil 2018]. Demandas legislativas impõem teorias, métodos e técnicas que abordem o desenvolvimento de software seguro, conforme previstos na LGPD, que exige que o desenvolvimento de produtos e soluções de software considerem a privacidade de dados pessoais desde a concepção e incorpore esta prática durante toda a vida do software [Saraiva et al. 2024].

Com o uso crescente de aplicativos digitais, violações de dados acontecem todos os dias. Além disso, o uso indevido dos dados dos usuários pode implicar em penalidades quando violado. Nesse sentido, projetistas e desenvolvedores de tais tecnologias devem cumprir normas que garantam a privacidade dos usuários, o que no Brasil é previsto pela 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].

Hoje se vive em uma 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]. 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]. Moura e Coutinho (2024) apontaram a conscientização do uso de dados como um desafio relacionado a LGPD, pois isso implica que em toda aplicação a coleta de dados deve estar associada a uma necessidade ou finalidade específica, bem definida, clara e estar em conformidade com as diretrizes vigentes na legislação. Devido a conformidade com a LGPD, a mudança do pensamento, dos hábitos de desenvolvimento será uma necessidade. 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.

O objetivo desta pesquisa é discutir aspectos da LGPD, especificamente para o item de tratamento de dados, sob o ponto de vista de aplicações *web*. Isso inclui diversas atividades comuns ao processo de desenvolvimento de software, como a interação com usuários, especificação de requisitos de software, planejamento de protótipos, desenvolvimento de aplicações, projeto de interfaces gráficas, dentre outras. O artigo está estruturado da seguinte forma, a Seção 2 apresenta alguns conceitos relacionados a LGPD; a Seção 3 apresenta alguns trabalhos relacionados; a Seção 4 lista algumas questões motivadoras; a Seção 5 apresenta desafios; e a Seção 6 apresenta as considerações finais.

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

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 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 discute 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.

Na lei, tem-se que a disciplina da proteção de dados pessoais possui 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. Esta lei aplica-se 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 objetos do tratamento tenham sido coletados no território nacional.

Segundo a LGPD, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas. Especificamente sobre o tratamento de dados, este pode ser considerado como toda operação realizada com dados pessoais, como as que se referem a acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização [Brasil 2021].

3. Trabalhos Relacionados

Neitzke et al. (2023) avaliaram e aprimoraram uma lista de verificação existente, a LGPD-Check, que é um método para avaliar a conformidade de sistemas de software com os atributos de qualidade relacionados a LGPD. A lista de verificação de avaliação consiste em múltiplos atributos distribuídos entre diversas categorias de avaliação, incluindo transparência de dados, consentimento do detentor, direitos do detentor, segurança de dados e responsabilidade do controlador. Isso está alinhado com a proposta dessa pesquisa pois há a necessidade de ter meios para analisar a aderência da LGPD.

Neves Camêlo e Alves (2023) discutem que a LGPD, assim como outras legislações existentes, são de difícil entendimento para analistas de requisitos, existindo dificuldades para se extrair e operacionalizar requisitos de privacidade. Este artigo propõe um catálogo de padrões de privacidade e um guia G-Priv, para auxiliar a especificação de requisitos de privacidade em conformidade com a LGPD. Isso está alinhado com a ideia desse artigo, que foca em aplicações web e precisam de requisitos alinhados com a LGPD.

4. Questões Motivadoras

Para esta pesquisa, duas questões motivadoras foram propostas para reflexão inicial.

4.1. Qual o impacto do tratamento de dados não adequado em uma aplicação *web*?

O mal uso dos dados de usuários de aplicações traz diversos impactos negativos, tanto para empresas, instituições, quanto principalmente para os próprios usuários. A falta de controle de acesso aos dados dos usuários possibilita vazamento de dados, roubo de informações, etc., o que pode trazer prejuízos financeiros e de reputação por exemplo [Zhang et al. 2022]. O compartilhamento indevido de dados, consequência de um controle de acesso deficiente, pode deixar o acesso livre para usuários maliciosos, falsificações, roubo de identidade, etc. Um tratamento de dados deficiente pode provocar a invasão de privacidade de usuários e instituições, o que leva a sérias consequências. Além disso, solicitações dos usuários podem não ser atendidas (por exemplo, exclusão

dos dados e revogação do acesso de funcionalidades), Por fim, sanções e multas para empresas podem ser incorridas em caso de não cumprimento da LGPD ou como forma de indenizações.

4.2. Como uma aplicação *web* poderia estar aderente a LGPD ou ter um tratamento dos dados adequado?

Inicialmente, para se ter uma adequação mínima a LGPD, deve-se ter conhecimento da lei de maneira geral. Especificamente para o tratamento de dados, onde diversas atividades são necessárias e implicam em mudanças nas aplicações, conhecimentos técnicos e de negócio são necessários. Uma boa prática seria a verificação dos casos exemplos da LGPD para o tratamento de dados. A implementação de funcionalidades (visuais ou não, *front end* ou *back end*) é uma consequência dessa adequação, e incorre em impactos em custos, prazos e esforços para as instituições. Os gestores das aplicações devem estar atentos ao tratamento de dados, pois alguma funcionalidade que não esteja aderente pode gerar problemas de privacidade de dados e judiciais. Por fim, muitas vezes será necessário que a aplicação passe por um *re-design*.

5. Desafios e Sugestões para o Tratamento de Dados da LGPD

Diversos desafios existem para o devido uso ou adequação dos sistemas à questões do tratamento de dados da LGPD. Nesta pesquisa, apenas alguns desafios e sugestões serão apresentados e discutidos.

5.1. *Privacy by Design*

A LGPD é inspirada na lei de privacidade de dados européia, a *General Data Protection Regulation* (GDPR) de 2018. A GDPR implementou o conceito de *privacy by design*, que possui como princípio evitar a prática comum de implementar contramedidas de segurança somente depois que as brechas de privacidade acontecem em um processo de negócio [Agostinelli et al. 2019].

O conceito de *privacy by design*, proposto por Ann Cavoukian [Cavoukian 2010], aborda a incorporação da privacidade e proteção de dados pessoais desde o início do processo de projeto de produtos e serviços. Aplicando *privacy by design* no desenvolvimento de interfaces seguras, os projetistas podem garantir a otimização da experiência de uso e conformidade com as regulamentações de privacidade. Sua aplicação em interfaces visuais de software implica na implementação de práticas de privacidade e segurança em todos os aspectos do *design*, desde a coleta e armazenamento de dados até a apresentação de informações e funcionalidades ao usuário [Cavoukian 2010]. Por definição, isto estaria bem alinhado com a adequação dos itens de tratamento de dados da LGPD.

Adicionalmente, o *privacy by design* também contribui para a criação de interfaces mais seguras ao promover a minimização de dados, limitação de propósito e implementação de medidas de segurança adequadas [Cavoukian 2010]. Por exemplo, a minimização de dados pode ser alcançada ao coletar apenas as informações estritamente necessárias para a funcionalidade em questão. A limitação de propósito pode ser garantida ao usar os dados coletados apenas para os fins especificados e nada mais. Medidas de segurança adequadas podem incluir a criptografia de dados, autenticação de dois fatores e *firewalls*.

Nesse contexto, aplicar *privacy by design* pode ser uma boa prática para sistemas estarem aderentes a LGPD. Porém, sempre há a necessidade de verificar a relação custo benefício deste esforço, considerando que há um esforço adicional de desenvolvimento e custos financeiros.

5.2. Consentimento e Revogação

O consentimento do usuário da utilização de seus dados é uma ação a ser considerada. Em outras palavras, é necessário solicitar a autorização do titular dos dados antes da ocorrer o tratamento dos dados. Do ponto de vista de interface gráfica, uma tela que explique bem conceitos, dados, finalidade, e que possibilite o usuário decidir como quer que seus dados sejam compartilhados seria uma boa opção inicial de discussão. Funcionalidades de aplicações que tenham como revogar o consentimento previamente autorizado também devem existir.

A questão relacionada ao consentimento é mais profunda, pois como garantir o correto consentimento e revogação? Isso implica em diversas decisões de projeto das aplicações, pois a forma como os dados são armazenados, qual o impacto da revogação do consentimento, como o usuário é comunicado sobre esses aspectos são aspectos a serem considerados.

5.3. *Design* de Interfaces

Para o projeto de uma interface gráfica é necessário conhecer sobre os requisitos, sobre regras de negócio da área em questão. Com a LGPD não é diferente, sendo necessário conhecer seus itens e implicações. Além disso, é necessário ter conhecimento de técnicas para projetar interfaces, sejam *web* ou *mobile*, conhecer ferramentas, dentro outros diversos conhecimentos que ajudam na definição de uma boa experiência para o usuário.

A Interação Humano Computador (IHC) apresenta conceitos, técnicas, guias de desenvolvimento, avaliações, etc, dentre outras maneiras de projetar e avaliar interfaces. *User Experience* (UX) e *User Interface* (UI) são dois exemplos. À medida que o UX preocupa-se de modo geral com a experiência final do usuário ao utilizar algum sistema, o UI dá enfoque na usabilidade, ou seja, um bom projeto de interface, agradável, acessível, fácil de utilizar, etc [Barbosa and Silva 2010].

A interface é a porta de visita de qualquer sistema, principalmente na questão de usabilidade e confiabilidade. Ou seja, o sistema deve ser agradável ao usuário, mas também deve passar confiança. O mesmo deve sentir-se confortável em fornecer dados sensíveis. Uma interface bem planejada necessita de fatores que englobem o máximo de usuários possíveis levando em conta possíveis limitações e preferências dos mesmos. O IHC analisa diversas questões que envolvem os aspectos de desenvolvimento e análise de interfaces e devem ser levados em consideração na produção ou adequação de qualquer sistema.

O IHC preocupa-se também com aspectos éticos. Nesse sentido, Barbosa e Silva (2010) abordam fatores como coleta de dados, porém esta abordagem não diz respeito explicitamente a fatores relacionados a LGPD. Interfaces pensadas para facilitar o acesso do usuário a informações importantes relacionadas a coleta, armazenamento e utilização de seus dados são fatores frequentemente negligenciados atualmente, não sendo pautados metodicamente no *design* de interfaces.

5.4. Adequação de Sistemas

Por envolver uma nova concepção a respeito do desenvolvimento, caso a LGPD seja pensada e inserida desde a fase de planejamento do projeto, é comum haver custos envolvendo possivelmente novos profissionais, treinamentos, pesquisa, etc. Porém deve-se levar em conta que tais custos podem ser considerados investimentos, e na verdade podem ser mais baixos que inserir elementos relacionados a LGPD depois do sistema pronto e em funcionamento, ou seja, pode reduzir futuros custos de adequação [Moura and Coutinho 2024].

Seguindo a mesma ideia dos custos de implementação da LGPD, mudanças nos processos internos podem ser um desafio, uma vez que até mesmo o conhecimento sobre a LGPD em algumas empresas é escasso por parte dos engenheiros de software e da equipe de desenvolvimento [Alves and Neves 2021]. Nesse caso, torna-se necessário uma maior atenção interna por parte destas em pesquisas técnicas existentes ou desenvolver novas maneiras de inserir a LGPD em meio a seus processos de desenvolvimento.

Para isso, algumas questões podem ser levantadas afim de identificar possíveis barreiras que possam impedir ou atrasar a incorporação da LGPD nos projetos desenvolvidos, e buscar oferecer suporte para solucioná-las, como identificar possíveis falhas de projeto, falta de treinamento da equipe, negligência nos requisitos relacionados a segurança e privacidade dos dados dos usuários, etc. Em outras palavras, uma mudança no pensamento das empresas a respeito da importância de estar em conformidade com as diretrizes da LGPD.

Para avaliar a adequação de um sistema a LGPD algumas ações podem ser cogitadas, como a utilização de guias com boas práticas de incorporação, analise da legislação, utilização *checklists*, uma boa elicitação e analise de requisitos, etc. Os trabalhos de Menegazzi e Silva (2023), Neves Camêlo e Alves (2023), Mendes et al. (2021), Araújo et al. (2021) e Neitzke et al. (2023) apresentam modelos de algumas das estratégias mencionadas.

Vale destacar também que incluir práticas do IHC sempre é uma boa estratégia nessa adequação, uma vez que o IHC visa a construção de um sistema de um ponto de vista mais ético, acessível e agradável ao usuário, possibilitando boas ideias de requisitos de usabilidade, coleta e proteção de dados por exemplo. Isso pode ser afirmado pois uma boa integração das praticas de IHC e Engenharia de Software (ES) podem resultar em um sistema bem adequado às normas da LGPD. Nesse caso, as informações sobre o porquê dos dados estarem sendo coletados, para que fim cada dado será utilizado e como serão armazenados, que respaldo o usuário teria em caso de vazamentos, que tipo de métodos de segurança serão utilizados. No geral o usuário não possui acesso a esse tipo de informação, apenas preenche variados campos de dados, como é o caso de formulários *web* por exemplo, sem saber para qual finalidade isso esta sendo feito e qual nível de segurança será empregado na proteção dessas informações.

5.5. Coleta, Armazenamento e Segurança de Dados

O atual contexto tecnológico demanda cada vez mais espaço para armazenamento de informações. No contexto *web* não é diferente, pois milhares de dados são gerados a todo momento, criptografados ou não. Armazenar esses dados naturalmente demanda soluções que nem sempre são baratas de implantar e manter.

A demanda cada vez maior por espaço em disco pode resultar algumas vezes no compartilhamento de dados sensíveis e não autorizados. Em alguns casos, até mesmo dados não criptografados são compartilhados com terceiros, como é o caso de servidores de armazenamento em nuvem, que armazenam dados de diversos tipos, milhares de usuários e empresas [Sun et al. 2020].

Em síntese, pode-se dizer que o cliente compartilha seus dados com a aplicação que está utilizando, porém devido a custos de armazenamento e a alta demanda de dados para serem armazenados, a empresa proprietária do sistema pode contratar uma outra empresa para armazenar esses dados, terceirizando os dados, e isso pode se caracterizar como um problema de segurança e confiabilidade.

Quanto à coleta, a quantidade de dados coletados às vezes é incompatível com a necessidade, ou seja, dados não necessários para aquele contexto são coletados. Há ainda a questão que muitos *sites* e aplicativos não deixam claro o porquê de estarem coletando tais dados. A LGPD determina que os dados sejam coletados para fins específicos, e estes devem ser informados ao usuário de forma clara e objetiva, e não podem ser compartilhados com terceiros ou usados para outras finalidades fora do contexto para qual foram coletados.

Essa coleta excessiva de dados, pode acarretar em problemas diversos, além da exposição desnecessárias de dados do usuário, podem ainda ser por exemplo utilizados para fins comerciais diferentes dos motivo pelo qual foram coletados, podendo acarretar na quebra de confiança entre o usuário e seu servidor [Sun et al. 2020]. Ainda, este mesmo motivo aumenta demasiadamente a quantidade de dados a serem armazenadas, aumentando custos de armazenamento, e acarretando maiores danos em caso de eventuais falhas de segurança e vazamentos de dados por exemplo.

A clareza na coleta e uso dos dados, assim como nas medidas de segurança empregadas podem convencer o usuário que determinada aplicação é confiável, assim como possíveis falhas de segurança e mal uso dos dados podem causar o efeito oposto. Informações sobre onde os dados serão armazenados, por quanto tempo, e de que maneira serão trados e utilizados raramente são disponibilizadas ao usuário, tal como o motivo de cada dado que esta sendo informado estar sendo coletado, o que vai contra os princípios básicos da LGPD.

No que diz respeito a segurança, Sun et al. (2020) mencionam o fato de avanços significativos na proteção de dados no contexto *web*, novas tecnologias de criptografia possibilitam maior nível de confiabilidade. Os autores abordam e avaliam diversos aspectos da segurança *web* como criptografia e compartilhamento seguro entre plataformas distintas, o que pode ser uma grande saída para a questão dos altos custos, já que a nuvem pública proporciona um certo nível de barateamento no armazenamento de dados.

Além da nuvem, em geral empresas também possuem servidores próprios, e neste caso, é de total responsabilidade das mesmas a segurança dos dados armazenados nos mesmos. Nem sempre as empresas de software planejam-se adequadamente para construir um sistema de segurança robusto e confiável, ou seja, em alguns casos seja por falta de investimento, ou de conhecimento, requisitos importantes relacionados a segurança acabam por ser negligenciados [Villamizar et al. 2020].

A coleta e utilização dos dados, seja na web, em máquina local ou até mesmo

física, é de caráter particular entre o usuário que fornece os dados e a empresa, nesse sentido, a LGPD define que é de responsabilidade da empresa assegurar a segurança, privacidade e usar de maneira condizente esses dados de acordo com o fim proposto. Como o foco deste trabalho em especial é o contexto web social, o desenvolvimento de aplicações apesar de ter avançado no que diz respeito a segurança, ainda apresenta fragilidades. [Villamizar et al. 2020] que a maioria das equipes de desenvolvimento ágeis de sistemas que coletam e armazenam dados de usuários, muitos deles sensíveis não contam com a participação de especialistas em segurança.

Essa fragilidade pode causar sérios problemas para as organizações, uma vez que escândalos e vazamentos diminuem em muito a credibilidade e reputação das mesmas, podendo em casos mais extremos serem responsabilizadas judicialmente acarretando em custos financeiros e até mesmo em encerramento das operações em contextos desfavoráveis.

Nesse sentido, mostra-se que a coleta consciente e investimentos adequados em requisitos de segurança devem ser levados em conta tanto na fase de planejamento do sistema, quanto em uma posterior adequação de um existente às diretrizes da LGPD. Embora possam haver custos associados a esta normatização, futuramente tais ações podem respaldar a empresa de enfrentar possíveis problemas. Um bom levantamento de requisitos sobre coleta e segurança dos dados devem ser avaliados a fim de melhorar a relação e a confiabilidade do usuário em fornecer seus dados, e da empresa de usá-los de maneira ética e mantê-los seguros.

6. Considerações Finais

Esta pesquisa foca em aplicações *web*, porém existem muitas aplicações *mobile*, e muitas delas são versões do mesmo sistema/aplicação, sendo apenas interfaces do usuário e dispositivos diferentes, tecnologias diferentes. Porém, a ideia é a mesma. Os princípios da LGPD valeriam para ambas. Mudanças nas aplicações podem ser simples ou complexas, podem ser visuais ou no lado servidor ou em um banco de dados, e na forma de interação com o usuário. Além disso, comunicação ou esclarecimentos sobre o tratamento de dados são essenciais para que as equipes de manutenção das aplicações tenham uma melhor compreensão e conscientização da lei.

Essa pesquisa possui diversas contribuições, tanto do ponto de vista do desenvolvimento, quanto para o próprio uso. Do ponto de vista do desenvolvimento de sistemas, desde as fases de requisitos conceitos da LGPD já poderiam ser observados. A maneira como os dados são mantidos e utilizados pode acarretar em problemas tanto para empresas quanto para usuários. Isso implica em esforços no projeto da aplicação, componentes, interfaces de usuário, etc. Adicionalmente, como os dados dos usuários são utilizados por terceiros também influencia no projeto das aplicações, principalmente em casos de interoperabilidade e compartilhamento de dados.

Outro aspecto importante é o que fazer em caso de problemas devido a má utilização dos dados dos usuários. Além de problemas particulares (indivíduo), o que podem resultar em prejuízos financeiros ou pessoais, há também problemas para empresas, o que pode resultar tanto em multas, sanções ou perda de confiança.

Uma questão de relevância para esse tema é no aspecto da interação com o usuário. Como as interfaces de usuário de aplicações *web* podem contribuir para uma melhor

aderência a LGPD? O fator conhecimento da LGPD, e como os dados podem ser tratados, impactaria no *design* das interfaces, pois o usuário deve ter conhecimento e dar consentimento sobre o quê e para quê aplicação vai usar seus dados.

Uma avaliação de um usuário da aplicação antes e depois da adequação a LGPD e tratamento de dados é um esforço, portanto essa pesquisa não pode discutir sobre o real impacto do tratamento de dados da LGPD para o desenvolvimento de aplicações *web*. Este é um cenário futuro da pesquisa. Também não há informação sobre o esforço e custo de uma empresa ou desenvolvedor para estar aderente a LGPD ou às diversas formas de tratamento de dados, podendo ser um trabalho futuro.

Por fim, a própria LGPD possui diversos itens, porém essa pesquisa focou apenas no tratamento de dados. Isso provoca uma dificuldade em estar totalmente aderente a LGPD, devido principalmente a custos e conhecimento da lei. Para estar realmente aderente, todos os itens da LGPD deveriam ser analisados, implementados e atendidos. Isso implica em todas as fases do desenvolvimento do software a interação com pessoas que detenham conhecimento da LGPD, havendo impactos no projeto de aplicações.

Agradecimentos

Este trabalho foi realizado com recursos do Programa de Demanda Social / CAPES da Universidade Federal do Ceará (UFC).

Referências

Agostinelli, S., Maggi, F. M., Marrella, A., and Sapio, F. (2019). Achieving gdpr compliance of bpmn process models. In Cappiello, C. and Ruiz, M., editors, *Information Systems Engineering in Responsible Information Systems*, pages 10–22, Cham. Springer International Publishing.

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 lgpd4bp method to evaluate and to model lgpd aware business processes. In *Proceedings of the XVII Brazilian Symposium on Information Systems*, SBSI '21, New York, NY, USA. Association for Computing Machinery.

Barbosa, S. and Silva, B. (2010). *Interação humano-computador*. Elsevier Brasil.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`.

Brasil (2021). Glossário de termos técnicos da lgpd. `https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd/glossario-de-termos-tecnicos-da-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).

Cavoukian, A. (2010). Privacy by design: The definitive workshop. a foreword by ann cavoukian, ph.d. *Identity in the Information Society*, 3(2):247–251.

Espinha Gasiba, T., Iosif, A.-C., Suppan, S., Lechner, U., and Pinto-Albuquerque, M. (2023). Reflections on training next-gen industry workforce on secure software development. In *Proceedings of the 5th European Conference on Software Engineering Education*, ECSEE '23, page 1–10.

Mendes, J. a., Viana, D., and Rivero, L. (2021). 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 *Proceedings of the XXXV Brazilian Symposium on Software Engineering*, SBES '21, page 263–268.

Menegazzi, D. and Silva, C. (2023). Conformidade com a lgpd por meio de requisitos de negócio e requisitos de solução. In *Workshop em Engenharia de Requisitos (WER23)*.

Moura, L. and Coutinho, E. (2024). Lgpd e requisitos de software: Desafios e oportunidades de pesquisa. In *CSBC 2024 - WASHES 2024 / GranDASHES-BR*.

Neitzke, C., Mendes, J. a., Rivero, L., Teixeira, M., and Viana, D. (2023). Enhancing lgpd compliance: Evaluating a checklist for lgpd quality attributes within a government office. In *Proceedings of the XXII Brazilian Symposium on Software Quality*, SBQS '23, page 218–227, 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.

Parliament, E. (2016). Général data protéction régulation (gdpr) - régulation (eu) 2016/679.

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., Araújo, J., and Soares, S. (2024). Ensino da adequação à lgpd no desenvolvimento de software através da aprendizagem ativa e centrada no discente. In *Anais do IV Simpósio Brasileiro de Educação em Computação*, pages 204–213.

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)*.

Sun, S., Ma, H., Song, Z., and Zhang, R. (2020). Webcloud: Web-based cloud storage for secure data sharing across platforms. *IEEE Transactions on Dependable and Secure Computing*, 19(3):1871–1884.

Villamizar, H., Kalinowski, M., Garcia, A., and Mendez, D. (2020). An efficient approach for reviewing security-related aspects in agile requirements specifications of web applications. *Requirements Engineering*, 25(4):439–468.

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., and Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. *Int. J. Informationand Computer Security*, 19(3):402–442.