Requisitos de Privacidade para Aplicações de Crowdsourcing no Contexto das Cidades Inteligentes

Mônica da Silva
monica_silva@ic.uff.br
Instituto Federal de Mato Grosso
Cuiabá, Mato Grosso

José Viterbo, Flávia Bernardini
viterbo,fcbernardini@ic.uff.br
Universidade Federal Fluminense
Niterói, Rio de Janeiro

Cristiano Maciel
cmaciel@ufmt.br
Universidade Federal de Mato Grosso
Cuiabá, Mato Grosso

RESUMO

As tecnologias são parte integrante do funcionamento das cidades inteligentes, sendo aplicadas em muitas áreas, como: saúde, mobilidade, serviços públicos etc. O uso de tecnologias, como *crowdsourcing*, permite as pessoas colaborarem na criação e aprimoramento dos produtos e serviços das cidades e pode ser amplamente utilizado. No entanto, o uso dessas informações pode causar problemas de privacidade para os usuários. Para fornecer proteção adequada às informações é necessário primeiro definir os requisitos envolvidos. Identificamos a partir de uma revisão de literatura os principais requisitos de privacidade. Esses requisitos foram observados em estudos de privacidade abrangendo o uso de *crowdsourcing* no contexto de cidades inteligentes e as novas legislações de privacidade.

PALAVRAS-CHAVE

Crowdsourcing, Crowdsensing, Privacidade, Cidades Inteligentes, Requisitos Funcionais, Requisitos Não-Funcionais

1 INTRODUÇÃO

Aplicações de *crowdsourcing* se enquadram em diversas estruturas das cidades inteligentes. As informações obtidas podem ser utilizadas para a melhoria da qualidade de vida das pessoas. Além disso, auxiliam na tomada de decisões dos gestores, provendo recursos à solução de problemas. Entretanto, a coleta de dados nas cidades inteligentes pode revelar informações pessoais, principalmente, se forem aplicadas técnicas que permitem a inferência dos dados, tanto de forma direta, quanto indireta [6].

IHC 2019 - TRILHA ARTIGOS INTERNACIONAIS, Outubro 21–25, 2019, Vitória, Brasil., In Anais Estendidos do XVIII Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais, Porto Alegre: SBC,

Objetivando à proteção da privacidade das pessoas perante as novas tecnologias, legislações foram criadas e atualizadas. Surgindo a Lei de proteção de dados pessoais da União Europeia (General Data Protection Regulation ou GDPR) [4], a Lei nº 13.709 do Brasil (Lei Geral de Proteção de Dados Pessoais ou LGPD) [1], entre outras. Com o avanço das legislações e as novas tecnologias, a proteção dos dados privados precisa ser considerado durante todo o desenvolvimento de uma aplicação.

Para implementar uma aplicação que irá fazer uso de dados pessoais torna-se necessário considerar alguns requisitos. Esses irão depender do contexto e tipo de informação que será coletada como imagens, vídeos, localização, som, temperatura, umidade, biometria etc. e que podem, consequentemente, afetar a privacidade das pessoas.

Realizamos um mapeamento sistemático da literatura, para a identificar os requisitos de privacidade presentes no desenvolvimento de aplicações de crowdsourcing no contexto das cidades inteligentes. Um maior detalhamento da pesquisa pode ser observado no estudo de Silva *et al.* [3].

2 OS REQUISITOS DE PRIVACIDADE

Os requisitos identificados foram distribuídos e estruturados a partir de uma adaptação da proposta de dimensões criada por Nam e Prado [7], no qual os requisitos foram distribuídos em: Pessoas, Leis e Tecnologias. A dimensão das tecnologias foi dividida em três subdimensões: coleta, comunicação e armazenamento e análise. Mesmo utilizando a distribuição de dimensões, observamos que alguns requisitos podem atuar em mais de uma dimensão, pois irá depender do contexto da aplicação.

Dimensão: Pessoas

Uma constante em toda a estrutura do crowdsourcing são as pessoas, isto é, visitantes, usuários, profissionais da área de TI, gestores, provedores de serviços etc. As pessoas interagem com a cidades inteligentes no provimento de informações, recebendo benefícios, obtendo lucros, gerando serviços etc. Neste processo, as pessoas podem ter problemas de privacidade que ocorrem de forma intencional ou não, especialmente em sistemas de compartilhamento de informações, por exemplo, redes sociais [6]. Para essa dimensão foram

identificados três requisitos como, por exemplo: “O aplicativo deve fornecer recursos e informações para as pessoas controlarem seus dados” [3].

Dimensão: Leis

A GDPR [4] e a LGPD [1] são leis que definem a proteção dos dados pessoais, e nas quais, fica evidente que as pessoas têm o direito de receber as informações de forma clara e precisa sobre como seus dados serão tratados [4].

Para essa dimensão foram descritos doze requisitos, um por exemplo é: “O aplicativo deve informar o objetivo/razão envolvida na coleta de dados, sendo transparente” [3].

Dimensão: Tecnologias

Atualmente, existem bilhões de dispositivos conectados nas cidades, e ainda irá aumentar, tornando muito fácil coletar dados das pessoas e, assim, inferir informações privadas. No estudo de Eckhoff e Wagner [5] observou-se que dados pessoais podem ser coletadas por diversas tecnologias.

Existem diferentes requisitos que precisam ser observados para garantir a privacidade quando tratamos das tecnologias. Essa é a dimensão é mais complexa, pois, assim como uma tecnologia pode causar problemas de privacidade, ela também pode auxiliar na proteção da privacidade.

Coleta: a coleta das informações é a primeira etapa que precisa de proteção. Identificamos nove requisitos referentes a coleta, um exemplo é: "os sensores médicos que coletam dados de saúde devem ser protegidos com soluções de privacidade" [3].

Comunicação: devido a restrita capacidade computacional de alguns dispositivos, a aplicação de proteções de privacidade durante a comunicação ainda é um desafio [2]. Identificamos dois requisitos referentes a comunicação.

Armazenamento e Análise: os dados devem ser protegidos antes do armazenamento e ao apresentar informações oriundas da análise dos dados coletados a aplicação deve utilizar proteções que não permitam a restauração de informações. Identificamos cinco requisitos de privacidade para essa subdimensão. Um exemplo dos requisitos descritos é: "O armazenamento não deve permitir a restauração dos dados após a aplicação de uma solução de privacidade" [3].

3 SOLUÇÕES DE PROTEÇÃO

Existem diversas soluções propostas para a proteção da privacidade. Distribuímos essas soluções, considerando o estudo de Vergara-Laurens et al. [8] entre: as que modificam atributos; e as que não modificam os atributos.

Soluções que modificam os atributos

Compreendem técnicas que aplicam algoritmos para agrupar, ofuscar, anonimizar, minimizar etc. alterando a estrutura dos dados para impedir a identificação de um indivíduo no grupo.

Soluções que não modificam os atributos

São técnicas que aplicam algoritmos de proteção sem alteração das informações como encriptação, criptografia homomórfica etc., mas essas técnicas exigem mais recurso computacional.

4 CONSIDERAÇÕES FINAIS

Desenvolver aplicações garantam a proteção dos dados pessoais é um desafio. Ficando mais complexo quando envolvem estruturas superconectadas, que possuem diversas formas de coleta de informações, como ocorre nas cidades inteligentes. Ao mesmo tempo, esta proteção é essencial para obter a confiança e participação das pessoas. Para atender a essa necessidade de proteção novas formas de atuar com os dados pessoais terão que ser adotados.

REFERÊNCIAS

[1] Brasil. 2018. Lei nº 13.709, de 14 de Agosto de 2018. *Presidência da República* (2018). Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acessado em: 05/09/2018.

[2] C. Chowdhury, S. Roy, H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke. 2017. Mobile crowdsensing for smart cities. *Smart Cities: Foundations, Principles, and Applications* (2017), 125–154.

[3] M. da Silva, J. Viterbo, F. Bernardini, and C. Maciel. 2018. Identifying Privacy Functional Requirements for Crowdsourcing Applications in Smart Cities. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 106–111. https://doi.org/10.1109/ISI.2018.8587316

[4] P. Europeu e Council. 2016. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. (2016), 1—-88.

[5] D. Eckhoff and I. Wagner. 2018. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys Tutorials* 20, 1 (Firstquarter 2018), 489–516. https://doi.org/10.1109/COMST.2017.2748998

[6] B. Greschbach, G. Kreitz, and S. Buchegger. 2012. The devil is in the metadata – New privacy challenges in Decentralised Online Social Networks. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. 333–339. https://doi.org/10.1109/PerComW.2012.6197506

[7] T Nam and T.A Pardo. 2011. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*. ACM, 282–291.

[8] I. J. Vergara-Laurens, L. G. Jaimes, and M. A. Labrador. 2017. Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges. *IEEE Internet of Things Journal* 4, 4 (Aug 2017), 855–869. https://doi.org/10.1109/JIOT.2016.2594205