

Proposta de Mecanismo de Consentimento na Lei Geral de Proteção a Dados - LGPD

Marcello Peixoto Bax , João Luiz Silva Barbosa

ECI - PPGGOC - Universidade Federal de Minas Gerais (UFMG)
Av. Antônio Carlos, 6627 - Pampulha - 31270-901
Belo Horizonte - Minas Gerais - Brasil

{ bax@ufmg.br , joaoluiz.barbosa@gmail.com }

Abstract. *This paper describes the current stage of a research that looks for enabling elements for the semantic integration of a consent mechanism under the General Data Protection Law - LGPD with legacy systems. It also research analogous methodologies that are already established for the General Data Protection Regulation - GDPR, as well as models instantiated by them, to guide the creation of an ontology and a systemic approach that enable this integration.*

Resumo. *Este artigo descreve o estágio atual de uma pesquisa que busca por elementos habilitadores para integração semântica de um mecanismo de consentimento válido no âmbito da Lei Geral de Proteção de Dados – LGPD com os sistemas legados. Investigam-se metodologias análogas já estabelecidas para a General Data Protection Regulation - GDPR, bem como modelos instanciados por estas, para orientarem a criação de uma ontologia e uma abordagem sistêmica que viabilizem esta integração.*

1. Introdução

Privacidade é um tema que sempre desperta interesse nos indivíduos e na sociedade. Um dos trabalhos mais famosos é o *Panóptico* de J. Bentham (2008) que concebeu um ambiente físico onde as pessoas seriam monitoradas. A aplicação deste conceito em escolas, vilas e prisões trariam uma melhor “gestão” do indivíduo e das informações referentes a ele. Outro trabalho conhecido é o livro de ficção científica 1984 de Orson Orwell (1948) que aborda uma sociedade distópica onde todos são vigiados através de recursos tecnológicos. As “*Teletelas*” de Orwell transmitiam a mensagem do “Grande Irmão” e, por uma câmera embutida, observava (vigilância) o que ocorria com cada um dos “cidadãos”. Tais concepções literárias, como as citadas, poderiam ser transportadas para hoje e viabilizadas através da difusão da internet e dos dispositivos conectados em uma rede de larga escala.

A tecnologia celular atual de dispositivos conectados traz mecanismos de rastreamento e monitoramento não anonimizados, ao centro da discussão sobre a privacidade. Identificar a origem e destino de mensagens, seu conteúdo e participantes passou a ser possível no estágio atual das tecnologias disponíveis e vão no sentido oposto dos princípios de privacidade das diversas Constituições Republicanas, como p. ex., a Constituição Brasileira (Brasil, 2008). A preocupação com a preservação da privacidade

levou à elaboração de novas leis, dentre as quais destacam-se: GDPR¹ (União Europeia, 2016), LGPD² (Brasil, 2018) e a CCPA³ (Califórnia, 2018).

Este artigo descreve o estágio atual da pesquisa que, empregando-se metodologias validadas por Noy & Guinness (2001), colhe elementos para conceber uma ontologia da LGPD, implementar mecanismo de consentimento de uso de dados privados e aplica-lo a sistemas legados.

2. Problema de pesquisa e objetivos

De forma geral, os sistemas são concebidos com segurança de acesso e rastreamento das operações, conforme protocolo AAAS⁵ (IETF, 2012). Controla-se quem acessa o sistema (*accounting*), garante-se que seja realmente quem se declara ser (*authentication*), que execute somente operações que possa executar (*authorization*) e que proteja a comunicação emissor/receptor (*secure transport protocol*). Além disso, registra-se as operações feitas, por quem, quando e de qual forma. Estes mecanismos atendem ao sistema, mas não aos titulares dos dados, de quem se armazenar a informação. No registro de informações médicas dos pacientes, os usuários - médicos, enfermeiros, técnicos - são identificados e suas operações rastreadas. Cada um possui senha para acessar somente o necessário ao seu trabalho. As informações do paciente estão devidamente protegidas em um banco de dados. O protocolo AAAS citado acima é plenamente atendido, mas não aborda os aspectos relacionados ao paciente em si, alvo do armazenamento, processamento e proteção. Não lhe é dada alternativa de privacidade de forma ou conteúdo, tampouco de temporalidade, com o descarte adequado após uso.

A LGPD traz conceitos de privacidade e proteção de dados pessoais. Passa a ser necessária autorização do titular dos dados antes do tratamento ser realizado, e esse consentimento deve ser recebido de forma explícita e inequívoca. A ocorrência da “não necessidade de consentimento” é a exceção e só é possível processar dados sem autorização da pessoa física quando isso for indispensável para cumprir outras determinações legais que constem em regulações, normas ou legislações. Portanto, a LGPD demanda por ajustes nos sistemas existentes bem como na forma de tratamento dos dados qualificados como dados privados. Esta nova forma de tratar informações demandará novos mecanismos de integração, seleção classificação, expurgo e operação destes sistemas. Um mecanismo de registro de consentimento mostra-se em um primeiro momento como um processo simples de registro do que é ou não informação privada, mas em uma análise aprofundada percebe-se que as dificuldades de integração surgem da necessidade de estabelecimento de filtros do que pode ser armazenado ou obtido dos sistemas legados. Esta necessidade, vista a partir de uma abordagem não intrusiva demanda uma alta integração com um desacoplamento inicialmente contraditório. Em função disto, o primeiro passo para construir este novo ambiente sistêmico passa pela concepção de elementos habilitadores desta integração semântica. Neste contexto, ontologias apoiam a classificação, conceituação semântica declarativa, processamento e qualificação da proteção necessária às informações dos titulares de dados.

¹ Regulamento geral sobre a proteção de dados. General Data Protection Regulation. Regulamento da União Europeia, nº 679 de 27 de abril de 2016;

² Lei Geral de Proteção de Dados Pessoais. Lei Brasileira, nº 13.709, de 14 de agosto de 2018;

³ Lei de Privacidade do Consumidor do Estado da Califórnia. California Consumer Privacy Act. Resolução Californiana, nº AB-375, de 28 de junho de 2018

⁵ Authentication, Authorization and Accounting with Secure Transport, RFC 6733

A existência de metodologias, técnicas e ferramentas apresentadas por Almeida & Bax (2003); a existência de iniciativas similares como a GDPR; o nível de detalhamento da legislação brasileira e a proximidade da vigência da LGPD, nos motivam a pesquisar a sobre modelos de representação do conhecimento associados ao tema. Novas leis, como GDPR, LGPD e CCPA trazem reflexões sobre a proteção de dados pessoais, buscando respostas aos seguintes tipos de perguntas: (i) o indivíduo quer ser identificado? (ii) o indivíduo quer ter seus dados divulgados? Todos eles? (iii) o indivíduo quer selecionar algumas informações e permanecer com estas em caráter privado? além de outras. Como no exemplo de informações médicas: (i) o paciente deseja ser identificado? (ii) quais informações ou características o paciente deseja que não sejam disponibilizadas para os médicos ou outros usuários do sistema? (iii) o paciente concorda em ser considerado nas estatísticas do hospital? Percebe-se que as novas leis introduzem conceitos e problemas que não eram, na ordem geral da concepção e uso dos sistemas, usualmente abordados. Esta nova forma tratar informações demanda novos mecanismos de integração, seleção, classificação, expurgo e operação.

Busca-se, portanto, desenvolver uma ontologia de domínio (Guarino, 1997) que represente os conceitos e princípios descritos na LGPD e transponha seus conceitos em dados para registro em sistemas de informação, bem como uma ontologia de tarefa de uso para adaptação não intrusiva dos sistemas existentes ao que é preconizado. Entende-se como objetivos específicos a obtenção das seguintes conclusões e artefatos:

- Correlacionar os princípios e conceitos da LGPD por um tesauro;
- Questões de competências associadas ao domínio de conhecimento jurídico associado;
- Investigar o mecanismo de consentimento, os direitos dos titulares de dados, os deveres dos controladores e demais aspectos relacionados à finalidade, processamento, armazenamento, descarte e uso das informações indicadas como sensíveis e privadas;
- Elaborar ontologia de domínio do ciclo de vida das informações privadas e mecanismos de consentimento;
- Validar a ontologia criando instâncias típicas ao uso comum de titulares, controladores e usuários destas informações;
- Conceber e validar uma proposta de arquitetura entre os sistemas existentes e o mecanismo de consentimento de forma a permitir a integração e interoperabilidade sistêmica não intrusiva para troca e filtro dos dados classificados dentro do processo de privacidade de dados do titular;
- Especificar uma forma capturar e registrar consentimentos.

3. Trabalho relacionados mais próximos

Considerando as diversas pesquisas feitas, a contemporaneidade do tema, a inexistência de artigos científicos referenciados sobre ontologias e LGPD, e priorizando os trabalhos associados a GDPR em função da maior similaridade a lei brasileira, foram selecionados os seguintes trabalhos como correlatos a esta pesquisa.

Monica *et al.* (2018) trazem um primeiro rascunho de uma ontologia jurídica no GDPR, que tem o objetivo de fornecer uma modelagem de conhecimento jurídico dos agentes de privacidade, tipos de dados, tipos de operações de processamento, direitos e obrigações. A metodologia usada aqui é baseada na análise da teoria jurídica, associada a

padrões ontológicos. As tecnologias da Web semântica e as ferramentas de raciocínio jurídico são usadas para suportar a privacidade por padrão e a conformidade legal.

Bartolini, Lenzini & Robaldo (2019) apresentam um modelo do GDPR que permite um processamento semiautomático de texto jurídico e o aproveitamento de abordagens de informática jurídica de ponta, úteis para raciocínio jurídico, design de software, recuperação de informações ou verificação de conformidade. O modelo faz uso do Akoma Ntoso (padrão XML para documentos jurídicos) e do modelo PrOnto.

Rantos *et al.* (2019) introduzem uma solução centrada no usuário que permite que os titulares dos dados controlem facilmente os consentimentos sobre o acesso aos seus dados pessoais no ecossistema da IoT e exerçam seus direitos definidos pelo GDPR. Também auxilia controladores e processadores de dados a atender aos requisitos de GDPR. Por fim, apresenta detalhes preliminares de uma implementação parcial da estrutura proposta

Pandit *et al.* (2019) abordam a base legal para o processamento de dados pessoais sob a GDPR, fornecendo restrições e obrigações quanto à validade do consentimento e dos direitos de retirada do consentimento a qualquer momento. Indica as formas de demonstração do cumprimento dessas obrigações e de como o consentimento foi obtido, usado e alterado ao longo do tempo. O trabalho demonstra a viabilidade de tecnologias da Web semântica na modelagem de informações e na determinação da conformidade. Em seguida, apresenta o GConsent, uma ontologia OWL2-DL para representação do consentimento e suas informações associadas, como sua origem. Por fim, o artigo apresenta a metodologia usada na criação e validação da ontologia, bem como um exemplo de caso de uso demonstrando sua aplicabilidade.

Piurcosky *et al.* (2019). O estudo busca descrever e compreender a realidade de organizações brasileiras quanto à adequação à LGPD. Tal abordagem se justifica mediante regulamentações estabelecidas pelo Estado brasileiro para a manipulação, tratamento e armazenamento de dados pessoais por organizações. Desenvolve uma pesquisa com abordagem qualitativa e realizada por meio de estudo de casos múltiplos.

Os trabalhos citados acima que, no geral, abordam a GDPR trazem propostas de ontologias, metodologias de análise e construção de ontologias no domínio jurídico, aplicabilidade deste conhecimento em sistemas de informação, possibilidade de correlação de termos comuns e analogia de termos com alguma similaridade, bem como estratégias de como transformar a lei em instrumento concreto de proteção da privacidade. Todos estes trabalhos associados a GDPR, em conjunto com os trabalhos em curso no Brasil trazem ao contexto desta pesquisa, hora em curso, um ambiente de compartilhamento e completude necessária a construção de um modelo específico e aplicável ao contexto brasileiro da LGPD.

4. Metodologia

Como metodologia científica para seleção e elaboração dos artefatos ao domínio do conhecimento será utilizada a *Design Science Research* - DSR apresentada por Hevner *et al.* (2004). Esta metodologia traz também atualizações como a abordagem por ciclos curtos de desenvolvimento (Hevner, 2007), que combinados com a classificação dos requisitos das diversas etapas de um processo descritos por Morana *et al.* (2018) e as técnicas de construção dos artefatos citadas por Brocke *et al.* (2017) espera-se obter uma estratégia consistente para elaboração do mecanismo. Em adição, será adotado o processo ágil descrito por Peron (2017) e específico para concepção de ontologias. Os elementos serão organizados em artefatos para desenvolver uma ontologia de domínio que

represente os conceitos associados a LGPD, a transposição destes conceitos em dados e sistemas de informação, bem como uma ontologia de tarefa de uso destes para adaptação dos sistemas existentes ao que é preconizado pela lei. Para a formalizar as regras do modelo semântico em um dicionário de dados específico para o mecanismo, bem como criar elementos que viabilizem a sua integração será empregado o formalismo semântico descrito por Rashid *et al.* (2020).

5. Conclusão

Considerando o estágio atual da pesquisa, a extensa pesquisa bibliográfica a respeito do tema, a inexistência de trabalhos correlatos no Brasil a respeito de metodologias e ontologias associadas a LGPD, bem como a proximidade do início de sua vigência em território nacional, percebe-se uma oportunidade de ineditismo e de elaboração de uma ontologia de alto nível que possa ser utilizada em trabalhos subsequentes e complementares. O escopo original de cobrir desde a elaboração das ontologias de domínio e tarefa, detalhamento das regras, elaboração de mecanismo exemplo de interface entre os sistemas de registro de consentimento e os sistemas legados, até a simulação efetiva com dados reais mascarados, representa um passo bastante significativo e abrangente.

Ao longo do trabalho de elaboração da ontologia de domínio, é mandatório reavaliar a oportunidade de um maior aprofundamento na modelagem, troca de informações com outros pesquisadores e busca de sinergias a fim de qualificar onde melhor este trabalho pode trazer contribuições, seja na evidenciação de uma ontologia de topo, seja na delimitação de uma arquitetura de referência para trabalhos futuros que detalhem os elementos descrito na gênese desta pesquisa. Em qualquer um destes dois cenários, entende-se que a pesquisa terá potencial para atingir o seu objetivo de disponibilizar os elementos habilitadores da integração dos sistemas que suportarão a implantação da LGPD em organizações.

6. Referências bibliográficas

- Almeida, M. B.; BAX, M. P. Uma visão geral sobre ontologias: pesquisa sobre definições, tipos, aplicações, métodos de avaliação e de construção. *Ciência da Informação*, v. 32, n. 3, p. 7–20, dez. 2003.
- Bartolini, C., Lenzini, G., Robaldo, L.: The DATA Protection REGulation Compliance Model. *IEEE Secur. Priv.* 17(6), 37–45 (2019).
- Bentham, Jeremy. *O Panóptico*. Organização de Tomaz Tadeu. Traduções de Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. 2. ed. Belo Horizonte. Autêntica Editora, 2008.
- Brasil. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal: Centro Gráfico, 1988.
- Brasil. LGPD LEI NO 13.709, DE 14 DE AGOSTO DE 2018. Disponível em http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337 . Acesso em 6 de julho de 2020.

- Brocke, Jan vom & Fettke, Peter & Gau, Michael & Houy, Constantin & Maedche, Alexander & Morana, Stefan & Seidel, Stefan. Tool-Support for Design Science Research: Design Principles and Instantiation. SSRN Electronic Journal, 2017. DOI:<https://doi.org/10.2139/ssrn.2972803>.
- California, EUA. CCPA. 2018. Disponível em https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Acesso em 6 de julho de 2020.
- Guarino, N. Understanding, building and using ontologies. *International Journal of Human-Computer Studies*, v. 46, nº 2-3, pp. 293–310, 1997.
- Hevner, Alan & R, Alan & March, Salvatore & T, Salvatore & Park, & Park, Jinsoo & Ram, & Sudha,. *Design Science in Information Systems Research. Management Information Systems Quarterly*. v. 28 , p. 75-105, 2004.
- Hevner, Alan & R, Alan. *Three Cycle View of Design Science Research*. v. 19, p. 7, 2007.
- IETF. RFC6733. Diameter Base Protocol. 2012. Disponível em <https://tools.ietf.org/html/rfc6733>. Acesso em 6 de julho de 2020.
- Monica, P., Michele Martoni, Arianna Rossi, Cesare Bartolini, Livio Robaldo, PrOnto: Privacy Ontology for Legal Reasoning, in EGOVIS 2018, A. Kő and E. Francesconi (Eds.), LNCS 11032, pp. 139–152, 2018.
- Morana, S. et al. Tool Support for Design Science Research—Towards a Software Ecosystem: A Report from a DESRIST 2017 Workshop. *Communications of the Association for Information Systems*, p. 237–256, 2018.
- Noy, N. F.; McGuinness, D. L. *Ontology Development 101: A Guide to Creating Your First Ontology*. Knowledge Systems Laboratory, v. 32, 2000.
- Orwell, George. 1984. 29ª ed. São Paulo: Ed. Companhia Editora Nacional, 2005.
- Pandit, H.J., Debruyne, C., O’Sullivan, D., Lewis, D.: GConsent - a consent ontology based on the GDPR. In: Hitzler, P., et al. (eds.) *ESWC 2019*. LNCS, vol. 11503, pp. 270–282. Springer, Cham (2019). DOI:https://doi.org/10.1007/978-3-030-21348-0_18.
- Piurcosky, P, Fabricio & Costa, Marcelo & Frogeri, Rodrigo & Calegario, Cristina. (2019). *The General Law for Protecting Personal Data in Brazilian Enterprises: An Analysis of Multiple Cases*. 10. 89-99. DOI:<https://doi.org/10.14349/sumneg/2019.V10.N23.A2>.
- Peroni, S. A Simplified Agile Methodology for Ontology Development. In: DRAGONI, M.; POVEDA-VILLALÓN, M.; JIMENEZ-RUIZ, E. (Eds.). *OWL: Experiences and Directions – Reasoner Evaluation*. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. v. 10161p. 55–69.
- Rashid, S. M. et al. *The Semantic Data Dictionary – An Approach for Describing and Annotating Data*. NSL Data Intelligence, p. 443–486, 21 abr. 2020.
- Rantos, Konstantinos & Drosatos, George & Demertzis, Konstantinos & Ilioudis, Christos & Papanikolaou, Alexandros & Kritsas, Antonios. (2019). *ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology*. DOI:https://doi.org/10.1007/978-3-030-12942-2_23.
- União Europeia. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation) (2016), Disponível em <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC> . Acesso em 6 de julho de 2020.