em questão
E-ISSN 1808-5245

Discussões sobre política de privacidade de dados em um sistema de informação governamental

Milton Shintaku
Doutor em Ciência da Informação; coordenador de Articulação, Geração e Aplicação de Tecnologia do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), Brasília, DF, Brasil;
milton.shintaku@gmail.com; ORCID: http://orcid.org/0000-0002-6476-4953

Rosilene Paiva Marinho de Sousa
Doutora em Ciência da Informação; Professora do Centro das Humanidades da Universidade Federal do Oeste da Bahia, Barreiras, BA, Brasil;
rosilene.sousa@ufob.edu.br; ORCID: http://orcid.org/0000-0002-4699-8692

Lucas Rodrigues Costa
Doutorando pela Universidade de Brasília; Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), Brasília, DF, Brasil
lucasrc.rodri@gmail.com; ORCID: http://orcid.org/0000-0002-0973-4866

Rebeca dos Santos de Moura
Doutoranda em Geografia pela Universidade de Brasília; assistente de pesquisa no Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), Brasília, DF, Brasil;
bcasamo@gmail.com; ORCID: http://orcid.org/0000-0002-7685-8826

Diego José Macedo
Mestrando em Ciência da Informação pela UNB; Tecnologista do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), Brasília, DF, Brasil
diegojmacedo@gmail.com; ORCID: http://orcid.org/0000-0002-5696-0639

Resumo: A implementação de sistemas de informação exige esforços para condução e otimização, de forma cíclica, da operacionalização do tratamento e da recuperação de dados e informações, o que, muitas vezes, envolve dados pessoais. O papel das políticas de privacidade em sistemas de informação evidencia a exigência legal de proteção de dados pessoais. Este trabalho analisa a política de privacidade do site do Sistema Nacional de Juventude, como modelo oriundo da adaptação de um sistema de informação governamental, ao uso de identificação pessoal dos usuários por meio de mídias sociais. O modelo proposto atende ao direito de privacidade, em particular, à proteção de dados pessoais, buscando examinar aspectos gerais dos sistemas de informação e sua relação com a Ciência da Informação. Além disso, o trabalho discorre sobre privacidade e proteção de dados pessoais pelo poder público e apresenta o papel das políticas de privacidade nos sistemas de informação. Como metodologia, foi adotada uma pesquisa qualitativa alinhada a estudos da Ciência da Computação. Ao final, foram descritos os principais aspectos utilizados na adaptação do sistema de informação governamental, em particular, a política de privacidade do site mencionado, apresentando, como resultado, seu delineamento a fim de atender a Lei Geral de Proteção de Dados pessoais.

Palavras-chave: Sistemas de informação. Poder público. Política de privacidade. Proteção de dados pessoais.

1 Introdução

A utilização de computadores no governo é antiga e remonta à própria história da computação. Um dos primeiros computadores criados, o *UNIVersal Automatic Computer* - *UNIVAC* foi financiado pelo governo americano e usado, entre outras coisas, no censo daquele país, realizado em 1950. Entretanto, somente com o surgimento da Internet e, posteriormente, da Web, muitos serviços informatizados chegaram diretamente aos cidadãos, por meio do crescente uso da tecnologia pelo governo.

Serviços governamentais ofertados pela Internet e Web têm se tornado cada vez mais comuns, facilitando o atendimento ao cidadão. Mesmo que estes serviços ainda não sejam ofertados em todas as esferas, principalmente nos pequenos municípios, onde a tecnologia ainda não é tão difundida. Dessa forma, quanto à oferta de serviços públicos, no que tange ao uso da Tecnologia de Informação e Comunicação (TIC), apresenta-se o contexto de governo eletrônico (e-Gov), sendo esse uma forma de atendimento aos anseios por serviços governamentais.

Mesmo que possa ser considerado um acrônimo de *electronic Government*, o e-Gov pode ser traduzido como governo eletrônico, governo digital, governança eletrônica, entre outros, o que revela a grande abrangência de atendimento. Segundo Gronlund e Horan (2005), o e-Gov emergiu ainda no final dos anos 1990 nas discussões entre profissionais, passando à academia como um tópico de estudo que tem angariado interesse de várias áreas, visto que governo e tecnologia são temas interdisciplinares. Assim, e-Gov é uma prática, mas também um objeto de estudo científico, com eventos e periódicos voltados a discutir e disseminar conhecimentos. Como prática, discute-se ainda se o e-Gov trata de governo ou de governança, mas, como descrevem Guimarães e Medeiros (2005), o termo refere-se ao conjunto de ações do governo. Por meio das TICs, o governo oferece informações e serviços à população.

Alguns serviços governamentais requerem a identificação do usuário, incluindo número de documentos e outros, de forma a garantir a autenticidade, o que eleva as preocupações com a segurança e com a privacidade da informação

em meios digitais. A exemplo disso, o governo brasileiro sancionou a Lei n. 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018), já alterada pela Lei nº 13.853 de 08 de julho de 2019 (BRASIL, 2019b), revelando a importância do tema.

Muitos sistemas, incluindo alguns dos governamentais, oferecem a funcionalidade de autenticação por meio de redes sociais, como Facebook ou ferramentas do Google, haja vista a grande adesão brasileira a estas redes. Wangham *et al.* (2018), discutindo o futuro da identificação digital, descrevem a autenticação por meio de redes sociais como federativas, sendo uma tendência, inclusive na academia, como a rede Café, no âmbito de gestão de identidades. Entretanto, o uso dessas formas federalizadas de identificação pode comprometer a privacidade dos usuários. Quanto a isso, Breeding (2019) relata que dados pessoais captados pelo Facebook e pelo Google são repassados a outros sistemas, podendo ocasionar riscos à segurança.

Nesse contexto, revela-se a complexidade relacionada a sistemas de informação de governo, gestão de identidade e privacidade de dados pessoais, tema que requer estudos interdisciplinares envolvendo conhecimentos da ciência da informação, da informática, do direito, entre outras. O problema de pesquisa deste estudo surge a partir do seguinte questionamento: 'Como adaptar sistemas informatizados governamentais às tendências de identificação por mídias sociais mantendo a privacidade dos usuários?'

O objetivo do presente trabalho pode ser sintetizado pela descrição da criação de um modelo de adaptação de sistema de informação governamental ao uso de identificação de usuários por intermédio de mídias sociais, atendendo às questões de privacidade. Tal modelo foi aplicado ao Sistema Nacional de Juventude (SINAJUVE) e serve como base para atender a demanda de vários órgãos de governo que enfrentam o mesmo problema. Sua criação contribui para o debate sobre privacidade de dados e informações em sistemas governamentais e para o uso dessas tendências na gestão de identidade no ambiente digital.

As principais contribuições deste trabalho compreendem a apresentação de aspectos que envolvem os sistemas informacionais e sua colaboração com a Ciência da Informação, no processo de recuperação da informação. Também são

analisados aspectos da privacidade e da proteção de dados pessoais pelo poder público, destacando-se a carência de adequação ao tratamento de dados pessoais em face da sua necessidade de estrita legalidade para a atuação governamental. Por fim, descrevem-se os aspectos das políticas de privacidade em sistemas de informação e a sua adequação à LGPD.

2 Privacidade e proteção de dados pessoais pelo poder público em sistemas de informação

A necessidade de adequação ao tratamento de dados pessoais pelo poder público envolve a observância de aspectos legais da proteção à privacidade e à proteção aos dados pessoais. Inicialmente, pode-se dizer que o direito à privacidade, reconhecido como um direito autônomo da personalidade, retoma o contexto histórico do fim do século XIX, quando a revolução tecnológica trouxe consigo a preocupação das sociedades e dos ordenamentos jurídicos – em nível mundial – com a proteção de valores fundamentais da esfera privada (MARINELLI, 2019).

No Brasil, a Constituição Federal de 1988 refletiu essa preocupação ao garantir o direito à privacidade, incluindo-o no rol dos direitos fundamentais, e a expressa proteção à vida privada e à intimidade. Como desdobramentos desses direitos, acrescenta-se o direito à proteção de dados pessoais, regulamentado pela Lei Geral de Proteção de Dados, cujo objetivo consiste em proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Segundo Maldonado (2019, p. 216), "[...] a proteção dos dados pessoais é uma das facetas do conceito maior de privacidade, e que brotou e floresceu por decorrência do desenvolvimento tecnológico ocorrido nas últimas décadas.".

A proteção à privacidade envolve o controle sobre os dados pessoais, evidenciando-se o dever das instituições – sejam elas privadas ou públicas – de informar com clareza e transparência o que fazem com os referidos dados, que são reconhecidamente pertencentes aos usuários titulares. Nesse contexto, a necessidade de proteção da privacidade tem sido evidenciada em face da exposição a que os titulares de dados e informações são expostos, considerando

o aumento no volume da produção de dados e informações pessoais. Evidencia-se, portanto, a necessidade de controle dos referidos dados e informações, e o consequente estabelecimento de modelos de governança para o respectivo tratamento destes, visando proteger os direitos fundamentais.

Nesse sentido, segundo Marineli (2019, p. 111), "[...] considerando que a privacidade é um direito fundamental de personalidade, que atua a serviço da promoção da dignidade da pessoa humana, é possível concluir que todas as pessoas naturais, sem qualquer exceção, são titulares de tão relevante proteção.".

Os direitos dos titulares expressos na LGPD foram vinculados aos direitos fundamentais, com o objetivo de ampliar as garantias aos titulares dos dados pessoais, concedendo-lhes a devida importância (MALDONADO, 2019). O artigo 18 da LGPD especifica os referidos direitos, tais como: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos e desatualizados; anonimização; portabilidade; eliminação; informações sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informações sobre a possibilidade de não consentir e sobre as consequências da negativa, além da revogação do consentimento.

Segundo Sousa e Silva (2020, p. 11),

> A autodeterminação informativa constitui o direito do indivíduo de decidir, em princípio, sobre o uso de dados relacionados à sua pessoa. Em outras palavras, consiste no direito do indivíduo de decidir quem utiliza, para quem são repassados e com que finalidades, dados e informações pessoais são utilizados.

Assim, esses direitos reforçam o controle pessoal do titular sobre seus dados durante todo o processo de tratamento das operações envolvidas no ciclo de vida dos referidos dados.

Nesse cenário, os princípios constitucionais que orientam o exercício de atividades inerentes ao Poder Público, previstos no artigo 37 da Constituição Federal (BRASIL, 1988), legitimam sua atuação no estrito cumprimento da lei. Tasso (2019, p. 251) ratifica esse entendimento ao expor que "[...] a Administração Pública atua somente conforme o que a lei prevê e autoriza [...]". Diante desses aspectos, o uso de sistemas de informação pelo Poder Público

envolve uma complexidade de fatores relacionados à necessidade de governança de dados e informações de modo eficaz. No bojo dessa governança, os respectivos fluxos devem ser orientados para a tomada de decisão – seja ela dentro do próprio governo ou nas suas relações com os cidadãos – e, ao mesmo tempo, para o cumprimento da lei.

Na atualidade, conforme exposto em Tasso (2019, p. 258), a existência de diversas normas aplicadas a setores específicos (a exemplo da Lei n. 8.159/1991, sobre a política nacional de arquivos públicos e privados; da Lei do *Habeas Data*; da Lei do Processo Administrativo; do Decreto n. 6.135, de 26 de junho de 2007, que regulamenta o Cadastro Único para Programas Sociais; da Lei de Acesso à Informação, dentre outras), demanda do Poder Público regras de conformidade e delimita a atividade de tratamento de dados de acordo com os padrões exigidos para o atendimento de suas finalidades.

A LGPD surge como marco normativo de caráter geral, alinhando aspectos de proteção aos dados pessoais que necessitam ser resguardados a partir de sua vigência. Ainda segundo Tasso (2019, p. 246), "[...] é inerente à atividade administrativa a gestão de uma série de bancos de dados potencialmente sensíveis, sendo que a coleta e tratamento desses dados é um ponto nevrálgico em termos de políticas públicas que tenham escala." . O autor ainda esclarece que o reconhecimento desse aspecto resultou nas normas de dirigismo da LGPD, que devem ser observadas pelas instituições públicas, otimizando o seu atributo de transparência no tratamento de dados.

O tratamento de dados pessoais pelo Poder Público no âmbito da LGPD ficou instituído em seu capítulo IV, dos artigos 23 a 30. Em seu artigo 23, fica estabelecido como requisito para o tratamento desses dados o atendimento de uma finalidade pública, na persecução do interesse público, com o objetivo de executar ou cumprir as competências e as atribuições legais do serviço público. Esse requisito deve ser complementado pela previsão do artigo 7º, inciso III, que prevê a autorização de tratamento de dados pessoais para execução de políticas públicas. Isso significa que o atendimento de uma finalidade pública consiste na execução de ato administrativo indicado por lei, direcionado a políticas públicas previstas na norma. Por outro lado, a execução do interesse público pode ser

vista como preservação do interesse legítimo do titular em relação à observação de seus direitos e garantias fundamentais, considerando-se as necessidades da coletividade. A execução de competências legais está relacionada à atribuição de um dever legal da administração. Essas determinações constituem prerrogativas para que o tratamento de dados possa ser realizado pelo Poder Público, considerando as pessoas jurídicas de direito público referidas no artigo 1º da Lei de Acesso à Informação (BRASIL, 2011).

Diante das exigências legais, surge a necessidade de se criar um modelo de adaptação de sistema de informação governamental direcionado ao uso de identificação (login e cadastro) de usuários, por meio de mídias sociais de maior alcance (Facebook e Google), observados os aspectos da privacidade.

Desse modo, no tocante aos sistemas de informação governamental, faz-se necessário – além dos aspectos de desenvolvimento do próprio sistema e de segurança para o alinhamento desse com a proteção da privacidade – considerar as políticas de privacidade. Elas devem estar em conformidade com as normas e ações que as orientam, pois esses documentos constituem boas práticas de gestão, refletindo decisões advindas do planejamento e da implementação dos Sistemas de Informação.

3 Metodologia

O modelo proposto neste estudo apresenta uma abordagem qualitativa com alinhamento à metodologia relacionada a Ciência da Computação, pois, como defende Wazlawick (2014), há estudos na informática voltados à resolução de problemas, com características mais qualitativas e permitindo que se proponham melhorias, novas técnicas etc. Corrobora tal proposição a inexistência de coleta de dados estatísticos no estudo, mas não de fundamentação teórica na resolução do problema, com o desenvolvimento de soluções.

Dessa forma, o estudo é aplicado na medida em que atende a um problema real, que ocorre em órgãos de governo com serviços que necessitam de identificação específica ou que utilizam gestão de identificação. Além disso, o trabalho alinha métodos e padrões tradicionais da área de informática com estudos da ciência da informação. Em relação a gestão da informação, o modelo

proposto se baseou em estudos empíricos como os de Souza (2007). Finalmente, destaca-se a interdisciplinaridade da Ciência da Informação e a estreita relação com a Ciência da Computação. O modelo proposto foi dividido em seis etapas:

a) **Seleção de tecnologia para criação de portal:** Estudos voltados à criação do ambiente de estudo abrangente, conhecido na área e replicável;

b) **Seleção de redes sociais para gestão de identificação:** Estudos voltados à identificação e seleção das redes sociais utilizadas como gestoras de identificação;

c) **Desenvolvimento de política de privacidade:** Estudos voltados à criação de instrumentos para o desenvolvimento de políticas de privacidade;

d) **Implementação de login por meio de redes sociais**: Estudos voltados à aplicação prática de identificação no portal por gestão de identificadores;

e) **Ajustes no Portal para implementar política de privacidade:** Verificação de atendimento à política de privacidade;

f) **Avaliação de resultados:** Consolidação dos resultados de cada etapa e formulação do modelo.

A possibilidade de verificação dos resultados pela replicação dos estudos – muitas vezes dificultados pelas diferenças contextuais dos estudos humanos e sociais – permite a criação de modelos que podem ser ajustados aos novos ambientes. Estudos de caráter aplicado, como o presente trabalho, alinham-se ao modelo proposto por Bjork (2007), para quem o objetivo da ciência é gerar novos conhecimentos e melhorar a qualidade de vida.

4 Resultados

Sistemas governamentais que tratam dados pessoais precisam estar em consonância com a LGPD, atendendo às suas especificações. Por isso, eles requerem estudos que os avaliem, de forma a verificar a conformidade da aplicação da lei. Por exemplo, o Sistema Nacional de Juventude (SINAJUVE),

criado pelo Estatuto da Juventude, oferta um portal, sistema informatizado governamental, que trata dos dados pessoais por intermédio de um cadastro de usuários.

Segundo Costa, Moura e Oliveira (2020), a proposta do SINAJUVE é descentralizar as ações para a juventude, buscando a cooperação entre os entes federativos e incentivando a participação social na definição de diretrizes da atuação governamental para cidadãos nesta faixa etária. Como relatam Macedo *et al*. (2020), um dos objetivos do portal do SINAJUVE é estimular a interação entre os usuários do sistema e compartilhar as informações de interesse público, inclusive com a identificação de usuários por meio de mídias sociais.

Quanto ao desenvolvimento da política de privacidade do portal do SINAJUVE, fez-se necessário considerar aspectos legais presentes em normas que se relacionam entre si. Para isso, observou-se: a) o Marco Civil da Internet, por estabelecer a proteção à liberdade de tráfego de informações, abordando a provisão de conexão e de aplicações de Internet; b) a Lei Geral de Proteção de Dados Pessoais, por delinear aspectos sobre controle, acesso e tratamentos de dados e informações pessoais; c) o Decreto n. 10.046 de 2019, que dispõe sobre governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados; e d) o Regulamento Geral de Proteção de Dados (General Data Protection Regulation - GDPR), caso seja necessário estabelecer relações com países europeus para o desenvolvimento de políticas públicas.

Tendo em vista as particularidades apresentadas, a criação de uma política de privacidade para o portal do SINAJUVE envolveu adaptações nas suas tecnologias e aperfeiçoamento de aspectos relacionados à segurança da informação. Dessa forma, foram desenvolvidas medidas de segurança, tais como adoção de protocolo de tráfego de dados seguro e modificações na estrutura interna do código fonte do servidor. Elas estão em conformidade com as normas da política de privacidade, visando garantir os direitos fundamentais e a privacidade dos usuários do portal, e, por fim, atendendo às exigências de proteção aos dados pessoais estabelecidas pela Lei Geral de Proteção de Dados.

O portal foi desenvolvido em *WordPress*, um Sistema Gerenciador de Conteúdos – ou *Content Management System* (CMS) –, que é uma tecnologia específica e apropriada para a criação de sites. Segundo Clemente (2019), o *WordPress* é a ferramenta livre, atualmente em uso, com maior estabilidade, sendo adotada em vários portais ao redor do mundo e com diversos *plugins*, que são capazes de ampliar as funcionalidades básicas da ferramenta.

De acordo com Dwyer (2011), identificou-se que as redes sociais de mais alcance na sociedade brasileira são o Facebook e o Google. Dessa forma, elas foram selecionadas para login e cadastro de usuários no portal desenvolvido. Ambas as plataformas exigem algumas medidas de segurança web para permitir a integração da gestão de identificação, além da política de privacidade definida.

Estas imposições culminaram na implementação de medidas de segurança no desenvolvimento do portal, aqui elencadas: adoção do protocolo *HyperText Transfer Protocol Secure* (HTTPS), proteção do servidor web, maior blindagem nas funções executadas no portal e no desenvolvimento da política de privacidade em sistema de informação governamental. O protocolo de transferência de hipertexto seguro (HTTPS), pautado pela *Request for Comments* (RFC) 2660, adiciona princípios de segurança da informação ao tráfego de dados no portal, tais como confidencialidade, integridade e autenticação (RESCORLA; SCHIFFMAN, 1999, documento eletrônico).

Para a implementação do protocolo no portal adaptado, é necessário um par de chaves, uma pública e outra privada, utilizadas em todas as conexões dos usuários ao portal, de forma a garantir os requisitos de segurança. Além do protocolo HTTPs, deve-se certificar que o servidor não possibilite a indexação, ou seja, que motores de busca consigam acessar os arquivos sensíveis dos usuários e os tornem públicos para a Internet. Isso inibe o acesso não autorizado aos arquivos de que o servidor dispõe no site.

Para isso, foi utilizado o servidor web Apache (https://httpd.apache.org/), que é um *software open source*, multiplataforma e extremamente confiável. Suas funcionalidades padrão foram expandidas para atender aos requisitos do portal desenvolvido. Inclusive, foi desenvolvido um *plugin* para o *WordPress*

que utiliza o Apache para verificar e restringir o acesso aos arquivos submetidos ao portal somente para os usuários autorizados. Estes são os respectivos donos dos arquivos, além dos usuários com autorização privilegiada no portal.

Para maior segurança, as funções sensíveis contidas no portal que fazem CRUD – *Create* (Criação), *Read* (Consulta), *Update* (Atualização) e *Delete* (Destruição) – foram adequadas para serem realizadas por meio de requisições POST e GET, que são os principais métodos de comunicação do protocolo HTTPs (BENTO, 2014). Assim, somente usuários devidamente autorizados nas páginas corretas podem colocar em prática tais requisições.

No que se refere à política de privacidade em sistema de informação governamental, foi construída a política do site SINAJUVE, a qual descreve os aspectos de sua adequação às necessidades da LGPD, considerando o uso de tendências na gestão de identidade no ambiente digital. Esta política ficou estruturada conforme apresentada na Figura 1.

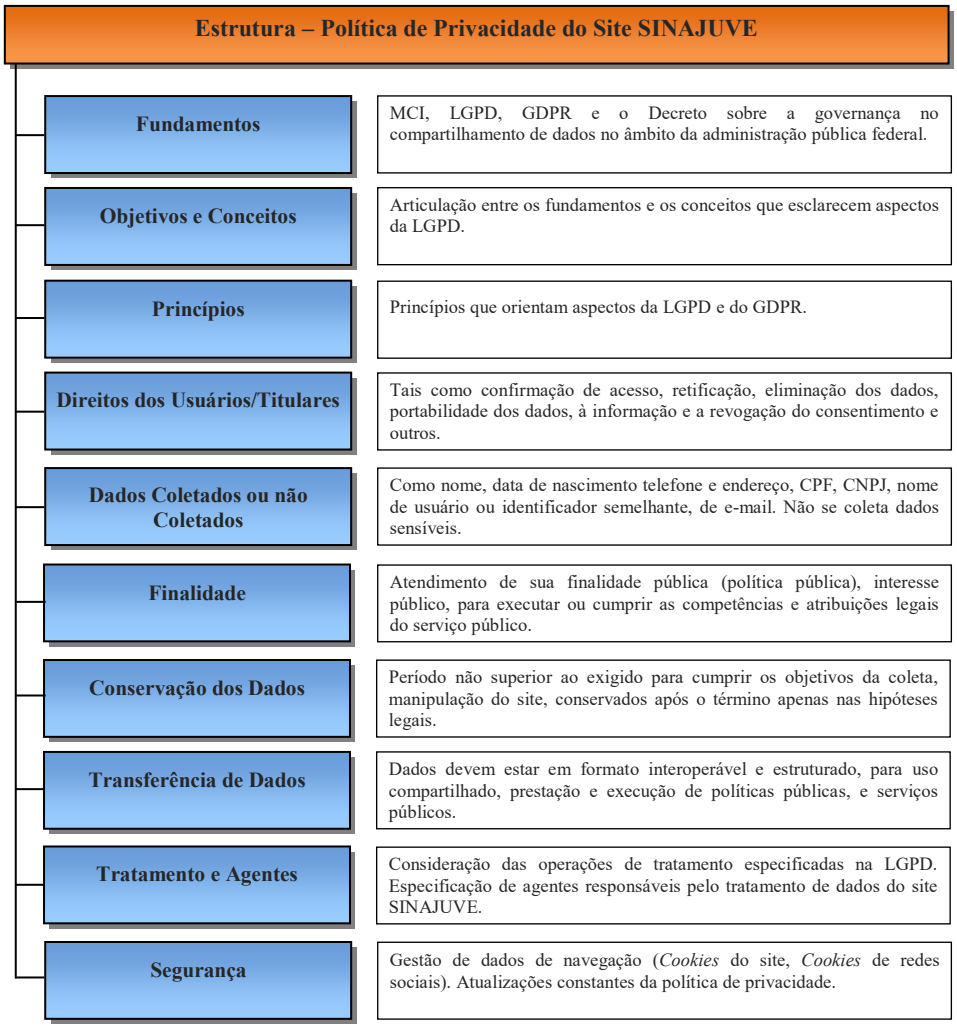

Figura 1 - Estrutura da Política de Privacidade do portal SINAJUVE.
Fonte: Elaborada pelos autores (2020).

Conforme Milagre e Santarém Segundo (2015, p. 51), "[...] compreender a proteção aplicável aos dados implica em conhecer previamente a natureza da informação que se pretende analisar, o que é papel da Ciência da Informação.". Os autores afirmam que, em face da grande quantidade de informações produzidas, torna-se necessária uma preocupação sobre como a informação está sendo tratada, de modo que se deve "[...] refletir sobre estas questões, pois a partir de tais reflexões poderemos em um futuro resolver problemas em relação a gerenciamento da informação, do seu ciclo de vida, privacidade, propriedade e segurança em geral." (MILAGRE; SANTARÉM SEGUNDO, 2015, p. 50).

Outrossim, o alinhamento à estrutura da política de privacidade adotada para o site SINAJUVE envolve a contribuição da Ciência da Informação no que se refere à gestão da informação, considerando o ciclo de vida dos dados, o

controle sobre seu tratamento, a privacidade e a segurança, para que o controle e a circulação dos mesmos ocorram de modo eficiente. Sousa e Silva (2020, p. 12) frisam que uma "[...] tomada de decisão focada no fluxo de dados e de informações torna-se capaz de refletir experiências que sejam passíveis de transformar as instituições e proporcionar a devida circulação e controle dos mesmos.". Seguindo esse entendimento, Sousa, Barrancos e Maia, (2019, p. 243) afirmam que, em relação à LGPD,

> [...] além de possibilitar a proteção da privacidade no uso da tecnologia, tem como uma de suas principais funções, proporcionar segurança para que informações pessoais possam circular adequadamente, ao buscar estabelecer várias instâncias de controle de forma responsável e tutelada, proporcionando meios claros e seguros para a sua proteção.

Para isso, tornou-se necessário considerar – além da contribuição da Ciência da Informação, como disciplina que estuda o comportamento e as propriedades da informação – proteção de dados pessoais como desdobramento do direito à privacidade, regulada pela LGPD, observando-se os requisitos previstos na referida lei. Segundo exposto por Siebra e Xavier (2020, p. 73), "[...] a privacidade é considerada um direito moral ou legal, está relacionada ao poder controlar suas próprias informações pessoais e exercer domínio perante o aproveitamento delas por terceiros.". Ainda segundo essas autoras,

> [...] a privacidade está ligada ao controle sobre a informação que lhe diz respeito. Se refere ao direito do indivíduo, grupo ou instituição controlar suas próprias informações e poder decidir quando, para quem e para que finalidade estas informações serão fornecidas. (SIEBRA; XAVIER, 2020, p. 72).

Desse modo, para a construção de uma política de privacidade da qual se possa extrair sua importância prática, é preciso observar, em todo o processo, os elementos relevantes da LGPD para sua elaboração, quaisquer que sejam: fundamentos, objetivos e conceitos, princípios, direitos dos usuários/titulares, dados coletados ou não, finalidade, conservação, transferência, tratamento, agentes e segurança dos dados. Quanto aos **Fundamentos** utilizados para o desenvolvimento da política de privacidade, referenciados na Figura 1, foram adotadas leis diretamente relacionadas à proteção da privacidade e dos dados

pessoais, tanto no âmbito nacional, como Marco Civil da Internet, Lei Geral de Proteção de Dados, Decreto n. 10.046 de 2019, quanto internacional, a exemplo do Regulamento Geral de Proteção de Dados Europeu (*General Data Protection Regulation* - GDPR), por ter sido tomado como modelo para a criação da LGPD.

Com relação aos **Objetivos** e **Conceitos** da estrutura, busca-se: a) esclarecer os interessados sobre os tipos de dados que são coletados, os motivos da coleta e forma como o usuário poderá atualizar, gerenciar ou solicitar a exclusão dessas informações, considerando as finalidades do processamento dos dados pessoais fornecidos; b) respeitar a autodeterminação informativa como fundamento da proteção de dados pessoais; e c) realizar o processamento necessário à execução de competências e atribuições legais do serviço público, bem como ajudar a tornar a visita ao site, pelo usuário/titular, a mais satisfatória possível, sucedendo de forma clara e segura. Além disso, no que concerne aos Conceitos, visa-se o esclarecimento de termos da LGPD e a compreensão do usuário/titular no momento de utilização do site do SINAJUVE, antes de o usuário fornecer seus dados para qualquer serviço de informação disponível.

Os **Princípios** orientam a aplicação da LGPD, de acordo com o GDPR, por estarem em consonância à proteção de dados pessoais. Considerou-se princípios tais como da boa-fé, licitude, lealdade e transparência, adequação, exatidão, integridade, confidencialidade, livre acesso, necessidade e responsabilização e prestação de contas.

São especificados os **Direitos dos Usuários/Titulares**, previstos na LGPD e na GDPR, envolvendo confirmação de acesso, retificação, eliminação, limitação do tratamento e portabilidade dos dados, bem como não submissão a decisões automatizadas, a informação e a revogação do consentimento.

Quanto aos **Dados Coletados**, a política de privacidade atende as exigências legais ao especificar, de forma clara, quais os referidos dados. Desse modo, indica-se que, para usuários "Assinantes do Portal", são coletados nome, sobrenome e e-mail; para usuários "Gestores de Unidade de Juventude", além dos dados de login, são coletadas informações a exemplo de CPF, sexo, cargo, escolaridade e telefone. Esses usuários também fornecem dados sobre as respectivas Unidades de Juventude, como endereço, telefone e documentos

necessários à adesão ao SINAJUVE. Com relação aos **Dados não Coletados**, a política esclarece que não se realiza coleta de dados sensíveis, ou seja, que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical do usuário, entre outros.

Quanto à **Finalidade** da coleta, fica estabelecido, como requisito para tratamento dos dados, o atendimento a uma finalidade pública, na persecução do interesse público, que corresponde ao desenvolvimento de políticas públicas pelo Sistema Nacional de Juventude. Desse modo, os dados pessoais do usuário coletados pelo site têm a finalidade de facilitar, agilizar e cumprir os compromissos estabelecidos pelo poder público com aquele usuário e de fazer cumprir as solicitações realizadas por meio do preenchimento de formulários.

Concernente à **Conservação dos Dados** pessoais dos usuários/titulares, fica esclarecido, na política de privacidade, que eles serão conservados por um período não superior ao exigido para cumprir os objetivos em razão dos quais são processados e, além disso, por um período necessário a correta manipulação do site, podendo ser conservados após o término de seu tratamento nas hipóteses previstas na LGPD.

A política de privacidade esclarece que a **Transferência de Dados** deve estar em formato interoperável e estruturado para uso compartilhado, prestação e execução de políticas públicas e serviços públicos. Em relação ao tratamento dos dados e aos agentes responsáveis, deve-se considerar as operações de tratamento especificadas na LGPD. A política apresenta ainda a especificação de agentes responsáveis pelo tratamento de dados do portal SINAJUVE.

No que diz respeito à **Segurança**, a política prevê a adoção de soluções que levem em consideração as técnicas adequadas, os custos de aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e as liberdades do usuário.

Mesmo seguindo a estrutura da Figura 1, uma política de privacidade pode sofrer atualizações constantes, revelando a importância do usuário/titular em consultar periodicamente o site para verificar as atualizações realizadas. Ainda deve-se observar a inclusão de materiais de terceiros em produtos, conteúdos e serviços disponíveis no portal, uma vez que links de terceiros nesse

ambiente podem direcionar o usuário para sites que não estão vinculados à Política de Privacidade em questão. Assim, é necessário deixar claro que os usuários/titulares devem revisar cuidadosamente as políticas e práticas de terceiros e atentar para as condições estabelecidas nas políticas de privacidade específicas antes de fornecer qualquer dado pessoal.

A aplicação da estrutura apresentada na Figura 1 e as medidas de segurança implementadas no portal constituem o modelo proposto para adaptação de um sistema de informação governamental ao uso de identificação de usuários por meio de seus cadastros em mídias sociais.

5 Considerações finais

Este trabalho apresenta um estudo empírico, que pode ser replicado, com pequenos ajustes, e presumivelmente com resultados semelhantes, visto que o modelo apresentado segue o padrão de portais para divulgação de informação e cadastro de usuários com uso de um Sistema Gerenciador de Conteúdos (CMS).

O Portal do Sistema Nacional de Juventude (SINAJUVE) é um ambiente que possibilita a imersão dos usuários no panorama brasileiro das políticas públicas de juventude. Esse portal fornece informações sobre a formulação, a implementação, o acompanhamento, a avaliação e o controle das políticas públicas de juventude para qualquer usuário que tenha interesse no tema, além de facilitar a divulgação de programas para a juventude.

Foi identificado que as redes sociais de maior alcance na sociedade brasileira são Facebook e Google, de modo que elas foram escolhidas para login e cadastro de usuários no portal do SINAJUVE. Além disso, por serem muito difundidas, a implementação da gestão de identificação entre essas plataformas e o CMS utilizado é de fácil desenvolvimento.

Enfatiza-se que o portal SINAJUVE foi desenvolvido considerando os aspectos de segurança da informação, alinhando-se sempre à necessidade de proteção da privacidade do usuário/titular dos dados.

Tornou-se possível realizar a articulação do desenvolvimento do sistema para uso de identificação (login e cadastro) de usuários, por meio de mídias sociais com uma política de privacidade que permite o acesso do usuário, de

forma clara e específica, a informações sobre quais dados pessoais são coletados, como eles são utilizados, quem necessita utilizá-los, que uso será dado aos mesmos e quais as consequências dessa utilização.

No que se refere à política de privacidade desenvolvida para o portal do SINAJUVE, embora não seja explícita na lei brasileira uma padronização de sua estrutura, buscou-se atender aos aspectos relevantes das principais normativas acerca do tema (MCI, LGPD e GDPR), considerando elementos necessários ao cumprimento dos direitos e deveres impostos nas normas e visando garantir a proteção de dados pessoais de seus usuários/titulares.

Referências

BENTO, E. J. **Desenvolvimento web com PHP e MySQL**. [*S. l.*: *s. n.*], 2014. Disponível em: https://dev.medialab.ufg.br/tainacan/wp-content/themes/tainacan/libraries/js/pdfThumb/pdfJS/web/viewer.html?file=https://dev.medialab.ufg.br/tainacan/wp-content/uploads/sites/5/2018/01/Desenvolvimento-web-com-PHP-e-MySQL-Casa-do-Codigo.pdf. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011 [Lei de Acesso à Informação]**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 [Lei Geral de Proteção de Dados Pessoais (LGPD)]**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 14 set. 2020.

BREEDING, M. Key Technologies with Implications for Privacy: Encryption, Analytics, and Advertising Tracking. *In*: BREEDING, M. **Protecting Privacy on Library Websites:** Critical Technologies and Implementation Trends. [*S. l.*: *s. n.*], 2019. v. 55, p. 8–16.

CLEMENTE, M. **O que é WordPress, para que serve e principais segredos desvendados**. 1 fev. 2019. RockContent. Disponível em: https://rockcontent.com/br/blog/wordpress/. Acesso em: 14 set. 2020.

COSTA, L.; MOURA, R.; OLIVEIRA, F. Guia prático de adesão ao Sinajuve. *In*: MILTON, SHINTAKU; LOZZI, MARIANA (orgs.). **Sistema Nacional de Juventude explicado**. Brasília: Ibict, 2020. p. 42–80. DOI 10.22477/9786588137284.cap4. Disponível em: https://bibliotecadigital.mdh.gov.br/jspui/handle/192/1365. Acesso em: 2 set. 2020.

DWYER, C. Privacy in the Age of Google and Facebook. **IEEE Technology and Society Magazine**, v. 30, n. 3, p. 58–63, 2011. DOI 10.1109/MTS.2011.942309. Disponível em: http://ieeexplore.ieee.org/document/6017276/. Acesso em: 14 set. 2020.

GUIMARÃES, T. de A.; MEDEIROS, P. H. R. A relação entre governo eletrônico e governança eletrônica no governo federal brasileiro. **Cadernos EBAPE.BR**, v. 3, n. 4, p. 01–18, dez. 2005. DOI 10.1590/S1679-39512005000400004. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1679-39512005000400004&lng=pt&tlng=pt. Acesso em: 14 set. 2020.

MALDONADO, V. N. Dos direitos do titular. *In*: MALDONADO, V. N.; BLUM, R. O. (orgs.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 215–242.

MARINELLI, M. R. **Privacidade e Redes Sociais Virtuais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MILAGRE, J.; SANTARÉM SEGUNDO, J. E. A propriedade dos dados e a privacidade na perspectiva da Ciência da Informação. **Encontros Bibli**: revista eletrônica de biblioteconomia e ciência da informação, v. 20, n. 43, p. 47-76, mai./ago., 2015. Disponível em: https://brapci.inf.br/index.php/res/download/48687. Acesso em: 22 mar. 2021.

RESCORLA, E.; SCHIFFMAN, A. **The Secure HyperText Transfer Protocol**, n. RFC2660. [*S. l.*]: RFC Editor, ago. 1999. DOI 10.17487/rfc2660. Disponível em: https://www.rfc-editor.org/info/rfc2660. Acesso em: 14 set. 2020.

SIEBRA, S. A.; XAVIER, G. A. C. Políticas de Privacidade da Informação: caracterização e avaliação. **Biblos**: Revista do Instituto de Ciências Humanas e da Informação, Rio Grande. v. 34, n. 02, p. 72-88, jul./dez. 2020. Disponível em: https://www.seer.furg.br/biblos/article/view/11870/8428. Acesso em: 22 mar. 2021.

SOUSA, R. P. M; BARRANCOS, J. E.; MAIA, M. E. Acesso à informação e ao tratamento de dados pessoais pelo Poder Público. **Informação & Sociedade**: Estudos, v. 29, n. 1, 27 mar. 2019. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/44485. Acesso em: 22 mar. 2021.

SOUSA, R. P. M.; SILVA, P. H. T. Proteção de Dados Pessoais e os Contornos da Autodeterminação Informativa. Revista **Informação & Sociedade**: Estudos. João Pessoa, v.30, n.2, p. 1-19, abr./jun. 2020. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483. Acesso em: 22 mar. 2021.

SOUZA, F. D. C. de. As possibilidades pedagógicas no ensino de metodologia da pesquisa científica em ciência da informação e os objetos deste campo científico: aproximações durkheimianas. **Encontros Bibli:** revista eletrônica de biblioteconomia e ciência da informação, v. 8, n. 16, p. 20–40, 5 nov. 2007. DOI 10.5007/1518-2924.2003v8n16p20. Disponível em: http://www.periodicos.ufsc.br/index.php/eb/article/view/103. Acesso em: 14 set. 2020.

TASSO, F. A. Do Tratamento de Dados Pessoais pelo Poder Público. *In*: MALDONADO, V. N.; BLUM, R. O. (orgs.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 245–288.

WANGHAM, M. S.; MARINS, A.; FERRAZ, C. A. G.; SILVA, C. E. da; SAADE, D. C. M.; SILVA, E. F.; MELLO, E. R. de; OLIVEIRA, F. B. de; SEIXAS, F. L.; OLIVEIRA, L. B.; LOPES, M.; HENRIQUES, M. O futuro da gestão de identidades digitais. *In*: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 2018., event-place: Natal. **Anais Estendidos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais** [...]. Porto Alegre, RS, Brasil: SBC, 2018. p. 146–166. Disponível em: https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/4152. Acesso em: 14 set. 2020.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. 2. ed. Rio de Janeiro: Elsevier, 2014. Disponível em: http://www.sciencedirect.com/science/book/9788535277821. Acesso em: 14 set. 2020.

Discussions on data privacy policy in a government information system

Abstract: The implementation of information systems requires efforts to conduct and optimize, cyclically, the operationalization of the processing and retrieval of data and information, which often involves personal data. The role of privacy policies in information systems highlights the legal requirement to protect personal data. This paper analyses the privacy policy of the Sistema Nacional de Juventude website, as a model derived from the adaptation of a government information system to the use of personal identification of users through social media. The proposed model complies with the right to privacy, in particular, the protection of personal data seeking to examine general aspects of information systems and their relationship with Information Science. In addition, the paper discusses privacy and protection of personal data by the government and presents the role of privacy policies in information systems. As a methodology, a qualitative research was adopted in line with Computer Science studies. Finally, the main aspects used in the adaptation of the governmental information system were described, in particular, the privacy policy of the mentioned website, presenting as a result its design aiming to comply with the General Data Protection Law of personal information.

Keywords: Information Systems. Public Power. Privacy Policy. Data Protection of Personal Information.

Recebido: 19/09/2020

Aceito: 06/04/2021

Declaração de autoria

Concepção e elaboração do estudo: Milton Shintaku, Rosilene Paiva Marinho de Sousa, Lucas Rodrigues Costa, Rebeca dos Santos de Moura, Diego José Macedo.
Coleta de dados: Milton Shintaku, Rosilene Paiva Marinho de Sousa, Lucas Rodrigues Costa, Rebeca dos Santos de Moura, Diego José Macedo.
Análise e interpretação de dados: Milton Shintaku, Rosilene Paiva Marinho de Sousa, Lucas Rodrigues Costa, Rebeca dos Santos de Moura, Diego José Macedo.
Redação: Milton Shintaku, Rosilene Paiva Marinho de Sousa, Lucas Rodrigues Costa, Rebeca dos Santos de Moura, Diego José Macedo.
Revisão crítica do manuscrito: Milton Shintaku, Rosilene Paiva Marinho de Sousa, Lucas Rodrigues Costa, Rebeca dos Santos de Moura, Diego José Macedo.

Como citar

SHINTAKU, Milton; SOUSA, Rosilene Paiva Marinho de; COSTA, Lucas Rodrigues; MOURA, Rebeca dos Santos de; MACEDO, Diego José. Discussões sobre política de privacidade de dados em um sistema de informação governamental**. Em Questão**, Porto Alegre, v. 27, n. 4, p 39-60. 2021. DOI: http://doi.org/10.19132/1808-5245274.39-60