OS IMPACTOS DA PUBLICAÇÃO DE DADOS DE AGENTES PÚBLICOS PARA A SEGURANÇA NACIONAL E SEGURANÇA PÚBLICA

Impacts of Agents Data Publication of public safety and national public security

Alcimar Sanches Rangel (1), Jorge Henrique Cabral Fernandes (2)

(1) Universidade de Brasília, Brasil, asrangel@gmail.com. (2) jhcf@unb.br.

Resumo

O presente artigo analisa os fatores de riscos expostos na comunicação entre o governo e a sociedade a partir da publicação dos dados e informações de agentes da administração pública federal (APF) que atuam na segurança nacional e segurança pública. Trata-se de recorte de investigação realizada no curso de Mestrado, que se utilizou de uma pesquisa exploratória e qualitativa por meio de investigação nos portais da *internet* que promovem a transparência pública. A pesquisa está inserida na perspectiva interdisciplinar da Ciência da Informação (CI), pois também, aborda os campos de estudo da Computação e do Direito. Participaram da investigação sete agentes públicos que atuam nas atividades relativas à segurança nacional e vinte e sete que atuam na segurança pública. O estudo revelou a facilidade de obtenção de dados pessoais por qualquer pessoa, utilizando o método proposto no estudo, que não requer o emprego de ferramentas automatizadas. Os resultados apresentados são preocupantes e demonstram a fragilidade do Estado brasileiro com a publicação de dados pessoais dos seus agentes públicos e a inexistência de orientações que estabeleça regras claras e objetivas sobre publicação de dados pessoais nos diversos portais de governo que promovem a transparência pública.

Palavras-chave: Publicidade; Transparência; Privacidade; Segurança da Informação; Classificação; Acesso à Informação.

Abstract

This article analyzes the risk factors set out in the communication between the government and society from the publication of data and information agents of the federal public administration (APF) working in national security and public safety. It is cut research conducted in the course of Master, which was used in an exploratory and qualitative research through research in the internet portals that promote public transparency. The research is inserted in interdisciplinary perspective of Information Science (CI), it also addresses the fields of study of Computation and Law. Participated in the investigation seven public workers involved in activities relating to national and twenty-seven who work in public safety security. The study revealed the ease of obtaining personal data by any person using the method proposed in the study, which does not require the use of automated tools. The results are worrisome and demonstrate the fragility of the Brazilian state with the publication of personal data of its public officials, and the lack of guidelines setting out clear and objective rules on publication of personal data in the various portals of government to promote public transparency.

Keywords: Publicity; Transparency; Privacy; Information Security; Classification; Access to Information.

1 Introdução

À medida que os países democráticos tendem a ampliar a relação entre governo e cidadão por meio da publicidade e transparência de seus atos, observa-se uma explosão informacional em decorrência dessa comunicação, principalmente, com uso da Tecnologia da Informação (TI) associada à *internet*.

No Brasil, são inúmeras iniciativas que confirmam essa tendência, principalmente, aquelas impostas por leis e orientações normativas, como por exemplo, a Lei de Acesso à Informação (LAI), que determina o uso da *internet* para a divulgação de informações produzidas e custodiadas pelos órgãos públicos, cujo interesse seja de caráter coletivo (Brasil, 2011).

Atualmente é possível obter várias informações sobre gastos públicos, processos judiciais, eleitorais, trabalhistas; resultados de auditorias diretamente da

internet. As publicações de tais informações são de responsabilidade de diversos órgãos, pertencentes a diferentes poderes e esferas governamentais. Tal fato, além de revelar a possibilidade de inconsistência dos dados, pode também caracterizar o indevido tratamento da informação, principalmente no que concerne à Segurança da Informação (SI).

Na ânsia do cumprimento do dever em prol da transparência, aspectos da SI podem ser desconsiderados. Nesse sentido, é preciso encontrar um equilíbrio entre o que é transparente e o que é seguro. Para auxiliar nessa harmonização, o uso da tecnologia pode oferecer excelentes soluções para a organização de grandes volumes de documentos dos órgãos públicos (Robredo, 2003).

Por outro lado, o uso da tecnologia interligada às redes pode oferecer riscos à informação e isto porque são inúmeras as ameaças do mundo virtual responsáveis por incidentes de segurança. De acordo com o Gabinete de Segurança Institucional da Presidência da República (GSI-PR), estes incidentes são eventos adversos relacionados à segurança dos sistemas computacionais ou das redes de computadores (GSI-PR, 2009, p. 3).

No entanto, independente da presença das possíveis ameaças que assombram o mundo cibernético, acredita-se que é de suma importância o desenvolvimento e ampliação de estudos voltados para a análise dos dados e informações divulgados pelo governo brasileiro na *internet*, a fim de verificar se há indícios de divulgação de vulnerabilidades que afetam a SI do Estado ou da sociedade.

Sendo assim, o objetivo principal deste artigo é apresentar os resultados de uma pesquisa exploratória e qualitativa, por meio de investigação nos portais da internet que promovem a transparência pública, a fim de identificar os fatores de risco que impactam a privacidade dos agentes públicos investigados, e consequentemente os riscos gerados à segurança nacional e à segurança pública federal decorrentes da exploração dessa informação.

2 Os direitos e garantias fundamentais para o acesso à informação

Para esta pesquisa, a expressão "acesso à informação" está relacionada ao efeito positivo do cumprimento da transparência pública. Para Jardim (2009), a noção de acesso à informação está presente nas diversas reflexões teóricas encontradas na Arquivologia, Biblioteconomia, Documentação e Ciência da Informação, como também, em outras áreas correlatas.

De acordo com a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), o acesso à informação é de suma importância para o desenvolvimento social do cidadão, tornando-o capaz de fazer melhores escolhas, bem como, compartilhar riquezas com os demais indivíduos da sociedade, que na visão marxista não se restringe apenas ao valor material das coisas, inclui-se principalmente a riqueza das relações humanas (UNESCO, 2014).

Sendo assim, exige-se cada vez mais dos profissionais da CI, pois estes são os elementos fundamentais para a garantia do livre acesso às informações essenciais para a sociedade atual e do futuro.

Existe uma relação direta entre o direito fundamental de acesso à informação com o princípio da publicidade. Por essa razão torna-se imprescindível a adoção de medidas voltadas a facilitar o acesso à informação para que haja a concretização do princípio da publicidade.

Indiscutivelmente, o uso de novas tecnologias associado à publicação de diversos atos administrativos vêm contribuindo para o cumprimento do princípio da publicidade (Rocha, 1994, p. 246). Atualmente, os órgãos públicos são dotados de poderosos bancos de dados que, além de possibilitar ao cidadão diversos tipos de consulta, emitem certidões e documentos, que no passado, requeriam custos e longo período de espera. O uso da *internet* para prestação de serviços públicos reduziu custos à administração pública, oferecendo considerável economia aos cofres públicos.

A disponibilização das edições dos diários oficiais dos diversos Poderes e esferas públicas em forma eletrônica na *internet* é um exemplo de medida voltada a facilitar o acesso à informação ao cidadão. No Diário Oficial da União (DOU), por exemplo, são publicados diversos atos de interesse do cidadão, que inclui desde nomeações e exonerações de agentes públicos, a publicação de atos normativos aprovados e sancionados pela União.

Notoriamente, os meios eletrônicos, em especial a *internet*, são as formas mais eficazes para publicação das informações públicas e o melhor caminho para a democratização do acesso às informações. No entanto, requer de cuidados especiais, visto o grande volume de dados e informações que estão armazenados em robustos bancos de dados dos governos.

No mesmo momento em que avançam as medidas para concretização do princípio da publicidade, verifica-se a necessidade de proteção da grande quantidade de informações disponível. Com isso, desenvolveu-se uma nova cultura de proteção para o desconhecido mundo virtual, e em consequência, foram produzidas inúmeras orientações normativas relativas a SI, especificamente para atender às exceções de sigilos impostas pela própria Constituição Federal, concluindo-se que o princípio da publicidade não é absoluto.

As formas de aplicação do princípio da publicidade são de responsabilidades dos órgãos governamentais dos diferentes Poderes e esferas administrativas. Estes possuem liberdade para execução e regulamentação, em

conformidade com as Leis vigentes, acima de tudo no que tange à publicação de dados pessoais. As consequências dessa liberdade são as diferentes formas de tratamento da informação e falta de padronização efetuada pelos órgãos de transparência pública. Sendo assim, o princípio da publicidade, na vertente pública, deve ser tratado de forma igualitária, a fim de evitar distorções e quebra de SI durante a divulgação de dados sensíveis e não públicos.

Atualmente, há uma discussão sobre a publicação das informações atinentes aos servidores públicos, como por exemplo, sua remuneração e seus dados cadastrais. A Controladoria-Geral da União (CGU) afirma que a divulgação da remuneração dos servidores da administração pública federal (APF) não viola o direito de privacidade e que tal ação garante a transparência dos gastos públicos previsto na LAI. O Superior Tribunal Federal (STF) também interpreta dessa forma, visto que, quando se discute a legalidade da publicação de informações funcionais e remunerações dos servidores públicos não há interferência na vida privada e nem na intimidade. Entretanto, o próprio STF alerta sobre os riscos gerados tanto para o servidor público, como para sua família com tais divulgações, que somente serão atenuados com a proibição da divulgação do Cadastro de Pessoas Físicas (CPF), endereço residencial e carteira de identidade.

> Não cabe falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo 'nessa qualidade' (§6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. (STF, 2011).

Fica assim evidenciado que há divergências entre a decisão tomada pelo STF (2011) com as publicações do governo sobre informações dos servidores públicos, pois, a publicação do CPF tornou-se uma prática usual em diversos portais do governo federal.

São muitos os desafios para preservar a privacidade de uma pessoa diante do ambiente virtual que é a *internet*. A exposição de informações pessoais está além dos prejuízos que afetam a reputação e a dignidade da pessoa, há questões relativas à segurança que pode impactar o titular dos dados, a sua família e se tratando de um agente público, pode impactar a organização em que este trabalha.

Frente às ameaças virtuais, o Brasil disciplinou o uso da *internet* na Lei nº 12.965 de 2014, também conhecida como Marco Civil da *Internet* (Brasil, 2014). Esta Lei objetiva o direito de acesso à *internet* a todos os cidadãos e o acesso à informação, fortalecendo o princípio da publicidade, por outro lado, inclui o direito da inviolabilidade da intimidade e da vida privada, fortalecendo assim o princípio da privacidade.

Para tal, torna-se imprescindível identificar se um determinado dado, ao ser divulgado, é pessoal ou não, e se essa divulgação pode afetar a privacidade ou vida do indivíduo. Diante desse problema, o Reino Unido publicou em 1998, uma orientação normativa conhecida como *Data Protection Act* (DPA) que visa estabelecer passos, formulados em oito perguntas, que determinam se um dado é de caráter pessoal (DPA, 1998).

Atualmente, o principal motivo que leva à erosão da privacidade é o forte interesse por informações pessoais. O Estado, no cumprimento do seu dever perante a sociedade, necessita de diversas informações dos cidadãos. Isso faz com que ele se torne um dos principais agressores do direito à privacidade. Entretanto, a erosão da privacidade está além da ingerência do Estado na vida da pessoa, pois na lista de agressores estão incluídas as empresas privadas, a sociedade e os próprios indivíduos titulares dos dados pessoais (Vidal, 2010).

3 A segurança da informação

Os normativos da Associação Brasileira de Normas Técnicas (ABNT) consideram que a SI é feita por ações que visam, principalmente, a preservação das propriedades de confidencialidade, de integridade e de disponibilidade das informações. O Governo Federal incorporou tais propriedades em seus normativos, porém, incluiu a preservação da autenticidade, que segundo Simião (2009, p. 61) é de suma importância no impacto dos processos de comunicações. Nesse sentido, para a APF surgiu uma nova denominação: gestão de Segurança da Informação e Comunicações (SIC).

> Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações. (GSI-PR, 2008, p. 2).

Para Rangel (2010, p. 38) houve um incremento da gestão de SI para a gestão de SIC, "muito em função dos avanços das tecnologias da informação e comunicação (TIC) e da interdependência e interconexão dos sistemas e redes de informação", consequentemente, aumentou-se a probabilidade da presença de ações adversas que inviabilizam a SIC, sendo que tais ações ou, até mesmo omissões, podem ser feitas de forma intencional ou acidental, e o resultado disso, de acordo com o GSI-PR (2008, p.2) é definido como quebra de segurança. Isso significa que uma ou mais propriedades da SIC –

disponibilidade, integridade, confidencialidade e autenticidade – foram comprometidas, e para evitar a quebra de segurança é preciso tratar a informação, assegurando essas propriedades em todo seu ciclo de vida (GSI-PR, 2014, p. 3).

O GSI-PR (2008, p.2) define disponibilidade como a "propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade"; já a LAI entende que disponibilidade é a "qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados" (Brasil, 2011).

Para garantir a disponibilidade das informações, é preciso "uma série de ações ou de boas práticas", como por exemplo, "o uso de backups; cópias de segurança; redundância de sistemas e eficácia no controle de acesso" (Simião, 2009, p. 54). Esta propriedade tornou-se o foco das atenções dos gestores de SI, pois, além dela contribuir com a transparência e o bom serviço prestado ao público (Simião, 2009, p. 55), a disponibilidade está diretamente relacionada com a observância da publicidade como preceito geral determinada pela LAI.

Também é preciso manter a integridade das informações disponibilizadas pelos órgãos da APF, ou seja, garantir que elas não sejam modificadas, nem destruídas de maneira não autorizada ou acidental (GSI-PR, 2008, p. 2).

Os controles de segurança necessários para a manutenção da integridade da informação não se limitam apenas aos controles lógicos das informações digitais. Também, é preciso manter a proteção dos documentos armazenados em suportes físicos. A Lei nº 8.159 de 1991, que dispõe sobre a política nacional de arquivos públicos e privados, determina que "é dever do Poder Público a gestão documental e o a proteção especial a documentos de arquivos". Esta proteção refere-se principalmente aos aspectos da preservação dos documentos que futuramente servirão "como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação" (Brasil, 1991). A LAI também menciona que "quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original" (Brasil, 2011).

Como visto, a disponibilidade e a integridade das informações são propriedades que fortalecem o princípio da publicidade e da transparência pública, no entanto, é preciso saber se tais informações são autênticas. Segundo a LAI e o GSI-PR, o conceito de autenticidade está relacionado à qualidade ou à propriedade da informação que tenha sido produzida, expedida, recebida ou modificada por pessoas, organizações ou sistemas (Brasil, 2011; GSI-PR, 2008, p. 2). Entretanto, tais conceitos não mencionam se essas pessoas, organizações ou sistemas são realmente as que deveriam ser. As considerações do Conselho Internacional de Arquivos (CIA) são mais coerentes ao afirmar que "para mostrar que um documento de arquivo é autêntico apenas é necessário provar que é o que afirma ser" (CIA, 2005, p.42).

Outra propriedade da informação a ser considerada no contexto da SI é a confidencialidade. No atual cenário em que o sigilo tornou-se uma exceção no governo federal, os legisladores resolveram não citar a confidencialidade das informações na LAI. O fato da retirada do sigilo "confidencial" nas normas do governo, não justifica a sua omissão na LAI, houve um falso entendimento ao associar confidencialidade e confidencial, o que já previa Simião (2009, p. 58):

> A confidencialidade, na maioria das vezes, é apresentada sob enfoque de sigilo, o que não deixa de estar correto, porém existe outro aspecto a considerar que é a ética de preservar ou guardar uma informação nem sempre classificada como sigilosa. Isto significa que nem sempre a informação tenha de receber um grau de sigilo para justificar a necessidade de medidas de proteção. (Simião, 2009, p.58).

Os normativos do GSI-PR não desprezaram a importância dessa propriedade, considerando-a de suma importância para a segurança do Estado e da sociedade e com isso, definiu-se que confidencialidade é a "propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado" (GSI-PR, 2008, p. 2).

Assim como as propriedades da disponibilidade, integridade e autenticidade possuem uma forte relação com o amplo acesso à informação, a propriedade da confidencialidade tem com as restrições de acesso. Contudo, para que seja realizado o adequado tratamento da informação é preciso considerar a presença de todas as propriedades nos diversos tipos de informação, quer sejam ostensivas, sigilosas e pessoais.

Enquanto o Projeto de Lei (PL) que dispõe sobre a proteção de dados pessoais e da privacidade não é aprovado, o cidadão fica exposto aos diversos riscos de SI. Os órgãos de governo responsáveis pelos portais e canais que promovem a transparência pública devem entender que tratar com dados pessoais é uma atividade de risco, pois pode causar danos e impactos de ordem patrimonial, moral e física ao cidadão, e consequentemente, responderão perante a Lei com obrigações de ressarcimento do dano gerado (Brasil, 2015).

4 Procedimentos metodológicos

O ato de verificar possibilidades ou hipóteses da quebra de SI durante a divulgação de dados e informações nos portais da *internet* do governo federal e torná-las explícitas, caracteriza esta pesquisa como exploratória

(Gil, 2002, p.41), pois "busca-se descobrir se existe ou não um fenômeno" (Matias-Pereira, 2007, p. 48), a fim de elucidá-lo ou explicar aquilo que ainda não é aceito apesar de ser evidente (Oliveira Netto, 2006, p. 9). Quanto à natureza, esta pesquisa é classificada como aplicada, pois envolve verdades e busca produzir conhecimentos para aplicação prática sobre a SI (Cervo; Bervian, 1983).

A partir dos dados obtidos na *internet*, é possível construir informações e conhecimentos que permeiam os paradigmas da CI apresentados por Capurro e Hjørland (2007), considerando que os dados e informações dos agentes públicos pesquisados estão inseridos no campo social, as informações do ambiente tecnológico da organização no campo físico, e por fim, o conhecimento gerado a partir dos dados e informações expostos pela organização, no campo cognitivo.

4.1 Ambiente de pesquisa

Para Meirelles (1998, p. 65) a "administração pública é todo o aparelhamento do Estado, preordenado à realização de seus serviços, visando à satisfação das necessidades coletivas", no entanto, as atividades executadas no ambiente da administração pública de quaisquer Poderes da União, dos Estados, do Distrito Federal e dos Municípios devem ser reguladas em conformidade com a Constituição Federal, principalmente em obediência aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Os indivíduos investigados na presente pesquisa pertencem ao quadro dos órgãos da APF responsáveis pela segurança nacional e segurança pública, entretanto o fato de existirem dados e informações pessoais desses agentes em outras esferas administrativas, o ambiente pesquisado inclui outros portais da *internet* de órgãos pertencentes aos demais Poderes da União, dos Estados e do Distrito Federal.

As atividades de segurança nacional são aquelas destinadas a combater crimes que venham lesar ou expor o perigo de lesão: a) a integridade territorial e a soberania do Estado; b) o regime representativo e democrático, a Federação e o Estado de Direito; e c) a pessoa dos chefes dos Poderes da União (Brasil; 1983, 1988). Nesse sentido, tais atividades são exclusivas às Forças Armadas (FFAA) e ao GSI-PR.

Devido à importância do papel das autoridades responsáveis pela classificação em níveis de sigilo das informações listadas no art. 23 da LAI para a segurança do Estado e da sociedade, consideraram-se nesta pesquisa tais autoridades como agentes públicos de segurança nacional.

Já as atividades de segurança pública federal são aquelas destinadas à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, e são exercidas no âmbito da APF pelo Departamento de Polícia Federal e pelo Departamento de Polícia Rodoviária Federal (Brasil, 1988), ambos pertencentes à estrutura do Ministério da Justiça.

Em virtude da sua importância na articulação e integração do Sistema Penitenciário Federal com os órgãos componentes do Sistema Nacional de Segurança Pública, principalmente no planejamento de atividades de inteligência, considerou-se, também, o Departamento Penitenciário Nacional, também vinculado ao Ministério da Justiça, como um órgão de segurança pública.

4.2 População da pesquisa

A população desta pesquisa é formada por agentes públicos que atuam nas atividades relativas à segurança nacional e segurança pública federal. Estes agentes estão lotados em diversos órgãos da APF, distribuídos geograficamente por todo o território nacional.

No contexto da segurança nacional, a população é representada pelos militares das FFAA, pelos oficiais de inteligência da Agência Brasileira de Inteligência (ABIN), pelos servidores da Secretaria de Segurança Presidencial, e também, pelas autoridades classificadoras estabelecidas pela LAI. Já no contexto da segurança pública federal, a população é formada pelos delegados da Polícia Federal (DPF), pelos policiais rodoviários federais (PRF) e pelos agentes penitenciários federais (AGPENF).

4.3 Amostra da pesquisa

Para Cooper e Schindler (2003, p. 150), é por meio da amostragem que se tira conclusões ao extrair elementos de uma determinada população. Na pesquisa quantitativa, a amostra consiste em escolher subconjuntos da população que se pretende estudar a fim de obter resultados de forma generalizada, entretanto, por se tratar de uma pesquisa qualitativa, a maior preocupação neste estudo é o aprofundamento e a abrangência da compreensão dos riscos inerentes à divulgação de dados de uma específica classe de agentes públicos.

Assim, esta pesquisa é qualitativa, pois além de responder questões particulares as quais não se pode quantificar, necessita de definições claras e objetivas dos sujeitos que comporão a amostragem dos indivíduos investigados (Minayo, 2001, p.21), haja vista que urge a necessidade de priorizar o critério de intencionalidade do pesquisador a fim de atender um fim específico (Gil, 2002, p. 145).

Sendo assim, com a finalidade de obter um "bom julgamento" das populações apresentadas no item anterior e considerando a intencionalidade do pesquisador, decidiu-se o uso da amostragem não

probabilística do tipo intencional (Silva; Menezes, 2005, p. 32) para construção de dois planos de amostragem.

O primeiro plano de amostragem é composto por sete indivíduos que possuem um importante papel no atual cenário nacional e internacional, bem como, detentoras de informações imprescindíveis à segurança da sociedade ou do Estado. Sendo dois Ministros de Estado; um servidor da secretaria de segurança presidencial; um oficial de inteligência; e três oficiais das FFAA, sendo um oficial da Marinha do Brasil atuante no programa nuclear brasileiro, um oficial do Exército Brasileiro atuante no setor político e estratégico e um oficial da Força Aérea Brasileira atuante na defesa do espaço aéreo nacional.

Já o segundo plano de amostragem é composto por vinte e sete indivíduos que atuam na segurança pública federal, distribuídos de forma a contemplar todas unidade federativas (UF) do Brasil. Considerando que os indivíduos ocupantes dos cargos de DPF e PRF estão distribuídos em todas UF e o cargo de AGPENF em apenas cinco UF que possuem penitenciárias federais, optou-se investigar onze DPF, onze PRF e cinco AGPENF.

5 Resultados obtidos

Nesta seção são apresentados os resultados obtidos durante a coleta de dados dos sete indivíduos constante da amostragem de agentes públicos que atuam na segurança nacional (Tabela I, no apêndice) e, também, os resultados obtidos da coleta de dados dos vinte e sete indivíduos constante da amostragem dos agentes públicos da APF que atuam na segurança pública federal (Tabela II, no apêndice).

Já os Gráficos 1 e 2 apresentam o percentual dos dados coletados dos investigados que atuam na segurança nacional e na segurança pública federal, respectivamente. Enquanto o Gráfico 3 apresenta os resultados obtidos dos trinta e quatro indivíduos investigados.

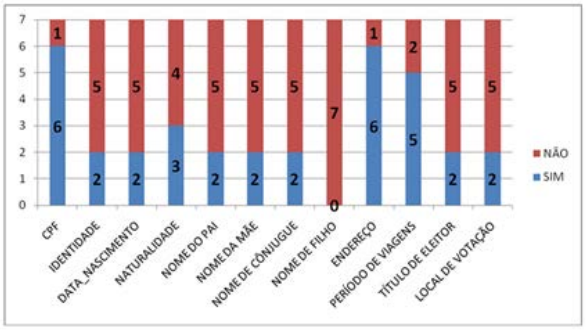

Gráfico 1. *Quantidade de dados coletados dos agentes de segurança nacional.*

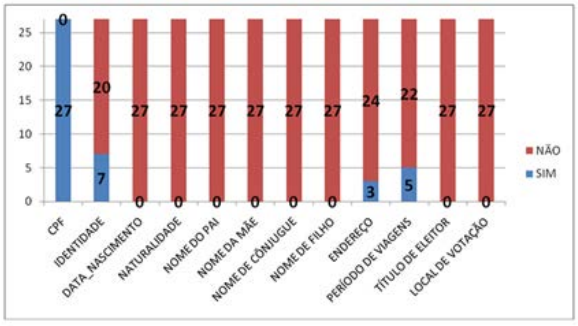

Gráfico 2. *Quantidade de dados coletados dos agentes de segurança pública federal.*

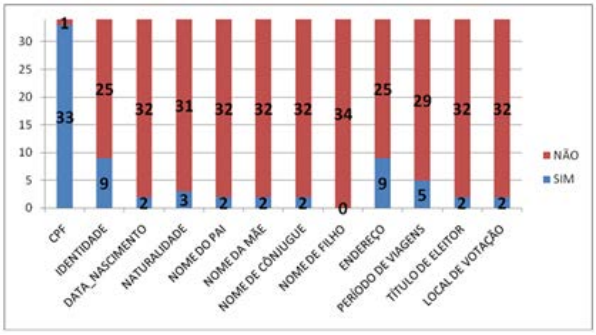

Gráfico 3. *Total de dados coletados dos indivíduos.*

6 Análises e discussões

Os resultados demonstraram que 33 dos 34 investigados tiveram seus CPF divulgados nos portais da *internet* dos órgãos de governo conforme apresentado no Gráfico 3. Isto vem em desencontro com o atual entendimento do STF (2011).

Neste contexto, ressalta-se que não obstante os esforços do governo federal em fortalecer as ações para a proteção de dados pessoais, não foi possível identificar no atual arcabouço jurídico, nem no já citado Projeto de Lei sobre proteção de dados pessoais e da privacidade (Brasil, 2015), orientações claras e objetivas sobre a divulgação do CPF na *internet*.

A Tabela I também apresenta uma grande quantidade de dados levantados atinentes aos indivíduos I_01 e I_02 em relação aos demais indivíduos. Possivelmente, os seguintes fatores cooperam para essa ocorrência: (a) Cumprimento do Art. 11 da Lei nº 12.813 de 16 de maio de 2013 que determina os órgãos divulgar, diariamente, por meio da *internet*, a agenda de compromisso das autoridades que ocupam cargo de ministro de Estado, de natureza especial, de presidente, vice-presidente e diretor de autarquias, fundações, empresas públicas ou sociedades de economia mista, como também, do Grupo-Direção e assessoramento, níveis 6 e 5 ou equivalente; e (b) Publicação da biografia dos ministros de Estado nos portais institucionais.

A publicação de alguns dados na biografia dos Ministros, como por exemplo, filiação e data de nascimento, aparentemente, não infere em erosão de privacidade e nem em quebra da SI, entretanto, foi por meio desses dados que o investigador desta pesquisa obteve informações eleitorais dos indivíduos I_01 e I_02, como: número do título de eleitor, zona, seção, local e endereço de votação, exemplificado nas Figuras 1 e 2.

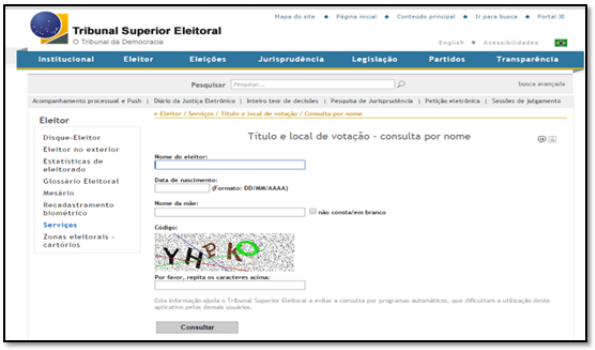

Figura 1. *Tela de consulta de título de eleitor por nome apresentada no site do Tribunal Superior Eleitoral.*

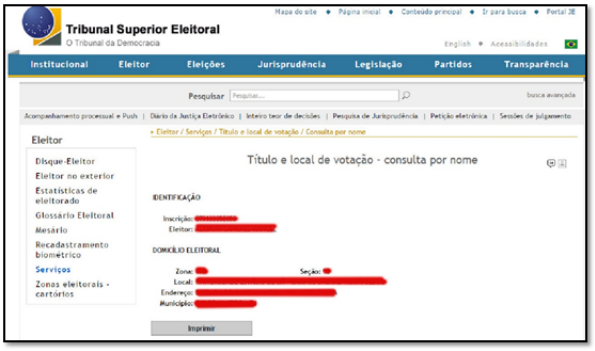

Figura 2. *Tela com resultado da consulta de título de eleitor por nome apresentada no site do Tribunal Superior Eleitoral.*

No Brasil, ainda não existe uma decisão jurídica sobre a exposição de dados eleitorais do cidadão na *internet*. Essa questão foi discutida intensamente, no ano de 2013, por ocasião da formalização do acordo de cooperação técnica nº 07/2013(1) celebrado entre a Justiça Eleitoral e a *Serasa Experian* para repasse de informações cadastrais de 141 (cento e quarenta e um) milhões de brasileiros para a empresa. Entretanto, por iniciativa da Corregedora-Geral Eleitoral, o citado acordo foi cancelado pelo Procedimento Administrativo nº 29.542/2012-TSE(2) com o fundamento da confiança na Justiça Eleitoral e na inexpugnabilidade dos dados a ela confiados.

Naquela época, o representante da empresa *Serasa Experian* alegou, em nota jornalística, que "todas as informações obtidas por ela, através do convênio, são públicas e de natureza cadastral, podendo ser acessadas no site do TSE"(3). Em resposta, na mesma nota, o Ministro do STF e também vice-presidente do TSE Marco Aurélio Mello declarou desconhecer essa permissão de consulta ao sítio do TSE, entretanto, os resultados aqui apresentados corroboram com a declaração da empresa.

O Gráfico 1 demonstrou que foi possível obter o endereço residencial de 6 indivíduos de um total de 7 agentes de segurança nacional investigados, ou seja, quase se aproximou da totalidade dos investigados. Nesse rol de agentes públicos estão incluídos Ministros de Estado, militares que atuam na defesa do espaço aéreo e no programa nuclear brasileiro, oficiais de inteligência, segurança pessoal da Presidência da República.

Já o Gráfico 2 apresentou uma relação bem inferior referentes à detecção dos endereços dos agentes de segurança pública federal, cujo resultado foi de apenas 3 endereços encontrados de um total de 27 investigados. No entanto, é importante frisar que um dos endereços levantados pertence a um agente penitenciário federal. A revelação desta informação poderá afetar drasticamente o sistema prisional brasileiro. Elementos do crime organizado poderão utilizar de tal informação para efetuar sequestros, seguido de chantagens, visando promover fugas de presidiários.

O fator determinístico para obtenção dos endereços residenciais de alguns investigados foi a fragilidade de controle de acesso lógico dos portais das Secretarias de Fazenda de algumas UF por ocasião da prestação de serviços de emissão de certidão negativa de débitos aos cidadãos. Isso explica os resultados do Gráfico 2, visto que a maioria dos seus investigados pertencem ao DF, e esta UF se encontra vulnerável conforme apresentado nos resultados do trabalho dissertativo que originou este artigo.

7 Conclusões

Esta pesquisa demonstrou por meio de uma análise dos dados publicados na *internet* referentes aos agentes públicos da APF que atuam na segurança nacional e na segurança pública que há evidências que comprovam a quebra da segurança da informação, o que compromete a privacidade de tais agentes e a segurança do Estado e da sociedade. Neste sentido, ao optar pela realização de uma pesquisa documental, este estudo obteve dados concretos acerca dos riscos que os indivíduos investigados e, também, o Estado estão expostos, frente às diversas ameaças do mundo real e virtual.

A partir dos dados levantados durante a investigação, foi possível identificar respostas que reforçam alguns

argumentos descritos no decorrer do estudo. Conforme apresentado na introdução, comprovou-se a necessidade de unificação das formas de tratamento da informação pública. Os resultados apontaram que os órgãos dos diferentes Poderes e esferas divulgam informações pessoais dos agentes públicos de forma diferenciada, com isso, aspectos de segurança ora são cumpridos por um, ora não são por outros.

O método apresentado para coleta de dados pessoais dos agentes públicos revelou a facilidade de obtenção de dados pessoais por qualquer pessoa sem o apoio de ferramentas automatizadas. Embora não tenha sido o cerne desta pesquisa, observou-se que alguns dados não encontrados referentes aos agentes públicos estavam disponíveis na *internet* em portais não governamentais, o que demonstra ser o problema bem maior do que aqui apresentado.

Os resultados da coleta de dados também apontaram que não existe uma política pública que estabelece regras claras e objetivas sobre a publicação de dados pessoais nos portais de transparência das UF. Nesse sentido, urge a necessidade de uma Lei específica que estabeleça um sistema único de transparência para todo o Estado brasileiro e um órgão central com as atribuições de supervisionar tal sistema.

Atualmente, existe no âmbito da APF um sistema de controle interno e de correição, supervisionado pela CGU, com a finalidade de prestar orientações técnicas por meio de normativos, entretanto, esse sistema não atende as necessidades apresentadas no estudo, visto que, o sistema existente destina-se apenas às unidades de ouvidoria do Poder Executivo Federal.

Ademais, pode-se concluir que a APF ainda se encontra em fase de consolidação frente às profundas exigências emanadas dos princípios da publicidade e transparência, bem como às imposições feitas pela LAI. Logo, por meio das análises e discussões aqui realizadas, é possível identificar os principais pontos vulneráveis e que merecem especiais atenções para o fortalecimento da SI, a fim de evitar ou mitigar impactos negativos para o agente público e para o Estado e sociedade.

Por fim, é possível concluir que o presente estudo apresenta resultados preocupantes que demonstram a fragilidade do Estado brasileiro com a publicação de dados pessoais dos seus agentes públicos. Por outro lado, esses resultados podem servir de alerta às autoridades e órgãos de controle e de transparência pública sobre uma visão ainda não pesquisada. Atualmente, as discussões sobre os impactos das publicações de dados pessoais são direcionadas apenas à quebra da privacidade, diferente do que apresentado nesta pesquisa que, além deste impacto, acrescentou os riscos decorrentes dessas divulgações à segurança do Estado e da Sociedade.

Notas

(1) Publicado no D.O.U nº 140 de 23 de julho de 2013 seção 3. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=3&pagina=148&data=23/07/2013.

(2) Procedimento Administrativo n. 29.542/2012 do Tribunal Superior Eleitoral. http://www.justicaeleitoral.jus.br/arquivos/tse-acordo-cooperacao-serasa.

(3) Nota do Jornal Nacional publicada em 07/08/2013. http://g1.globo.com/jornal-nacional/noticia/2013/08/presidente-do-tse-quer-fim-de-acordo-que-permite-repasse-de-dados-de-eleitores-serasa.html

Referências

Brasil (1983). Lei nº 7.170, de 14 de dezembro de 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Brasília, DF. 1983. http://www.planalto.gov.br/ccivil_03/leis/l7232.htm.

Brasil (1988). Constituição da República Federativa do Brasil. Brasília, DF. 1988. http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm (23-12-14).

Brasil (1991). Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília, DF. 1991. http://www.planalto.gov.br/ccivil_03/leis/L8159.htm (23-12-14).

Brasil (2011). Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações. Brasília, DF. 2011. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (23-12-14).

Brasil (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. (23-12-14).

Brasil (2015). Projeto de Lei. Dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências. 2015. http://www.acessoainformacao.gov.br/menu-de-apoio/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf (20-01-15).

Capurro, Rafael; Hjørland, Birger. (2007). O conceito de informação. Perspectivas em Ciência da Informação 12:1 (jan./abr. 2007) 148-207.

Cervo Amado I.; Bervian, Pedro A. (1983). Metodologia científica: para uso dos estudantes universitários. 3ª ed. São Paulo: McGraw-Hill do Brasil, 1983.

CIA, Conselho Internacional de Arquivos. (2005). Documentos de Arquivo Electrónicos: Manual para Arquivistas (ICA Estudo nº 16). Publicado inicialmente em inglês como "Electronic Records: a Workbook for Archivists" pelo Comité de Arquivos Correntes em Ambiente Electrónico (2000-2004) do Conselho Internacional de Arquivos, 2005. http://www.ica.org/download.php?id=1616 (23-12-2014).

Cooper, D. R.; Schindler, P. S. (2003). Métodos de pesquisa em administração, 7ª ed. Porto Alegre: Bookman, 2003.

DPA. (1998). Data Protection Act. Personal data. United Kingdom of Great Britain and Northern Ireland, 1998. http://legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (12-06-2015).

Gil, Antônio Carlos. (2002). Como elaborar projetos de pesquisa. 4. ed. São Paulo: Altas, 2002.

GSI-PR. Gabinete de Segurança Institucional da Presidência da República (2008). Instrução Normativa nº 01 do GSI-PR, de 13 de Junho de 2008 (IN01/DSIC/GSI/PR). Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. 2008. http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf (20.12-14).

GSI-PR. Gabinete de Segurança Institucional da Presidência da República (2009). Norma Complementar nº 5 da Instrução Normativa nº 01 GSI-PR (NC05/IN01/DSIC/GSI/PR), de 14 de agosto de 2009. Criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR. 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf>. Acesso em: 20 de dez. 2014.

GSI-PR. Gabinete de Segurança Institucional da Presidência da República (2014). Norma Complementar nº 20 da Instrução Normativa nº 01/GSI-PR (NC20/IN01/DSIC/GSI/PR rev. 1), de 15 de dezembro de 2014. Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal. 2014. http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf (20-12-14).

Jardim, José Maria. (2009) O acesso à informação arquivística no Brasil: problemas de acessibilidade e disseminação. Niterói: EdUFF, 2009. http://www.conarq.arquivonacional.gov.br/Media/publicacoes/mesa/o_acesso_informao_arquivistica_no _brasil.pdf (11-01-15).

Matias-Pereira, José. (2007) Manual de metodologia de pesquisa científica. São Paulo: Atlas, 2007.

Meirelles, Hely Lopes. (1998) Direito Administrativo Brasileiro. 23.ed. São Paulo: Malheiros, 1998.

Minayo, Maria Cecília de Souza (org). (2001). Pesquisa social: teoria, método e criatividade. Petrópolis/RJ: Vozes, 2001

Oliveira Netto, Alvim Antônio de. (2006). Metodologia da Pesquisa Científica: Guia Prático para Apresentação de trabalhos Acadêmicos. 2º ed. Florianópolis: Visual Books, 2006.

Rangel, Alcimar Sanches. (2010). Estudo da Metodologia de Análise de Riscos EBIOS para Aplicação na Administração Púbica Federal: Potencial Alinhamento à Legislação Brasileira. Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a obtenção do título de Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações. Brasília: 2010.

Robredo, J. (2003). Da Ciência da informação revisitada aos sistemas humanos de informação. Brasília: Thesaurus, 2003.

Rocha, Cármen Lúcia Antunes. (1994). Princípios Constitucionais da Administração Pública. Belo Horizonte: Del Rey, 1994.

Silva, Edna Lúcia da; Menezes, Estera Muszkat. (2005). Metodologia da pesquisa e elaboração de dissertação. 4. ed. rev. atual. Florianópolis: UFSC, 2005.

Simião, Reinaldo Silva. (2009). Segurança da Informação e Comunicações: conceito aplicável em organizações governamentais. Brasília: UnB, 2009. http://dsic.planalto.gov.br/cegsic/83-monografias-da-1o-turma-do-cegsic (23-12-14).

STF. Superior Tribunal Federal. (2011). Suspensão de Segurança n.º 3.902-4/SP. Relator Ministro Min. Ayres Britto, Tribunal Pleno, julgado em 09/06/2011 – Brasília: 2011. http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID =6281985 (22-12-14).

UNESCO. (2014). Relatório Global: Abrindo novos caminhos para o empoderamento: TIC no acesso a informação e ao conhecimento para as pessoas com deficiência; tradução: DB Comunicação. -- São Paulo: Comitê Gestor da Internet no Brasil, 2014. http://cetic.br/publicacao/relatorio-global-unesco-abrindo-novos-caminhos-para-o-empoderamento-tic-no-acesso-a-informacao-e-ao-conhecimento-para-as-pessoas-com-deficiencia/ (22-12-14).

Vidal, Gabriel Rigoldi. (2010) Privacidade e internet. Universidade Estadual Paulista – Faculdade de Ciências Humanas e Sociais, 2010. http://www.direitorp.usp.br/arquivos/noticias/sites_eventos/3_semana_juridica_2010/papers/Gabriel%20Rigoldi%20Vidal.pdf (22-12-14).

Received: 2015-06-23. Accepted: 2016-02-21.

Apêndice

Identificação	Cargo	UF do órgão	CPF	Identidade	Data de nascimento	Naturalidade	Nome do pai	Nome da mãe	Nome do conjugue	Nome de filhos	Endereço	Período de viagens	Título de eleitor	Local de votação
I_01	Ministro de Estado 1	DF	V	V	V	V	V	V	V	X	V	V	V	V
I_02	Ministro de Estado 2	DF	V	X	V	V	V	V	V	X	V	V	V	V
I_03	Segurança Presidencial	DF	V	X	X	X	X	X	X	X	V	V	X	X
I_04	Oficial de Inteligência da ABIN	DF	V	V	X	X	X	X	X	X	V	X	X	X
I_05	Oficial da Marinha do Brasil	SP	X	X	X	X	X	X	X	X	X	X	X	X
I_06	Oficial do Exército Brasileiro	DF	V	X	X	V	X	X	X	X	V	X	X	X
I_07	Oficial da Força Aérea Brasileira	DF	V	V	X	X	X	X	X	X	V	X	X	X

Legenda: V - Encontrado X - Não encontrado

Tabela I: Resultados da coleta de dados dos agentes de segurança nacional.

Identificação	Cargo	UF do órgão	CPF	Identidade	Data de nascimento	Naturalidade	Nome do pai	Nome da mãe	Nome do conjugue	Nome de filhos	Endereço	Período de viagens	Título de eleitor	Local de votação
I_08	Delegado da Polícia Federal	AC	V	X	X	X	X	X	X	X	X	X	X	X
I_09	Policial Rodoviário Federal	AL	V	X	X	X	X	X	X	X	X	X	X	X
I_10	Delegado da Polícia Federal	AM	V	X	X	X	X	X	X	X	X	X	X	X
I_11	Policial Rodoviário Federal	AP	V	X	X	X	X	X	X	X	X	X	X	X
I_12	Delegado da Polícia Federal	BA	V	X	X	X	X	X	X	X	X	X	X	X
I_13	Policial Rodoviário Federal	CE	V	V	X	X	X	X	X	X	X	X	X	X
I_14	Agente Penitenciário Federal	DF	V	V	X	X	X	X	X	X	V	X	X	X
I_15	Delegado da Polícia Federal	ES	V	X	X	X	X	X	X	X	X	X	X	X
I_16	Policial Rodoviário Federal	GO	V	X	X	X	X	X	X	X	X	X	X	X
I_17	Delegado da Polícia Federal	MA	V	X	X	X	X	X	X	X	X	X	X	X
I_18	Policial Rodoviário Federal	MG	V	X	X	X	X	X	X	X	X	X	X	X
I_19	Agente Penitenciário Federal	MS	V	V	X	X	X	X	X	X	X	X	X	X
I_20	Delegado da Polícia Federal	MT	V	X	X	X	X	X	X	X	X	X	X	X
I_21	Policial Rodoviário Federal	PA	V	X	X	X	X	X	X	X	X	X	X	X
I_22	Delegado da Polícia Federal	PB	V	X	X	X	X	X	X	X	X	X	X	X
I_23	Policial Rodoviário Federal	PE	V	X	X	X	X	X	X	X	X	X	X	X
I_24	Delegado da Polícia Federal	PI	V	X	X	X	X	X	X	X	X	X	X	X
I_25	Agente Penitenciário Federal	PR	V	V	X	X	X	X	X	X	X	X	X	X
I_26	Policial Rodoviário Federal	RJ	V	X	X	X	X	X	X	X	X	X	X	X
I_27	Agente Penitenciário Federal	RN	V	V	X	X	X	X	X	X	X	X	X	X
I_28	Agente Penitenciário Federal	RO	V	V	X	X	X	X	X	X	X	X	X	X
I_29	Delegado da Polícia Federal	RR	V	X	X	X	X	X	X	X	X	X	X	X
I_30	Policial Rodoviário Federal	RS	V	X	X	X	X	X	X	X	V	X	X	X
I_31	Delegado da Polícia Federal	SC	V	V	X	X	X	X	X	X	X	X	X	X
I_32	Policial Rodoviário Federal	SE	V	X	X	X	X	X	X	X	X	X	X	X
I_33	Delegado da Polícia Federal	SP	V	X	X	X	X	X	X	X	X	X	X	X
I_34	Policial Rodoviário Federal	TO	V	X	X	X	X	X	X	X	V	X	X	X

Legenda: V - Encontrado X - Não encontrado

Tabela II: Resultados da coleta de dados dos agentes de segurança pública federal.