

GOVERNO ELETRÔNICO, CIDADANIA VIRTUAL E PROTEÇÃO DE DADOS PESSOAIS: desafios ao Estado brasileiro.

Rosane Leal da Silva
Lahis Pasquali Kurtz

SUMÁRIO: Introdução; 1 O Governo Eletrônico e a emergência de novas dimensões da cidadania; 2 A proteção de dados pessoais na sociedade informacional: desafios ao Estado; 3 A privacidade do cidadão usuário do governo eletrônico: medidas de proteção adotadas no Brasil; Considerações finais; Referências.

RESUMO: Este trabalho apresenta e discute os desafios impostos pela utilização das tecnologias da informação e comunicação por parte do Estado Brasileiro, com ênfase para as atividades desempenhadas pelo Governo Eletrônico. Para tanto, utiliza-se do método dialético, com ênfase para a dialética da complementaridade, a partir do qual destacam-se aspectos positivos decorrentes da adoção das novas tecnologias, tais como a abertura de novos canais de comunicação e de participação entre o cidadão e o gestor público, bem como as facilidades de acesso rápido e fácil a inúmeros serviços públicos disponibilizados via Internet. Em contraponto a essas vantagens que ampliam o exercício da cidadania, apresentam-se e discutem-se aspectos de risco e vulnerabilidade aos direitos fundamentais do cidadão, sobretudo aqueles relacionados à privacidade *lato sensu*, que podem ser atingidos pelo acesso e utilização desautorizado dos dados pessoais do cidadão. Partindo dessa constatação, apontam-se medidas já adotadas no Brasil para garantir a segurança e confiabilidade do Governo Eletrônico, ações consideradas insuficientes por serem unilaterais, voltadas apenas para o funcionamento do próprio E-Gov, sem abranger políticas públicas de preparação da população para o exercício da cidadania virtual.

PALAVRAS-CHAVE: Cidadania; Dados Pessoais; Direitos Fundamentais; Governo Eletrônico; Políticas Públicas.

ABSTRACT: This work presents and discusses the challenges imposed by the use of information and communication technologies by the Brazilian State, emphasizing the activities performed by the Electronic Government. The dialectic method is used to accomplish this, with emphasis to the complementarity dialectic, from which positive aspects coming from the adoption of these new technologies are highlighted, such as opening new channels of communication and participation between the citizen and the public manager, as well as the benefits of easy and fast access to numberless public services available via Internet. In opposition to these advantages which enlarge the access to citizenship, it is presented and discussed aspects of risk and vulnerability to the citizen's fundamental rights, mainly the ones related to *latu sensu* privacy, which may be reached by the non-authorized access and use of the citizen's personal data. From this evidence, the measures already adopted in Brazil to guarantee the security and trust of the Electronic Government are pointed out, actions considered insufficient because they are unilateral, only to make the E- Govern work, without including public policies to prepare the population for this exercise of virtual citizenship.

KEY-WORDS: Citizenship; Personal Data; Fundamental Rights; Electronic Government; Public Politics.

INTRODUÇÃO

Os últimos anos registram o esforço do Brasil para promover a inclusão digital de sua população, entendendo-se que o acesso às novas tecnologias da informação e comunicação, notadamente a Internet, possibilitarão a ascensão econômica, social e cultural dos brasileiros. A esses benefícios se soma o incremento da cidadania, o que tem sido perseguido a partir da implantação do Governo Eletrônico no Brasil, cujo marco inicial data do início do ano 2000.

O termo Governo Eletrônico é utilizado para definir o uso das novas tecnologias informacionais numa gama de funções desempenhadas pelo governo, que vão desde a atuação interna dos órgãos que compõem a Administração Pública, até a sua relação com o cidadão, que tem assumido novos contornos a partir da ampliação dos canais de comunicação e participação política.

A implantação do Governo Eletrônico possibilita que se desenhe uma nova configuração de gestão, mais democrática e participativa, na qual o cidadão acessa as informações em tempo real e sem necessidade de deslocamento físico, o que lhe permite fazer consultas, acompanhar as ações dos gestores públicos e realizar serviços públicos por meio da Internet. Ao lado dessas potencialidades, a adoção das tecnologias por parte do Estado brasileiro tem inspirado preocupações, sobretudo com a proteção de dados pessoais do cidadão, considerados como integrantes de seus direitos fundamentais.

É sobre essa temática que versa o presente trabalho, elaborado de acordo com método dialético, a partir do qual são feitas contraposições de vantagens/potencialidades e riscos/vulnerabilidades para o exercício de uma nova dimensão da cidadania, aqui denominada como cidadania virtual. As reflexões apresentadas se constituem em estudos parciais realizados no âmbito do Projeto “A Gestão Pública na Sociedade Informacional”, realizado na Universidade Federal de Santa Maria, com financiamento do CNPq.

1 O GOVERNO ELETRÔNICO E A EMERGÊNCIA DE NOVAS DIMENSÕES DA CIDADANIA.

O surgimento das tecnologias informacionais data da segunda metade do Século XX, tendo como berço os Estados Unidos, que desenvolveram uma rede interna com o objetivo de interligar os computadores dos órgãos encarregados da defesa do Estado. Com isso visava-se estimular a pesquisa interativa e garantir o sigilo das informações enviadas e compartilhadas, que ficariam protegidas contra as investidas de seu principal *inimigo* da Guerra Fria. Não tardou muito, no entanto, para que o uso inicial, de caráter eminentemente militar, cedesse espaço para outras apropriações, o que ocorreu com a criação da Internet, nos anos setenta. Mas o grande divisor de águas se deu quando os universitários e a cultura dos *campi* norte-americanos se apropriaram dessa tecnologia, acrescentando-lhe novas funções de uso pessoal relacionadas à interação e à formação de redes. Logo o mercado percebeu o potencial dessa tecnologia e passou a investir em novos usos, o que contribuiu para que seu uso se expandisse junto à população.

Desse período até os dias atuais se processou uma verdadeira revolução informacional, pois essa tecnologia, ao proporcionar comunicação interativa, instantânea e global, transformou os relacionamentos interpessoais. A esse impacto nas comunicações se somam outros ligados à valorização da informação, erigida a “mercadoria de primeira grandeza no mercado globalizado, altamente valorizada e

rentável” .

Não tardou para que os Estados percebessem as potencialidades da Internet, passando em investir nessa tecnologia. Mas ao lado das inúmeras vantagens apresentadas, revelaram-se desafios, pois a nova tecnologia não respeitava os mapas políticos, permitindo que rapidamente as informações ultrapassassem as fronteiras dos Estados, desafiando os governos, que logo perceberam a insuficiência das suas tradicionais formas de atuação. Era preciso dar outros usos institucionais à tecnologia, pois a burocracia característica de órgãos públicos, com padrões de prestação rígidos e imutáveis de atendimento se tornou ineficiente quando contraposta às possibilidades da Internet, que se beneficia de serviços descentralizados e feitos sob medida *para e pelos* próprios usuários. Essa nova realidade também foi percebida pelo Governo Brasileiro.

Desde meados da década de 90, quando a internet começou a operar no Brasil, criou-se o Comitê Gestor da Internet no Brasil, órgão de composição mista, encarregado de coordenar os serviços no país. Nessa esteira, a partir o ano 2000 foi implementado o voto eletrônico e, na mesma época, os internautas brasileiros, que chegavam a um número de 9,8 milhões, passaram a ter possibilidade de acessar a rede através do aparelho celular.

À medida que mais atividades diárias das pessoas passaram a ser realizadas por meio de computadores, inclusive contratações de serviços, compras, pagamentos, contatos interpessoais, cresceu a importância de também o governo inserir-se nesse espaço. Isso é reconhecido até mesmo nos documentos oficiais, como se vê na Proposta de Política de Governo Eletrônico para o Poder Executivo Federal, onde se evidencia a transformação no *modus operandi* do Estado: “Os impactos no Estado Moderno também serão significativos. Informação pública, gratuita, abundante e acessível será um dos bens mais importantes que o Estado deve oferecer aos seus cidadãos” . Acesso, informação, comunicação e gestão desburocratizada e transparente assumem papéis de destaque.

Esse novo cenário ampliou as responsabilidades do Estado Brasileiro, o que se deu, sobretudo, devido ao incremento da Política de Governo Eletrônico para o Poder Executivo Federal, elaborada em 2000, ano a partir do qual diversos serviços do governo passaram a ser prestados na Internet:

Há também uma série de serviços governamentais já em operação na Internet, como as declarações do Imposto de Renda, certidões de pagamentos de impostos, divulgação de intenções de compras governamentais, leilão eletrônico, cadastramento de fornecedores, matrículas escolares, acompanhamento de

processos judiciais, acesso a indicadores econômicos e sociais, apoio na realização de censos, informações sobre aposentadorias, capacitação à distância, quiosques de acesso à Internet nos Correios, diversos aplicativos de informações gerenciais, e o novo modelo de gestão por programas do Avanço Brasil, entre outras iniciativas.

A iniciativa concretizou-se com o Decreto Presidencial de 3 de abril de 2000 (revogado pelo decreto nº 4.195, art. 22) e ganhou o nome “E-Gov”. Assim, valendo-se dos meios eletrônicos, o governo busca prestar serviços aos cidadãos, reduzindo a necessidade de deslocamento ao estabelecimento físico onde se situa a repartição pública e o tempo de espera por atendimento para a prática de atos relacionados aos deveres de cidadania, como, por exemplo, declaração de imposto de renda. O E-Gov atua também para aproximar o cidadão do governo, já que sistematicamente programas digitais do governo armazenam informações sobre quem utilizou os serviços, quais foram suas consultas e dúvidas e em que datas acessou o sistema.

Um dos objetivos do Governo Eletrônico é a ampliação de canais de comunicação entre os gestores públicos e o cidadão e para tanto há espaços nos *sites* destinados ao usuário, que pode oferecer sugestão e propostas de mudança para melhoria dos serviços. Com isso se abre a oportunidade de os cidadãos participarem mais diretamente da gestão pública, opinando e buscando informações, o que por certo permite melhores condições de exercer sua cidadania social e política. Ao lado dessas dimensões, começa a se erigir outra, típica da sociedade informacional.

Para compreender a evolução do tema convém resgatar as lições de Pérez Luño (2004, p. 47), segundo o qual a partir da Modernidade a cidadania significa um vínculo jurídico de pertencimento ao Estado de Direito, abrangendo um conjunto de direitos políticos que definem a participação imediata dos titulares na comunidade estatal. São direitos que variam de um Estado a outro, recebendo influência direta do período histórico e das escolhas políticas realizadas. Esse conceito moderno de cidadania se satisfazia com a noção de nacionalidade, o que foi gradativamente se ampliando na medida em que as sociedades se tornaram complexas e plurais, o que exigiu a abertura do conceito. O momento presente requer um passo além, pois além de uma cidadania transnacional, a sociedade informacional amplia o sentido e o alcance desse conceito.

Com efeito, não se deve esquecer que a cidadania vai além do mero exercício de direitos políticos, manifestando-se em várias esferas da vida, como ensinado por Sêda (1995, p. 16), para quem o conceito de cidadania apresenta três dimensões: a) a civil, referente à forma como a pessoa manifesta e tem reconhecida a sua vontade na esfera

civil, sendo autorizada a negociar, contratar, fazer testamentos; b) a dimensão política, que se refere à participação nas questões públicas e, por fim, c) a dimensão social. Segundo ele, esta seria a primeira dimensão da cidadania, pois se liga ao exercício de proteção dos próprios direitos fundamentais, ou seja, seria o momento em que a pessoa, independentemente da idade, busca nos mecanismos sociais a proteção dos seus direitos fundamentais.

Ao lado dessas dimensões pode-se dizer que emerge outra, típica da sociedade informacional, que é dimensão digital. Com efeito, a sociedade informacional, por se revelar mais aberta e flexível, oferece condições para o desenvolvimento de novas facetas da cidadania. O fato de as novas tecnologias oportunizarem que as pessoas se informem sobre os rumos da Administração Pública e que usem esta via para dirimir suas dúvidas e para protestar, sem a necessidade de realizar deslocamento físico, amplia sua participação e seu envolvimento em projetos de interesse coletivo. Ademais, como destacado por Cardoso (2007, p. 31-33), o uso dessas ferramentas favorece a formação de redes de relacionamento, aumentando as oportunidades de emergência de projetos coletivos, o que muitas vezes pode se mostrar útil tanto para a resolução de problemas locais, como os do bairro, quanto para o enfrentamento de questões de interesse nacional e até global.

Em que pese as vantagens e o empoderamento dos cidadãos, é inegável que ao acessar os serviços do Governo Eletrônico o usuário disponibiliza alguns dados pessoais, nem sempre devidamente resguardados pelos sistemas informáticos. Tal observação remete ao debate sobre a implementação de mecanismos de segurança nos *sites* e portais governamentais para que o exercício dessa nova dimensão da cidadania não coloque em risco os dados pessoais do cidadão, considerados direitos fundamentais, conforme se verá a seguir.

2 A PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE INFORMACIONAL: desafios ao Estado.

O desenvolvimento tecnológico experimentado no segmento informacional tem permitido novas práticas, tanto individuais quanto empresariais, redefinindo, inclusive, as formas de atuação do Estado, como constata Fagúndez:

Há empresas virtuais, comunidades virtuais, Estados virtuais, tecnologias virtuais, que promovem uma profunda reformulação na ciência, corrompendo os conceitos de espaço e tempo. Uma informação circula imediatamente em todo o planeta e produz efeitos concretos, na realidade, boatos a respeito de países e empresas. O mundo virtual possui grande potencialidade real.

Foi a busca por utilização desse potencial em seu favor que inspirou a criação dos governos eletrônicos, projetos de comunicação e interação entre entes da Administração Pública e cidadãos no ambiente virtual. Não obstante esses avanços e facilidades, o que representou grande passo para a Administração Pública pode ter gerado novas questões de insegurança para os cidadãos.

Nesse novo contexto originado pelo crescente desenvolvimento e utilização das tecnologias informacionais, uma pauta nova de preocupações e conflitos se apresenta, merecendo destaque a proteção de dados pessoais.

Sob o ponto de vista da privacidade, a implementação do Governo Eletrônico deve considerar a grande ameaça contida no fato de esses serviços serem virtualmente realizados. Conforme Abelson, Ledeen e Lewis, todas as informações sobre a vida inteira de uma pessoa poderiam ser facilmente armazenadas em formato digital; e muitas informações de fato o são. Apesar do evidente aspecto positivo dessa capacidade, há as consequências geradas por conteúdo sensível sobre cidadãos estar em formato facilmente reproduzível e organizado, como o é o dos bancos de dados.

Criado para consultar a relação entre dois ou mais fatos, o banco de dados permite reunir, para fins de pesquisa ou de publicidade, os mesmos dados de determinado grupo de indivíduos, sem identificação direta, como nome ou endereço completo. Conforme explicado por Abelson, Ledeen e Lewis, para encontrar uma informação geralmente é necessário lançá-la no sistema, de onde advirá sua correspondente, e é possível a partir daí usar a lógica para formar conjuntos de informações que são correlacionadas entre si nos bancos de dados.

Os autores explicam que devido ao grande contingente de indivíduos que integram os bancos de dados é improvável conseguir, utilizando somente esforços humanos, correlacionar a quantidade de dados suficientes para reconstruir a identificação dos envolvidos nas pesquisas. No entanto, essa situação muda quando se trata de um computador buscando e unindo os dados, como exemplificado por um caso no qual a divulgação de estatísticas sobre a saúde da população estadunidense tornou possível descobrir doenças que pessoas específicas possuíam, o que foi obtido graças à inclusão

de informações aparentemente impessoais para agrupar os dados, tais como gênero, código postal e data de nascimento.

Esse exemplo, entre tantos outros, mostra ser possível constituir um dossiê detalhado acerca de alguém utilizando somente informações estatísticas e programas de computador, o que se deve à capacidade das tecnologias digitais de reunir, em alta velocidade, uma quantidade considerável de dados segundo padrões. E é nessa capacidade que reside o maior desafio para a inserção de serviços do governo na Internet: garantir a privacidade de seus usuários. A partir dessa constatação, é cabível questionar até que ponto se estende essa garantia, e a extensão que devem ter as medidas tomadas no âmbito do Governo Eletrônico para assegurá-la.

Tal questionamento tem importância porque nome, características físicas, idade, gostos e preferências são alguns dos aspectos definidores da personalidade de alguém. Informações como essas são, essencialmente, o que identifica uma pessoa. Os dados que as compõem fazem parte da visão subjetiva de mundo de cada um, são parâmetros da relação de um sujeito com seu meio exterior, possibilitadores de construção de novos conceitos sobre o mundo e sobre si, o que legitima seu titular a protegê-los da ingerência externa.

Essa ideia, aliás, não se constitui em novidade, sendo defendida por Hannah Arendt em sua afirmação “uma existência vivida inteiramente (...) na presença de outros, torna-se, como diríamos, superficial”, o que evidencia a necessidade de o ser humano, em sua interação com o meio, delimitar uma área de proteção, criando momentos e espaços que sejam só seus. Compreendido nessa necessidade encontra-se o direito de controle sobre quais espaços entrarão em contato com o mundo exterior, que dados pessoais serão disponíveis e publicizados e quais devem ser mantidos intactos ou com acesso limitado por constituírem aspectos privados de sua existência.

Com a incorporação dos direitos de personalidade à Constituição Federal de 1988 esses aspectos têm suas dimensões juridicamente valorizadas, pois como preceitua o art. 5º, X, são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

No que tange a delicadeza dos contornos da privacidade, as discussões de maior repercussão iniciaram-se nos Estados Unidos, nas últimas décadas do século XIX. Houve nessa época quantidade considerável de demandas judiciais que recorrentemente chegavam à Suprema Corte, referentes a fotos e informações veiculadas em jornais sem

a devida permissão dos titulares, o que tornou necessária a delimitação desse direito. Originalmente, foi definido como “direito de ser deixado só”, por Cooley, e começou a ser levado a amplitudes maiores por Warren e Brandeis.

A dupla de advogados estadunidenses chamou atenção para a novidade representada pelo surgimento da mídia de massa: a possibilidade de empresas de comunicação se apropriarem de materiais que diziam respeito a indivíduos e, sem seu consentimento, levá-los ao conhecimento de um número potencialmente infinito de pessoas. Isso era feito sem realização de contrato e a autorização do titular para publicar fatos sobre si era dispensável, já que eram considerados propriedade da empresa que os descobrira.

A tutela de fatos cotidianos era vista pelo direito no mesmo patamar da propriedade intelectual, como se narrativas e imagens sobre a vida privada fossem iguais a uma narração literária ou uma fotografia artística. Sabe-se que hoje esse entendimento mudou e o resguardo de dados pessoais não pode ser identificado com um direito patrimonial, como se as diversas faces do âmago de uma pessoa pudessem ser vistas destacadamente do todo que a identifica. Essas informações não são meramente de propriedade da pessoa, elas fazem *parte da pessoa*, integram e definem sua personalidade, e sua violação tem potencial para atingir a dignidade do titular dos dados.

E nesse ponto cabe lembrar as palavras de Sarlet, para quem a dignidade

[...] é algo que simplesmente existe, sendo irrenunciável e inalienável, na medida em que constitui elemento que qualifica o ser humano como tal e dele não pode ser destacado, de tal sorte que não se pode cogitar na possibilidade de determinada pessoa ser titular de uma pretensão a que lhe seja concedida dignidade.

Portanto, por serem elementos essenciais à dignidade, os dados pessoais não podem ser tratados como posses, como se hierarquicamente inferiores ou distintas da honra e da imagem, essas desde cedo reconhecidas e protegidas, tanto pelo Direito Civil, quanto Penal.

Com a privacidade caracterizada como direito fundamental, o Estado obrigou-se a defender os cidadãos de violações ao direito de determinar o que pode ser disponibilizado para terceiros. De acordo com essa interpretação, Pérez Luño afirma que na atualidade “[...] a intimidade se contempla como a possibilidade de conhecer, acessar e controlar as informações que concernem a cada pessoa”.

A partir desse breve histórico, verifica-se a intrínseca relação entre as tecnologias

da informação e comunicação – cujo aprimoramento oportunizou a origem do E-Gov – e os conflitos envolvendo privacidade. Com a disponibilização de dimensões virtuais de serviços aos cidadãos e de informações públicas em *sites* governamentais, a tarefa da Administração Pública de garantir a segurança de dados pessoais assumiu novas perspectivas.

A complexidade e a relevância do tema despontam com um simples exemplo: quando utilizam serviços eletrônicos do *site* da Receita Federal, os cidadãos têm seus dados lançados na Internet, ou seja, guardados não só num computador em um prédio público, mas em diversos computadores do órgão que mantém a rede funcionando, e potencialmente em todos os computadores que a ela tiverem acesso. O problema deixa de ser o sentimento de posse que a pessoa jurídica pode ter sobre um fato ou uma informação obtida sobre algum cidadão, e passa a ser a *total ausência de sentimento de posse* ou responsabilidade das instituições, privadas e públicas, sobre a informação que detêm sobre as pessoas, que não mais se limita aos formatos passíveis de controle. Tal situação é definida por Pérez Luño como perda da autodeterminação informacional, algo que pode acontecer tanto por ação das instituições privadas, como pela atuação da Administração Pública na sociedade informacional.

Nessa nova realidade, Abelson, Ledeen e Lewis destacam que “[...] dados sensíveis sobre todos numa nação poderiam caber em um ‘laptop’ [...]”, e vão além ao afirmar que “Conexão fácil de fontes de informação “públicas” que costumavam ser guardadas em gavetas de arquivos em Albuquerque e Atlanta, mas agora são, ambas, eletronicamente acessíveis da Argélia – isso é novo também.”

Assim, quando o E-Gov publiciza dados estatísticos, apesar de objetivar o respeito aos princípios da transparência e da acessibilidade, deve considerar a potencial ameaça à privacidade dos indivíduos envolvidos. Quanto maior o número de informações colhidas, armazenadas, tratadas e, quiçá, publicadas a respeito de determinado grupo de pessoas, mais completo será o perfil traçado sobre cada uma, especialmente se forem recombinações os bancos de dados. E é por essas razões que o tema da privacidade ganha relevo na atuação do Governo Eletrônico: o governo é responsável por uma das maiores concentrações de dados pessoais dos cidadãos. Tal condição demanda ir além da abstenção de divulgação descuidada de dados pessoais, para considerar também medidas de proteção e instrução do cidadão para o uso de serviços do E-Gov.

É sobre esse novo papel que versará o próximo tópico, que destaca a necessidade de atuação preventiva e preparatória a ser empreendida pelo Estado ao ofertar serviços

do Governo Eletrônico.

3 A PRIVACIDADE DO CIDADÃO USUÁRIO DO GOVERNO ELETRÔNICO: medidas de proteção adotadas no Brasil.

Desde suas ações iniciais, o E-Gov visou à possibilidade de disseminação rápida e barata de informações por meio da Internet. Um de seus primeiros projetos, o “Infovia Brasília”, envolveu a instalação de sistemas de cabos de fibra óptica que conectavam os prédios da Administração Pública em Brasília, permitindo a transmissão instantânea de dados entre diferentes órgãos do governo.

Era o começo da era de digitalização de informações acerca de cidadãos e do governo, a qual seguiu avançando conforme as tecnologias evoluíram, e até então tem seu auge na proposta de criação de um banco universal de dados “públicos”, que por ora se constitui em registros que estão disponíveis oficialmente apenas entre órgãos do governo, não podendo ser acessado por particulares sem autorização específica.

Essas restrições referentes ao acesso aos dados pessoais do cidadão, todavia, não impedem a sua circulação pela Internet, o que os coloca em situação de vulnerabilidade devido à possibilidade de o sistema ser atacado por *hackers*. Assim, observando-se essa iniciativa à luz de todos os riscos já apresentados concernentes à disponibilização de dados na Internet, denota-se que esse benefício em favor da desburocratização pode se tornar, nas mãos de particulares, fonte de ameaças aos direitos fundamentais dos cidadãos.

A situação de vulnerabilidade aos direitos fundamentais dos cidadãos não ocorre apenas pela exposição de dados, muitos deles reveladores de aspectos de sua intimidade. Ocorre também em razão do acesso de outros particulares aos dados pessoais disponibilizados em páginas governamentais, o que permite o repasse de dados pessoais a terceiros, com a conseqüente exposição do usuário às novas práticas do ambiente virtual, como a publicidade via *spam*, por exemplo.

Além dos dados obtidos irregularmente por atuação dos particulares que violam os sistemas de segurança, deve-se considerar que há aqueles disponíveis diretamente nos *sites* do E-Gov. Destes se exige ainda maior segurança, pois muitas vezes esse é o único meio para o cidadão prestar informações ao Estado ou dele receber determinados serviços (a exemplo de inscrição em concursos públicos). Logo, o acesso desautorizado, a falta de zelo no armazenamento e tratamento dos dados coletados por páginas

governamentais constituem violação inigualável de direitos fundamentais, já que em muitos casos o cidadão sequer tem direito de escolha em disponibilizar ou não as informações.

Os órgãos que integram a Administração Pública brasileira não ignoram tais situações de riscos, tanto que os documentos oficiais que regulamentam a implantação do E-Gov dedicam grande destaque aos padrões de interoperabilidade (e-PING), cartilhas com instruções técnicas e gerais sobre criação de páginas na Internet por órgãos públicos, nas quais se verificam os critérios de segurança adotados.

Na versão de 2011 do Documento de Referência e-PING, identificam-se diversas medidas previstas que visam à proteção e o respeito a princípios de segurança digital, tais como: a) disponibilidade; b) integridade; c) autenticidade e d) confidencialidade dos dados. Dentre elas, interessa destacar que a “interoperabilidade na prestação dos serviços de governo eletrônico deve considerar o nível de segurança requerido pelo serviço, com a máxima transparência” e “o uso de criptografia e certificação digital, para a proteção do tráfego, armazenamento de dados, controle de acesso, assinatura digital e assinatura de código, deve estar em conformidade com as regras da ICP-Brasil [Infra-Estrutura de Chaves Públicas Brasileira].”

A preocupação com a segurança do sistema se manifesta em várias passagens do documento, destacando-se:

O cidadão deve se sentir confortável e ter confiança no sistema ao fornecer informações ao governo. Termos de uso, segurança e privacidade devem estar escritos de forma clara, objetiva e de fácil visualização.

A segurança do sítio e dos sistemas envolvidos tem um impacto significativo na confiabilidade e na imagem do órgão perante o cidadão. Os sítios oficiais devem garantir a confidencialidade das informações de caráter pessoal armazenadas em suas bases de dados, sejam elas relativas aos usuários ou pessoas que compõem a Administração Pública [...]

Esse Guia ainda cita as principais regulamentações que compõem a política de segurança das páginas governamentais, destacando-se: a) o Decreto nº 3.505, de 13 de junho de 2000; b) a Portaria nº 31 GSIPR/CH, de 6 de outubro de 2008; c) as orientações da Resolução nº 07, de 29 de julho de 2002; d) as orientações do GT de Segurança dos Padrões de Interoperabilidade de Governo Eletrônico (e-PING), institucionalizado pela Portaria nº 5, de 14 de Julho de 2005.

Nas duas referências fica expresso o reconhecimento da importância da segurança no tratamento dos dados digitalizados por parte da Administração Pública, sendo que o primeiro faz menção direta à ICP-Brasil, importante medida técnica que possibilita a

certeza de que os dados enviados pela Internet chegarão intactos a seu destino, e numa forma que somente o destinatário poderá acessá-los. Essa Infra-Estrutura também está citada nos textos da resolução nº 07 de 2002, que deixa a encargo da ICP-Brasil a certificação das páginas governamentais – na Resolução remete-se ainda ao Decreto nº 3.396 de 2001, que dispõe sobre os serviços de certificação digital, também dependentes da ICP-Brasil. A Portaria nº 31 de 2008 institui a Rede Nacional de Segurança da Informação e Criptografia (RENASIC), por sua vez prevista no Decreto nº 3.505 de 2000, que versa sobre a Política de Segurança da Informação nos órgãos públicos. A Portaria nº 5 de 2005, por sua vez, é estruturante dessa Política porque cria a coordenação do e-PING, responsável por manter a atualização das cartilhas.

Evidencia-se, diante dessa brevíssima exposição, que nos documentos que normatizam o E-Gov há preocupação com os aspectos técnicos de confiabilidade do sistema e que o Governo Brasileiro realiza esforços em atualização tecnológica para manter padrões mínimos de segurança das informações por ele recebidas e tratadas.

A despeito disso, estiveram em destaque na mídia fatos alarmantes ocorridos em 2010 por falhas de segurança nos sistemas públicos, como o acesso desprotegido a dados pessoais e sigilosos dos estudantes que realizaram o Exame Nacional de Ensino Médio (ENEM) em 2007, 2008 e 2009, e o vazamento de dados de contribuintes do imposto de renda. A relevância desses acontecimentos reside no fato de, em ambos os casos, ter sido alegado pela Administração Pública algum fator externo às limitações do controle técnico dos sistemas. Nas duas situações, o ocorrido se deu pela quebra do sigilo das informações por parte de algum de seus usuários autorizados: no caso do ENEM, alguma das instituições que possuía a senha do *site* fez uso indevido dela, e no caso do imposto de renda, concluiu-se que funcionários que trabalhavam com os bancos de dados estavam acessando-os sem necessidade.

Como já descrito na seção anterior, no entanto, deve-se lembrar que a novidade não está no uso indevido de informações pelas pessoas, mas pela ampliação de possibilidades desse uso que ocorre com as novas tecnologias. O número de cidadãos utilizando serviços do governo no meio virtual aumentou mais de 50% num intervalo de cinco anos, chegando a 27% da população brasileira em 2009. Assim, considerando o crescimento já registrado, a expectativa é que nos próximos anos haja considerável aumento no número de usuários do E-Gov, o que impõe que se observe atentamente a implementação de mecanismos de segurança nos sistemas.

Nesse contexto, existem algumas iniciativas em documentos que mencionam

padrões de serviços do E-Gov mais voltados à interface das páginas, aos mecanismos com os quais o cidadão tem contato direto ao acessar um *site* governamental. Quanto a esses aspectos, algumas previsões são feitas na já mencionada Resolução nº 7, de 2002, cujo art. 5º determina que os sítios governamentais devem: a) ser de fácil legibilidade; b) apresentar os conteúdos de forma clara, simples e objetiva, mantendo-os atualizados; c) usar linguagem direta e simples nas páginas iniciais; d) utilizar imagens de maneira cuidadosa e somente quando associadas diretamente ao órgão ou serviço; e) manter todo o ciclo de transição do serviço dentro do próprio sítio quando ele for disponível por meio de formulários.

Essa resolução também dispõe sobre organização do conteúdo dos *sites*, funcionamento dos mecanismos interativos contidos neles e manutenção de sua acessibilidade, estabelecendo objetivos de acessibilidade e confiabilidade. Entretanto, não existe uma regulamentação específica voltada a instruir o usuário para que ele possa minimizar os riscos que corre por meio de ações próprias. Todas as ações previstas no capítulo VI da referida Resolução, intitulado “Da segurança dos sítios”, são atos unilaterais de implementação da Administração Pública

O exame dos documentos indica a pouca importância conferida à educação do cidadão usuário dos serviços públicos *online*. Segundo apurado na 5ª Edição da Pesquisa sobre o Uso das Tecnologias da Informação e Comunicação (TICs) no Brasil, 13% dos entrevistados que acessam a Internet afirmaram não utilizar o E-Gov por considerarem muito complicado ter contato com a Administração Pública por meio eletrônico, o que só corrobora a necessidade de o Governo adotar políticas públicas com vistas à preparação da população para o Governo Eletrônico.

Defende-se, pois, que o tema do Governo Eletrônico não seja tratado apenas pelo ângulo da Administração Pública, reduzindo-se o papel do cidadão a mero *usuário* ou *consumidor* de informações e serviços disponibilizados pelos órgãos da Administração Pública. Como o tema envolve uma nova dimensão da cidadania, como acima defendido, sua promoção requer ações específicas, devidamente programadas, dotadas de orçamento próprio, de pessoal treinado para tratar do assunto, observando-se, sobretudo, a continuidade das ações, haja vista que a constante incorporação de novos usuários da Internet importará na constante preparação dos novos internautas para se integrar e participar do Governo Eletrônico.

Convém destacar que ao defender essa tese, emprega-se o termo política pública como as ações relacionadas à esfera do público e que objetivam a responder às

questões coletivas que envolvem o Estado na esfera de suas ações governamentais. Seu conceito, no entanto, vai para além do meramente estatal, pois como salienta Schmidt, as políticas públicas se desdobram em estatal e não-estatal, e esse termo pode ser utilizado ora para indicar um campo de atividade, ora um propósito político que se efetivará a partir de um programa de ações. No presente caso, entende-se que tanto pode ser tomada como um campo de atividade, quanto como programa de ações, mostrando-se salutar, inclusive, que se firmem parcerias com instituições privadas (academias, empresas que exploram as mídias tradicionais), tanto para divulgar os benefícios do E-Gov junto à população, como também para orientá-la para a adoção de medidas de segurança.

Tais medidas devem ser implementadas com certa prioridade, pois o despreparo da população não é o único fator que impede o acesso aos serviços prestados *online*: conforme apurado na 1ª Pesquisa sobre o Governo Eletrônico, realizada no ano de 2010 pelo Comitê Gestor da Internet no Brasil (CGI.br), embora cerca de 70% dos entrevistados tenha se utilizado de serviços de Governo Eletrônico nos últimos doze meses que antecederam a pesquisa, apenas 22% sentem-se seguros em colocar dados pessoais, como RG e CPF, na Internet, e 26%, em *sites* do governo. Esse dado mostra que os usuários ainda não confiam suficientemente nos serviços ofertados pelo Governo, o que aponta para a necessidade de a Administração Pública propor medidas nessa seara.

CONSIDERAÇÕES FINAIS

O presente trabalho evidenciou a utilização das tecnologias informacionais, como instrumento gerador de grandes possibilidades na maneira de interação entre cidadão e Administração Pública, e crescentes iniciativas para aproveitar esse potencial. No entanto, percebem-se alguns aspectos frágeis na implementação dessas ações, especialmente quanto à garantia dos direitos fundamentais que abrangem dados pessoais.

Apesar do reconhecimento pelo Governo brasileiro da importância de se garantir a privacidade dos dados do cidadão e de ser perceptível a preocupação com a segurança do sistema, reiteradamente referidos nos documentos do E-Gov, o cotejo entre a previsão constitucional de respeito aos direitos fundamentais dos cidadãos, os documentos oficiais produzidos no âmbito desse projeto e, sobretudo, a percepção dos próprios usuários participantes da Pesquisa sobre o Governo Eletrônico no Brasil revela pontos de fragilidade na proteção desses direitos. O ponto de tensão reside no fato de que,

enquanto os documentos e as técnicas aproximam-se cada vez mais dos objetivos idealizados para atender às demandas da sociedade informacional, as práticas de construção de páginas não se mostram suficientemente adequadas às imprevisibilidades de seu uso pelos cidadãos. Tal situação se deve em parte pela incipiente experiência do Governo Eletrônico no Brasil, bem como pela falta de habilidade dos internautas que acessam os serviços, que não se encontram devidamente preparados para exercer essa nova forma de cidadania, a cidadania virtual.

Defende-se, pois, a necessidade de o Governo Brasileiro, ao lado dos investimentos no acesso da população às tecnologias informacionais e das ações visando à estruturação dos órgãos que integram a Administração Pública, priorize programas governamentais destinados a: a) divulgar junto à população os serviços que são ofertados *online*; b) usar as mídias tradicionais e com maior penetração para incentivar a população a acessar os *sites* e portais governamentais, acompanhando as ações e programas que são desenvolvidos pelo Estado, por meio das mídias tradicionais; c) promover a pronta resposta às demandas apresentadas pelo cidadão, para que se perceba a efetividade da comunicação realizada entre a Administração Pública e o administrado; d) preparar campanhas de esclarecimento sobre medidas de prevenção e de proteção de dados pessoais lançados na Internet; e) promover medidas efetivas de proteção e segurança dos *sites* governamentais. Urge, portanto, estabelecer políticas públicas direcionadas à preparar os brasileiros para o exercício da cidadania virtual.

REFERÊNCIAS

ABELSON, Hal; LEDEEN, Ken; LEWIS, Harry. *Blown to Bits*. Addison-Wesley, 2008.

Disponível em: <http://www.bitsbook.com/wp-content/uploads/2008/12/B2B_3.pdf>.

Acesso em: 6 fev. 2011.

ARENDT, Hannah. *A Condição Humana*. 8ª ed. Rio de Janeiro: Forense Universitária, 1997.

BRASIL. Comitê Executivo de Governo Eletrônico. *Documento de Referência e-PING*.

Disponível em:

<<http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padrees-de-interoperabilidade/versoes-do-documento-da-e-ping>>. Acesso em: 15 fev. 2011.

_____. _____. *Resolução n° 07 de 29 de julho de 2002*. Disponível em:
<<http://www.governoeletronico.gov.br/o-gov.br/legislacao/resolucoes>>. Acesso em: 15 fev. 2011.

_____. Comitê Gestor da Internet no Brasil (CGI.br). *Pesquisa Sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil 2005-2009*. São Paulo, Comitê Gestor da Internet no Brasil: 2010.

_____. _____. *Pesquisa sobre o uso das tecnologias da informação e comunicação no Brasil 2009*. Comitê Gestor da Internet no Brasil, 2010 a. Disponível em: <
<http://www.cetic.br/tic/2009/index.htm>>. Acesso em: 20 ago 2010.

_____. _____. *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil: TIC Governo Eletrônico - 2010 = Survey on the use of information and communication technologies in Brazil : ICT eletronic government - 2010 / [coordenação executiva e editorial/executive and editorial coordination, Alexandre F. Barbosa ; tradução/translation Linguagem Idiomas]. -- São Paulo: Comitê Gestor da Internet no Brasil, 2010*

_____. *Constituição da República Federativa do Brasil*. Disponível em:
<http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 4 fev. 2011.

_____, Grupo de Trabalho Interministerial Novas Formas Eletrônicas de Interação. *Política de Governo Eletrônico para o Poder Executivo Federal*. Brasília, 20 set. 2000. Disponível em:
<http://www.governoeletronico.gov.br/anexos/E15_90proposta_de_politica_de_governo_eletronico.pdf>. Acesso em: 15 fev. 2011. p. 2.

_____, Ministério da Fazenda. *Receita Federal do Brasil*. Disponível em:
<<http://www.receita.fazenda.gov.br/>>, Acesso em: 15 fev. 2011.

_____. Núcleo de Informação e Coordenação do Ponto BR. Comitê Gestor da Internet: pesquisa sobre o uso das tecnologias da informação e comunicação no Brasil 2009.

Comitê Gestor da Internet no Brasil, 2010. Disponível em:

<<http://www.cetic.br/tic/2009/index.htm>>. Acesso em: 20 ago 2010.

_____, Presidência da República. *Decreto nº 6.932, de 11 de agosto de 2009*. Brasília, 11 ago. 2009. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D6932.htm>. Acesso: em 15 fev. 2011.

CARDOSO, Gustavo. *A mídia na sociedade em rede: filtros, vitrines, notícias*. Rio de Janeiro: Editora FGV, 2007.

CASTELLS, Manuel. *A galáxia da Internet: reflexões sobre a Internet, negócios e a sociedade*. Traduzido por Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

_____. *A sociedade em rede*. 11. ed. Traduzido por Roneide Venâncio Majer. São Paulo: Paz e Terra, 2008. v. 1.

COOLEY apud WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review, Vol. IV, nº 5. Boston, 1890. Disponível em:

<http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> Acesso em: 6 fev 2011.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Disponível em:

<<http://www.doneda.net/artigos/tese.cap1.pdf>>. Acesso em: 7 fev. 2011.

G1. *Vazamento de dados de estudantes do ENEM será apurado, diz Inep*. 04 ago. 2010.

Disponível em:

<<http://g1.globo.com/vestibular-e-educacao/noticia/2010/08/vazamento-de-dados-de-estudantes-do-enem-sera-apurado-diz-inep.html>>. Acesso em: 27 abr. 2011.

GRPCOM, Grupo Paranaense de Comunicação. *Vazamento pode atingir 2,6 mil contribuintes, admite Receita*. 07 set. 2010. Disponível em:

<<http://www.gazetadopovo.com.br/votoconsciente/conteudo.phtml?tl=1&id=1044015&tit=Vazamento-pode-atingir-26-mil-contribuintes-admite-Receita>>. Acesso em: 27 abr. 2011.

FAGÚNDEZ, Paulo Roney Ávila. *A Virtualidade*. In: Direito e Informática. ROVER, Aires José (org.). Barueri: Manole, 2004. p. 124.

PÉREZ LUÑO, Antonio-Enrique. *¿Ciberciudadaní@ o ciudadaní@.com?* Barcelona: Editorial Gedisa, 2004.

_____. *Derechos humanos, Estado de Derecho y Constitución*. 9. ed. Madri: Editorial Tecnos, 2005.

RNP, Rede Nacional de Ensino e Pesquisa. *A Internet no Brasil*. 22 ago. 2009. Disponível em: <<http://www.rnp.br/noticias/imprensa/2001/not-imp-010310.html>>. Acesso em: 15 fev. 2011.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 4. ed. Porto Alegre: Livraria do Advogado Editora, 2004.

SAWAYA, Márcia Regina. *Dicionário de informática & Internet*. 3. ed. São Paulo: Nobel, 1999

SÊDA, Edson. *A proteção integral: um relato sobre o cumprimento do novo Direito da Criança e do Adolescente na América Latina*. 3. ed. Campinas: E. Seda: 1995.

SCHMIDT, João Pedro. Para entender as políticas públicas: aspectos conceituais e metodológicos. In: REIS, Jorge Renato dos; LEAL, Rogério Gesta. *Direitos Sociais e Políticas Públicas: desafios contemporâneos*. Santa Cruz do Sul: EDUNISC, 2008, p. 2306-2333.

VEIGA, Luiz Adolfo Olsen; ROVER, Aires J. *DADOS E INFORMAÇÕES NA INTERNET: é legítimo o uso de robôs para formação de base de dados do cliente?* In: Direito e Informática. ROVER, Aires José (org.). Barueri: Manole, 2004.

WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review, Vol. IV, nº 5. Boston, 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> Acesso em: 6 fev 2011.