A WEB 2.0 NO E-GOVERNO, APLICAÇÕES EM SEGURANÇA PÚBLICA E POTENCIAIS PROBLEMAS DE PRIVACIDADE[1]

José Gustavo Viégas Carneiro[*]
Vinícius Ramos Toledo Ferraz[**]
Maria Cecília Vecchiato Saenz Carneiro[***]
José Silvio Govone***
Antônio Carlos Simões Pião***
Farid Nourani****

RESUMO Neste artigo, são descritos conceitos de Web 2.0 e de e-Governo, destacando as suas afinidades e também as possíveis aplicações para a aproximação do Estado com os cidadãos nos processos decisórios entre os mesmos. Defende-se a utilização do paradigma Web 2.0 como facilitador do e-Governo, focando nas aplicações para definição de políticas de Segurança Pública. Outra questão abordada é sobre o acesso a informação e o seu controle para garantir a intimidade da pessoa, conforme o paradigma constitucional vigente e garantidor desta intimidade pessoal. Serão citadas as novas tecnologias que estão sendo implantadas nas instituições policiais e privadas com o objetivo de contribuir com o desenvolvimento pacífico da sociedade e como as tecnologias de informação e comunicação podem auxiliar o cidadão.

PALAVRAS-CHAVE: E-governo. Segurança pública. Tecnologias de informação, Web 2.0. Controle da informação digital.

1. INTRODUÇÃO

A interação de Instituições Públicas, no contexto atual em que se apresenta a violência social brasileira, é de suma importância na garantia do Estado Democrático de Direito, compartilhando saberes e práticas vivências, capaz de forma transversal fundamentar novos valores éticos garantidores da justiça social.

---

[1] texto originado de pesquisas realizadas pelo grupo de estudo GestaFUV - Grupo de Estudo e Análise de Fenômenos Urbanos da Violência

*Mestre em Direito, delegado de Policia Civil da Seccional de Rio Claro e Prof. da Academia de Policia Civil de São Paulo

**Discente do Curso de Bacharelado em Ciências da Computação, IGCE,UNESP.

***Doutores em Ciências da Engenharia Ambiental, docentes do Depto. Estatística, Matemática Aplicada e Computação, IGCE, UNESP. Caixa Postal 178, CEP 13500-230 Rio Claro, SP. e-mail: jsgovone@rc.unesp.br

**** Mestre em Engenharia Elétrica, docente Depto. Estatística, Matemática Aplicada e Computação, IGCE, UNESP. Rio Claro, SP. e-mail faridn@rc.unesp.br

A construção de novos saberes pressupõe a gestão do conhecimento através de sistemas de inteligência, inclusive, a policial.

A criminalidade e os fenômenos da violência atuam diretamente na conformação dos espaços, principalmente, os urbanos. Novas formas da criminalidade, como a organizada, promovem profundas alterações socioeconômicas, espaciais e nas conformações dos poderes estatais visto que, atuam diretamente nas suas estruturas. A complexidade dos novos crimes, dentre os quais, os dos espaços fictos, a exemplo dos espaços digitais, obriga que o gestor ou cientista que se dedicam a estes fenômenos relacionados à violência tenha percepções acuradas, inclusive, monitorando rotas do crime.

Com o advento da cibernética é que se abrem novas oportunidades às ciências criminais. Os "fractais" ou frações podem ser utilizados para a reconstrução do todo. E este princípio tem aplicação na investigação. Porém, é necessário integrar todas as tecnologias disponíveis para estudar os fenômenos da criminalidade e investigar os atos ilícitos. A padronização e integração de bases de dados e o uso de práticas de desenvolvimento já consagradas, são essenciais para a interoperabilidade e o potencial colaborativo das tecnologias que dêem apoio à análise criminal.

Atualmente, o principal desafio no Brasil e a integração dos setores de inteligência, criando-se um Sistema Único de Segurança Pública que tenha a participação da Abin, das unidades de inteligência policial (Polícia Civil, Polícia Militar, Polícia Federal, Polícia Rodoviária Federal, Polícia Ferroviária Federal), os setores de inteligência dos Comandos Militares (Exército, Marinha e Aeronáutica), da inteligência de órgãos de fiscalização (Receita Federal, INSS e IBAMA), pelos setores de inteligência direcionados à área financeira coordenada pela COAF, cuja missão é combater a lavagem de dinheiro.

Avanços já aconteceram é atualmente já existe um banco de dados alocado na RENISP (Rede Nacional de Inteligência em Segurança Pública), que já é atualizado em tempo real, facilitando trocas de informações entre as instituições responsáveis pelo sistema de segurança pública.

No Estado de São Paulo, a Polícia Civil já conta com o Departamento de Inteligência Policial – DIPOL, responsável pela coordenação da produção de conhecimentos sensíveis e de suma importância à gestão da segurança pública. A inteligência policial tem por missão

criar doutrinas para a defesa da sociedade e do Estado, obtenção de informações, produção de conhecimento, estudar estados da mente, coordenar operações de inteligência, e, finalmente, desenvolver tecnologias aplicáveis à segurança pública a exemplo, de sistemas de tecnologia da informação e comunicação.

Alguns sistemas tecnológicos já estão em implantação com olhos na e-governança da sociedade com objetivo de melhorar o serviço público da segurança, podendo ser mencionados:

- ***Sistema Guardião*** cuja tecnologia nacional foi desenvolvida em Santa Catarina, constituindo-se num sofisticado programa de computador que permite interceptar até 400 linhas telefônicas simultaneamente, permitindo também cruzar dados com arquivos policiais do País e do mundo;

- ***Registro digital de ocorrências (RDO)*** que substituirá o arcaico Boletim de Ocorrência, sendo um sistema informatizado que permite alimentar "online" os bancos de dados da polícia e dá acesso imediato a toda a rede policial;

- ***Sistema Ômega*** – é um sistema de inteligência artificial que integra informações e as qualifica junto a toda a comunidade de inteligência do sistema nacional;

- ***Infocrim*** – desenvolvido pela *Prodesp* (Empresa de Processamento de Dados de São Paulo), constitui-se de um banco de dados (SYSBO) que permite mapear as ocorrências policiais. Este sistema é muito criticado diante da falta de rigor científico na coleta de dados, necessário aos aplicativos de SIG (Sistemas de Informação Geográfica) adequados;

- ***Infoseg*** – integra as informações entre os organismos policiais e as informações do Poder Judiciário.

Estes sistemas computacionais têm contribuído de maneira decisiva para o uso inteligente dos recursos policiais. Por outro lado, estes recursos tecnológicos têm potencial para evoluir a ponto de invadir a intimidade de um cidadão, o que pode ser negativo para sua vida pessoal. A questão crucial que se apresenta com as novas tecnologias é a viabilização de um Estado Policial e qual o grau de abdicação da privacidade em favor da segurança pública.

2. A WEB 2.0 E SUAS AFINIDADES COM A GOVERNANÇA ELETRÔNICA

O advento da *World Wilde Web*, um dos serviços da rede mundial de computadores, facilitou consideravelmente o acesso e a publicação de informações (Berners-Lee e Cailliau, 1990). Com exceção de certos conteúdos restritos pela lei internacional e de raras censuras locais, a *Web* é um território livre para o compartilhamento de idéias. Qualquer indivíduo com acesso à rede e um conhecimento técnico mínimo pode expor seu ponto de vista para todos os interessados em sabê-lo.

A ascensão de um novo paradigma na Internet, referida pelo termo "Web 2.0", tem influenciado sensivelmente a maneira como acessamos e produzimos o conhecimento (Sangüesa e Fages, 2007). Nesse paradigma, o internauta comum passa a ser o principal ator dos processos de produção do conhecimento – diferente da postura anteriormente mais comum de simples receptor de informações.

A Web 2.0 é uma atitude, não uma tecnologia (O'Reilly, 2005). Além dos conceitos de participação colaborativa, o termo agrega um conjunto de práticas consagradas de desenvolvimento de sistemas para torná-los colaborativos – tanto no seu uso quando na sua modificação - e interoperáveis, que é o potencial de um sistema ser integrado a outro. Tais práticas consistem na padronização dos bancos de dados, do transporte desses dados, da documentação dos sistemas, das técnicas de engenharia de software e, principalmente, na padronização das tecnologias de desenvolvimento *Web*, regulamentadas pelo W3C (*World Wide Web Consortium*).

Do ponto de vista econômico, a Web 2.0 define os produtos como serviços e os consumidores como usuários desses serviços e seus próprios supervisores, sendo a qualidade de serviço (*QoS*) atestada pela freqüência de uso do mesmo e, para as aplicações comerciais, pela receita advinda da publicidade. Do ponto de vista social, o internauta se torna elemento essencial num processo colaborativo de manutenção de comunidades virtuais e produção do conhecimento. Do ponto de vista político, existe a oportunidade de considerar o internauta como cidadão e a "nova *Web*" como a plataforma de aproximação com o estado e com o processo democrático.

Neste cenário, temos que a atual realidade da *Web* – razoavelmente dominada pelos conceitos de Web 2.0 – é altamente favorável ao desenvolvimento de novas e ricas aplicações de governança, seja com objetivo de aproximar o cidadão do Estado, seja no sentido de

integrar diferentes instituições nas atividades relacionadas a um objetivo comum, como por exemplo, os diversos poderes envolvidos na questão da Segurança Pública.

Apesar da utilidade democrática dos sistemas de governança eletrônica, faz-se necessária, no entanto, uma profunda reflexão acerca da segurança desses sistemas e do potencial de violação de privacidade que trás a padronização de técnicas de desenvolvimento. Uma vez que os bancos de dados e as técnicas de desenvolvimento dos sistemas são padronizados, aumenta o número de pessoas que terá, teoricamente, o potencial para desvendar do funcionamento interno de tais sistemas e acessar dados confidenciais. No mesmo sentido, os sistemas colaborativos freqüentemente levam o usuário a disponibilizar voluntariamente dados pessoais, que devem ser protegidos, de alguma maneira, do uso ilícito desses dados por outros usuários.

3. PRIVACIDADE, TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA PÚBLICA

Vivencia-se atualmente uma era digital que vem provocando profundas modificações comportamentais e re-organizações do espaço, ocorrendo uma tensão entre o privado e o público. Esta sociedade, chamada por Castells (1999) de “Sociedade em Rede”, configuram-se diversos e cada vez mais complexos desafios para governos, organizações e pessoas. Entre eles o desenvolvimento acelerado das Tecnologias de Informação e Comunicação (TICs) e a grande quantidade de informações sendo produzida e circulando na Internet.

Estas tecnologias de informação e comunicação ganham destaque no mundo financeiro, pois todo o banco de informações de uma pessoa física ou jurídica passa a ter considerável valor mercantil, muitas vezes, superior ao valor patrimonial imobilizado, passando a ser considerados como uma *commodity* (GALVÃO, 1999).

Surgem novos paradigmas na economia globalizada, dentre os quais a passagem da sociedade industrial para a sociedade da informação.

Com o valor estratégico conferido à informação e a conexão da sociedade em rede, surgem, além de inúmeras facilidades e benefícios, algumas questões éticas a serem discutidas e avaliadas. Uma delas é a privacidade da informação, um grande desafio e assunto de interesse de toda a sociedade.

Na ordem jurídica oportuno destacar alguns preceitos legais. De acordo com a Declaração Universal dos Direitos Humanos (art. 12), adotada pela ONU em 1948, a privacidade do indivíduo é um dos direitos humanos fundamentais a serem respeitados e assegurados.

No Brasil, a liberdade de preservar ou não a própria intimidade é um direito do cidadão. (PAESANI, 2000) O direito à privacidade é também assegurado pela Constituição Federal (artigo 5º, incisos X, XI e XII).

Para Dyson (1998, p. 217), "a privacidade real - que é o respeito pelas pessoas e não mera ausência de dados – depende do discernimento humano e do bom senso". A privacidade está ainda ligada à vigilância e à segurança. É preciso, portanto, que se encontre um equilíbrio para estes elementos (controle, privacidade e segurança) de forma a garantir a preservação dos direitos tanto coletivos como individuais. No entanto, esta equação na prática não tem se mostrado fácil. (SÊMOLA, 2001)

4. E-GOVERNO E SEGURANÇA PÚBLICA

Segundo Zweers & Planqué (2001, p. 92), o conceito de e-Governo pode-se dizer:

> Governo Eletrônico é um conceito emergente que objetiva fornecer ou tornar disponível informações, serviços ou produtos, através de meio eletrônico, a partir ou através de orgãos públicos, a qualquer momento, local e cidadão, de modo a agregar valor a todos os stakeholders envolvidos com a esfera pública[2].

No Estado de São Paulo algumas experiências exitosas de e-Governo tem ocorrido na Segurança Pública, facilitando o relacionamento do cidadão como o Estado através da Web.

A Delegacia de Polícia Digitalizada permite ao cidadão elaborar algumas ocorrências policias pela internet e, pode obter cópia imediata imprimindo em sua configuração computacional. São registradas ocorrências sobre furtos de veículos, objetos, etc., como também extravios de documentos.

2Tradução livre do Coordenador do Portal EBAPE - Prof. Luiz Antonio Joia - http://www.ebape.fgv.br/e_government/asp/dsp_oquee.asp

A ocorrência é encaminhada a circunscrição policial da área do fato para seu prosseguimento, sendo que a referida Delegacia de Polícia Digital atende todo o Estado de São Paulo.

Outro exemplo de e-Governo também acontece no Departamento Estadual de Trânsito (Detran/SP), sendo que o proprietário de veículo pode fazer a documentação por meio de rede bancária.

Também na e-governança o Estado de São Paulo, utilizando-se da *Web*, implantou o *Poupatempo Online*, permitindo ao cidadão a obtenção imediata de documentos de veículos, habilitação, documento de identidade e antecedentes criminais.

Por meio da *Web* é possível acessar o *site* da Secretaria da Segurança Pública e ter acesso a fotos de pessoas procuradas, orientações sobre segurança, endereços de unidades policiais e também fazer denúncias, inclusive, anônimas, sobre criminosos e abusos policiais.

No *site* da Secretaria da Segurança Pública também é possível ter acesso a algumas estatísticas policiais, porém, constantemente os dados e gráficos estatísticos exibidos são criticados pela sociedade e comunidade científica que denunciam a falta de rigorismos metodológicos e de suas manipulações para fins políticos.

Um exemplo estrangeiro e pioneiro na implantação de um sistema complexo e bastante completo de e-Governo com ênfase na segurança pública é o município de San Francisco, nos EUA. Sua plataforma de mapeamento de ocorrências criminais na *Web* (www.sfgov.org/site/gis_index.asp) permite tanto aos membros do poder público quando aos cidadãos o acesso a uma base de dados geográfica atualizada em tempo real. Os níveis de acesso aos dados são controlados, restringindo os detalhes dos crimes (como por exemplo, as pessoas envolvidas) à polícia. O banco de dados criminal da polícia de San Francisco segue uma padronização rigorosa (Lowerly, 2004), o que permite a integração desses dados a outros sistemas – um dos conceitos da Web 2.0, a interoperabilidade.

Quanto à utilização dos conceitos de Web 2.0 em aplicações de e-Governo para segurança pública, há alguns exemplos nacionais e estrangeiros, inclusive algumas aplicações desenvolvidas por pesquisadores autônomos e instituições privadas que não se tratam de

ferramentas governamentais oficiais, o que não afeta sua utilidade pública, mas podem perder em confiabilidade dos dados em maior e menor grau.

Um grupo privado estadunidense reuniu dados de utilidade pública (inclusive criminais) de municípios e órgãos de imprensa através de parcerias e iniciativas e criou um grande portal chamado EveryBlock (www.everyblock.com) para publicação desses dados de maneira pura ou processada (através de mapeamentos ou estatísticas). Há grande confiabilidade nos dados por não envolver o cidadão na alimentação direta dessas bases, restrita aos dados fornecidos pelos órgãos parceiros.

Um exemplo nacional é o WikiCrimes (www.wikicrimes.org), ferramenta concebida por um grupo de pesquisas da Universidade de Fortaleza que permite o mapeamento colaborativo de ocorrências criminais, inclusive as não registradas oficialmente, pois as próprias vítimas podem registrar diretamente no site as ocorrências que consideraram um crime. Nesse caso a confiabilidade dos dados é de certa forma comprometida, mas podem ser comparadas com notícias da imprensa para diminuir o problema.

5. CONCLUSÕES

Nos últimos anos o avanço da *Web* como plataforma de e-Governo facilitou o relacionamento do cidadão com o Estado, suprimindo a exacerbada burocracia cartorial da cultura brasileira. São os exemplos exitosos da Delegacia de Polícia Digital e do *Poupatempo Online*.

Parte destes avanços, os conceitos da Web 2.0 têm favorecido o desenvolvimento de ferramentas que aproximam o cidadão do Estado e a colaboração entre as instituições governamentais, pois facilita a criação de conhecimento colaborativo e fomenta a padronização dos dados, técnicas e tecnologias envolvidas. Os exemplos dados demonstram o potencial da aplicação dos conceitos de Web 2.0 nas ferramentas de e-Governo para Segurança Pública, mas levantam importantes questões no campo da segurança dos dados e da privacidade do cidadão.

A questão de como as tecnologias de informação e comunicação poderá afetar a privacidade, devassando-a em prol da coletividade no concernente à Segurança Pública, é crucial. Neste mesmo sentido, se faz oportuno que se elabore mecanismos de controle do

Estado sobre o uso das informações pessoais. Se a Constituição Federal de 1988 garantiu o acesso e a retificação dos dados pessoais do cidadão através do remédio jurídico do *habeas data,* por outro lado, a sociedade não se faz presente no controle das informações das agenciais estatais de inteligência, que podem eventualmente ser utilizadas para fins ilegítimos e ilegais.

São questões ainda recentes e que há de se buscar um equilíbrio entre a utilidade pública na Web e a intimidade das pessoas.

REFERÊNCIAS

CASTELLS, M. *Sociedade em Rede.* (A era da informação: economia, sociedade e cultura); Volume 1, São Paulo: Paz e Terra, 3a. ed., 1999.

DYSON, E. *Release 2.0*. A sociedade digital. Um roteiro da vida na Internet. Rio de Janeiro: Campus,1998.

GALVÃO, A. P. A informação como commodity: mensurando o setor de informações em uma nova economia. *Ciência da Informação*. Brasília, v.28, n.1, p.67-71, jan. 1999.

PAESANI, L. M. *Direito e Internet*; Liberdade de Informação, Privacidade e Responsabilidade Civil. Atlas. São Paulo. 2000.

SÊMOLA, Marcos. Hora da escolha: privacidade ou mais segurança. *Módulo Security*,2001. <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=244&pagecounter=0&idiom=0> Acesso em: 13 jul. 2004.

BRASIL. Constituição (1998). *Constituição da República Federativa do Brasil***.** Org. Alexandre de Moraes. 17.ed., São Paulo: Atlas, 2001.

BRASIL. *Código de Defesa do Consumidor***:** Lei nº 8.078, de 11.9.1990. 13. ed. São Paulo: Atlas, 2000.

Carneiro, J.G.V.; Lombardo, M.A.; Carneiro, M.C.V.S. *Georreferenciamento e Inteligência Policial – construindo políticas públicas de segurança***.** Anais do VII Seminário de Pós-graduação em Geografia da Unesp – campus Rio Claro, ISBN: 978-85-88454-14-9, 2007, pp.242-60.

Zweers K & Planqué K. (2001) - *Electronic Government. From a Organizational Based Perspective Towards a Client Oriented Approach***,** In: D*esigning E-Government*, Prins J.E.J. (ed.), Kluwer Law International, pp. 92

Berners-Lee, T.; Cailliau,R. *WorldWideWeb***:** Proposal for a HyperText Project. W3C, 1990. <http://www.w3.org/Proposal> Acesso em 11 de abril de 2008.

Sangüesa, R.; Fages, R. Good practice exchange from a Web 2.0 point of view. *European Journal of ePractice*. Vol. 1, Article 1, 2007. disponível em: <http://www.epracticejournal.eu/document/4157> Acesso em: Acesso em:11 abr. 2008.

O'Reilly, T. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *O'Reilly Media,* 2005. disponível em: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html> Acesso em:11 abr. 2008.

Lowerly, L. M. *Developing a Successful E-Government Strategy***.** UNPAN Documents, 2004. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN000343.pdf> Acesso em 11 de abril de 2008.