poliTICs
Uma publicação do Instituto Nupef • setembro / 2012 • www.politics.org.br

A nova base de dados de DNA brasileira:
solução de crimes ou erosão de direitos humanos?

poliTICs nº 13

Índice

Editorial

Esta décima terceira edição da poliTICs vem robusta – não apenas no tamanho, mas principalmente no peso político dos artigos que a compõem. Textos instigantes e reveladores nos mostram o quanto o cidadão brasileiro contemporâneo está suscetível em relação ao armazenamento, uso e processamento de seus dados pessoais. Trazemos nesta edição um alerta sobre novo Registro de Identidade Civil que, como mostram Danilo Doneda e Marta Kanashiro, carece de elementos que garantam a proteção dos indivíduos ao unificar diferentes sistemas de identificação da pessoa, vulnerabilizando os cidadãos em nome da "modernização".

Outra luz se acende quando abordamos o tema da nova lei que cria uma base de dados nacional de DNA – um projeto que, nos moldes em que está evoluindo, parece orientar-se muito mais pelo interesse na criação de novos mercados do que na proteção de quem quer que seja. O imperdível artigo de Helen Wallace, escrito com exclusividade para a poliTICs, chama a atenção sobre a falta de debate público a respeito de um projeto que pode ter implicações diretas e imprevisíveis para a vida de qualquer um de nós, cidadãos e cidadãs brasileiras.

Além das reflexões sobre o atual cenário distópico no que diz respeito à proteção de dados pessoais, privacidade e direitos humanos no país, esta edição traz também provocações sobre novas possibilidades de conexão à Internet através do uso de rádios cognitivos e dos espaços disponíveis no espectro radioelétrico – os "espaços em branco". Carlos Afonso explica como esta oportunidade está sendo explorada em outros países e aponta para a necessidade de os agentes reguladores brasileiros tratarem com responsabilidade esta alternativa às ofertas dos conglomerados de telecomunicações e de mídia.

Kelli Angelini conta a história da criação do SACI - Sistema de Administração de Conflitos de Internet para domínios no .br. Seu artigo detalha como opera o SACI e mostra a eficiência da solução de disputas de titularidades de nomes de domínio envolvendo principalmente marcas, nomes empresariais e artísticos.

O texto de Jeremy Malcolm vai direto ao ponto, afirmando que a governança da Internet está em crise. Além de evidenciar que vivemos num cenário de incoerência regulatória e de ausência de políticas globais consistentes sobre temas de governança da Internet, Jeremy também aponta para a necessidade de que exista uma organização capaz de desenvolver orientações sobre políticas globais de Internet, sugerindo as características que esta deveria ter para preencher o vácuo que o engessado IGF não foi capaz de ocupar. ●

▶ Esperamos que você aprecie a leitura, participe e opine – o espaço está aberto em **www.politics.org.br**

Um abraço,

Graciela Selaimen – *Editora da poliTICs*

> **Helen Wallace** Diretora do GeneWatch UK

A nova base de dados de DNA brasileira:

solução de crimes ou erosão de direitos humanos?

A nova lei brasileira no 12.654 de 28 de maio de 2012 cria uma base de dados nacional de DNA com o objetivo de ajudar a polícia a solucionar crimes. Entretanto, as garantias incluídas na lei são inadequadas para prevenir o mau uso desta base de dados para fins de vigilância, não garantem a proteção da privacidade e nem o respeito aos direitos humanos, assim como não asseguram prevenções quanto a possíveis erros do Judiciário. Enquanto isso, regulações estão sendo desenvolvidas que poderiam tratar de algumas destas questões – e mais do que nunca é importante que a sociedade civil esteja de fato engajada neste debate.

:: UM BREVE HISTÓRICO

O uso de análise de DNA como prova pode ter um papel importante na solução de crimes, mas bases de dados de DNA levantam uma série de preocupações com relação a vigilância, privacidade, direitos humanos e as potenciais falhas do sistema judicial. Algumas garantias importantes incluem: restrições sobre quando os dados e amostras podem ser recolhidos e retidos; padrões científicos e sistemas de controle de qualidade de serviços laboratoriais; e salvaguardas quanto ao uso destas provas nos tribunais.

A empresa norte-americana Life Technologies (proprietária da Applied Biosciences) está fazendo lobby globalmente para a expansão das bases de dados forenses de DNA para garantir que o mercado de teste de DNA se expanda – isso é feito através de sua empresa de lobby Gordon Thomas Honeywell Governmental Affairs (GTH).[1] A Life Technologies também financia grupos de vítimas de crimes para fazerem lobby pela criação de bases de dados de DNA, tanto de maneira direta quanto através de sua empresa de relações públicas Harris D. McKinney.[2,3,4,5] A Gordon Thomas Honeywell acredita que a nova lei brasileira provavelmente gerará uma onda de legislações similares em toda a América Latina.[6] A empresa de lobby também afirma, no mesmo artigo, que o Brasil está posicionado para tornar-se detentor da maior base de dados de DNA da América Latina – e uma das maiores do mundo.

A análise do DNA pode ajudar a solucionar crimes, mas o papel das bases de dados de DNA tem sido extrapolado. Argumentações falsas por parte de lobistas pode resultar na adoção de políticas que não são efetivas, ou que não valem a pena em termos de custo/benefício, ou ainda que falham em alcançar o equilíbrio apropriado entre a expansão deste tipo de bases de dados e a proteção da privacidade e dos direitos humanos das pessoas.

É, portanto, muito importante que quaisquer fragilidades na legislação sejam abordadas.

:: O PAPEL DAS BASES DE DADOS DE DNA NA SOLUÇÃO DE CRIMES

O uso de DNA em investigações criminais requer a coleta de amostras de DNA das cenas dos crimes. Mostras de material biológico (por exemplo, saliva, sangue, sêmen) são coletadas da cena e analisadas em laboratório. Os perfis genéticos computadorizados que são obtidos (uma sequência de números baseados em partes do DNA) podem então ser comparados com os perfis dos suspeitos, das vítimas e de outras pessoas, de forma a estabelecer quem esteve na cena investigada.

A interpretação de qualquer cruzamento de perfis com base no DNA depende das circunstâncias. Por exemplo, o sangue da vítima pode ser encontrado nas roupas de uma pessoa suspeita, mas outras provas são necessárias para estabelecer se a pessoa foi a autora do crime ou se estava tentando ajudar a vítima; a saliva de um suspeito pode ser encontrada num resto de cigarro na cena do crime, mas este material pode ter sido plantado na cena ou ter sido deixado lá muito tempo antes da ocorrência do crime. No caso de um suposto estupro, o DNA pode ajudar a comprovar que houve relação sexual, mas não ajuda a resolver disputas sobre a questão do possível consentimento para a relação. Além disso, as amostras de DNA obtidas em cenas de crimes com frequência são degradadas ou misturadas: isso significa que pode ser difícil obter um perfil completo de DNA com base nas provas disponíveis.

1. Ver em http://www.dnaresource.com/sponsor.html 2. Ver em http://www.dna4africa.org/ 3. Ver em http://dnaproject.co.za/sponsors
4. Ver em http://dnasaves.org/ 5. Ver em http://www.ncvc.org/ncvc/main.aspx?dbID=DB_DNAResourceCenter240 6. "Brazil's innovative war on crime." *US Daily Review*. 2 de junho de 2012. Ver em http://usdailyreview.com/brazils-innovative-war-on-crime

A análise de DNA pode ser usada nas investigações criminais sem que se estabeleça uma base de dados de DNA – porque o DNA de suspeitos conhecidos acusados de serem autores do crime pode ser comparado diretamente com os perfis de DNA obtidos na cena do crime. Uma correspondência de perfil com base no DNA – ou a falta de correspondência – pode ter um papel importante na condenação da pessoa que cometeu o crime, ou pode exonerar de culpa uma pessoa erroneamente acusada. O papel que a análise do DNA desempenha em um caso deve sempre depender do contexto no qual o DNA foi encontrado e das várias explicações alternativas sobre como a amostra pode ter parado no local. A falha em considerar estas questões pode levar a erros judiciais (o caso Amanda Knox é um exemplo recente[7]).

Bases de dados de DNA podem conter perfis de DNA de indivíduos específicos e aqueles obtidos em cenas de crimes.

A coleta de perfis de DNA em cenas de crimes e seu armazenamento em bases de dados pode ajudar a polícia de duas maneiras importantes: (i) ao associar duas ou mais cenas de crimes se o mesmo perfil foi deixado nestes locais, sugerindo que uma mesma pessoa pode ter estado em todas as cenas; (ii) ao permitir que uma investigação antiga seja reaberta caso uma pessoa tenha seu DNA coletado tempos depois e, quando comparado aos perfis armazenados na base de dados de DNA obtido em cenas de crimes, leve a uma correspondência de perfis.

Já a retenção de perfis de DNA de *indivíduos* numa base de dados trata o indivíduo como suspeito de um possível crime futuro. Isso só será útil se a pessoa realmente cometer um crime para o qual a prova de DNA for relevante, e se este indivíduo não puder ser identificado como suspeito pelo crime por outros meios. Em alguns casos, um '*cold hit*'[8] numa base de dados de DNA pode ser uma maneira efetiva de levar a polícia à pessoa perpetradora do crime. Entretanto, a identificação de suspeitos por meio de '*cold hits*' na base de dados transfere o ônus da prova, uma vez que o suspeito provavelmente terá que oferecer outras provas de sua inocência: isso aumenta o risco de erros judiciais por conta de falsas correspondências de perfis de DNA (o que pode acontecer devido a erros de laboratório ou por outras circunstâncias); ou mesmo porque pode haver uma outra explicação para a presença do DNA do indivíduo na cena do crime ou próximo à cena, sendo a pessoa inocente.

Interesses comerciais frequentemente fazem lobby para que se incluam mais perfis de DNA de *indivíduos* nas bases de dados de DNA, porque na verdade o número de provas recolhidas em cenas de crimes é relativamente pequena, em comparação com o número de indivíduos em uma determinada população. Portanto, o mercado de testes de DNA será muito maior se os países adotarem legislações que dão à polícia amplos poderes para coletar o DNA das pessoas.

7. Jabr, F (2011). "DNA doubts help clear Amanda Knox of murder." *New Scientist*. 3 de outubro de 2011. Ver em http://www.newscientist.com/article/dn21002-dna--doubts-help-clear-amanda-knox-of-murder.html 8. Um '*cold hit*' refere-se a uma situação em que uma ou mais conexões são feitas entre uma vítima de crime, um(a) prepetrador (a), e/ou uma cena de crime, sem que quaisquer pistas na investigação levem a esta conexão. Fonte: *World of Forensic Science*. Gale Cengage, 2006.

Entretanto, o impulso para expandir este mercado tende a ir de encontro às evidências que mostram que a retenção de perfis de DNA de alguns indivíduos é útil, mas que os benefícios diminuem à medida que as bases de dados de DNA aumentam – e que analisar mais amostras obtidas em cenas de crimes é muito mais vantajoso em termos de custos.

O lobby pela criação ou expansão de bases de dados de DNA frequentemente envolve muitas alegações falaciosas sobre o papel do DNA na solução de crimes. Por exemplo, lobistas da Gordon Thomas Honeywell (GTH) fizeram uma apresentação em Brasília em 2010 na qual afirmavam que 3.000 estupros cometidos por pessoas estranhas à vítima puderam ser resolvidos por ano no Reino Unido graças à amplitude da base de dados de DNA daquele país.[9] Na verdade, é possível calcular, usando estatísticas oficiais, que de aproximadamente 13.000 estupros por ano no Reino Unido[10], apenas uns poucos casos (entre 5 e 27, aproximadamente) são solucionados usando a base de dados de DNA.[11]

Fatores que limitam a eficácia das bases de dados de DNA na solução de crimes de estupro incluem:

(i) falha em coletar, encontrar ou analisar DNA da cena do crime (geralmente o sêmen do estuprador), o que requer um imediato exame da vítima após o ataque;

> Na verdade, a expansão da base de dados de DNA do Reino Unido para incluir perfis de mais de um milhão de pessoas inocentes não ajudou a solucionar mais crimes

(ii) problemas com a análise do laboratório, que nem sempre provê um perfil de DNA útil, especialmente quando há uma mistura do DNA do criminoso com o da vítima;

(iii) disputas com relação à alegação de que houve consentimento da vítima (mais do que sobre a identidade do criminoso);

(iv) o fato de que a maioria dos estupros não é cometida por estranhos (em tais casos, o DNA frequentemente oferece provas úteis que confirmam que houve intercurso sexual, mas não leva a polícia a encontrar o suspeito através de checagem na base de dados). Questões similares se aplicam a outros tipos de crime: por exemplo, a maioria dos assassinos não deixam amostras válidas de DNA na cena do crime e muitos dos que deixam são conhecidos da vítima e são identificáveis

9. Ver em http://www.dnaresource.com/documents/BRAZILBrasiliaJuly2010(2).pdf <http://www.dnaresource.com/documents/BRAZILBrasiliaJuly2010%282%29.pdf>
10. Home Office (2009). *Crime in England and Wales 2008/09*. Ver em http://webarchive.nationalarchives.gov.uk/20110220105210/http://rds.homeoffice.gov.uk/rds/crimeew0809.html 11. Em 2008/2009 houve 3.411 ocorrências (crimes que vão ao tribunal) de estupro: somente 184 envolveram uma coincidência de DNA (incluindo estupros por desconhecidos e por suspeitos conhecidos). Entre 5% e 25% dos estupros foram cometidos por estranhos, o que significa que nove a 46 estupros por estranhos foram detectados utilizando DNA. Com base no número de ocorrências que levaram a condenações em 2008/2009 (59%), isso significaria cinco a 27 processos bem sucedidos com base em coincidência de DNA.

por outros meios – o DNA neste caso oferece provas que serão úteis no tribunal, mas a base de dados de DNA não desempenha um papel relevante na identificação do suspeito. Com frequência o DNA da vítima (por exemplo, seu sangue nas roupas do criminoso) é um elemento importante na investigação, mas para este tipo de prova a informação sobre o DNA do criminoso é irrelevante.

Os lobistas geralmente ressaltam que a grande base de dados de DNA do Reino Unido (que contém registros de aproximadamente seis milhões de pessoas, ou 9% da população do país) é um sucesso. Entretanto, eles na maioria das vezes citam o número de correspondência de perfis de DNA que estão na base de dados com os de cenas de crimes, e não o número de crimes resolvidos por conta disso. Devido ao fato de que qualquer pessoa que é presa na Inglaterra e no País de Gales ter rotineiramente seu DNA adicionado à base de dados, muitas dessas correspondências dizem respeito a vítimas ou passantes, ou a suspeitos que já haviam sido identificados sem o uso do DNA. A despeito da dimensão da base de dados do Reino Unido, a maioria dos crimes solucionados pelo uso de DNA utilizam amostras de pessoas já reconhecidas como suspeitas, ou utilizam correspondências entre perfis de indivíduos cujo DNA foi recém coletado e os perfis obtidos a partir de amostras de DNA coletadas em cenas de crimes. Os perfis de indivíduos que estão armazenados têm um papel relativamente insignificante na solução de crimes, e na maioria das vezes ajudam a identificar criminosos reincidentes em casos de roubos e furtos. Na verdade, a expansão da base de dados de DNA do Reino Unido para incluir perfis de mais de um milhão de pessoas inocentes não ajudou a solucionar mais crimes: o número de crimes envolvendo uma correspondência de DNA que chegam aos tribunais permaneceu quase o mesmo por dez anos, a despeito do fato de a base de dados ter praticamente triplicado de tamanho.[12] Por conta de a expansão da base de dados de DNA ter sido mal sucedida, por ter gerado a oposição pública e levado a uma decisão contra o governo do Reino Unido na Corte Europeia de Direitos Humanos[13], mais de um milhão de perfis de pessoas inocentes estão sendo retirados neste momento da base de dados de DNA.[14]

Por outro lado, a coleta de mais amostras de DNA de cenas de crimes ajudou a resolver mais crimes tanto no Reino Unido quanto nos EUA. Priorizar a análise de DNA encontrado na cena do crime é muito mais vantajoso em termos de custos do que armazenar perfis de DNA de um número enorme de pessoas.[15]

12. GeneWatch UK. *National DNA Database: Submission to the Home Affairs Committee*. Janeiro de 2010. Ver em http://www.genewatch.org/uploads/f03c6d66a-9b3545357738483c1c3d49e4/GWsub_Jan10.doc 13. European Court of Human Rights. Grand Chamber. *Case of S. and Marper v. the UK*. Dezembro de 2008. Ver em http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051 14. Home Office (2012). *Sweeping reforms to restore British liberties*. 01 de maio de 2012. Ver em http://www.homeoffice.gov.uk/media-centre/news/protection-of-freedoms 15. Goulka J, Matthies C, Disley E, Steinberg P (2010). *Toward a Comparison of DNA Profiling and Databases in the United States and England*. RAND Center on Quality Policing. Technical Report. Ver em http://www.rand.org/pubs/technical_reports/TR918.html

:: PROBLEMAS COM A NOVA LEI BRASILEIRA

A nova lei brasileira no. 12.654 inclui algumas salvaguardas que são bem-vindas; entretanto, a lei cala quanto a um número de aspectos importantes que precisam ser abordados antes que a lei venha a ser aplicada. Estes erros de omissão parecem ter ocorrido por causa de uma visão exagerada sobre os possíveis benefícios da base de dados de DNA para a solução de crimes, bem como devido à falha em avaliar os problemas que podem ser causados por erros ou mau uso dos dados.

Muitas questões precisam ser tratadas se o sistema proposto realmente destinar-se a prover proteção adequada à privacidade e aos direitos humanos e a prevenir erros judiciais.

As áreas importantes incluem:

- regulação do processo de coleta, análise e destruição de amostras, incluindo-se que seja assegurada a qualidade dos laboratórios;
- regulação do armazenamento de perfis de DNA e outras informações pessoais associadas, o que deve incluir um processo de remoção de registros que já não sejam necessários, e um sistema transparente de governança da base de dados;
- uma avaliação das potenciais falhas na correspondência de perfis e identificação errônea de suspeitos, e medidas para prevenir equívocos da justiça, o que deve incluir a adoção de um sistema de criação de perfis de DNA com suficiente poder discriminatório e requerimentos para a oferta de provas que corroborem a suspeita, além do DNA.

As prioridades devem incluir medidas para assegurar a destruição de amostras biológicas após os perfis de DNA usados para fins de identificação terem sido extraídos; e um processo automatizado para garantir a exclusão dos perfis de DNA de pessoas inocentes da base de dados, de forma confiável e com celeridade.

:: VIGILÂNCIA, DIREITOS HUMANOS E PRIVACIDADE

As bases de dados de DNA de indivíduos podem ser usadas como um sistema de vigilância, com sérios impactos sobre os direitos humanos das pessoas e em sua privacidade.

Estas bases de dados de perfis de DNA de indivíduos permite que as pessoas sejam rastreadas e que seus parentes sejam identificados mesmo que elas não sejam suspeitas de nenhum crime (possibilitando a "biovigilância" de pessoas ou grupos pela polícia, pelos governos ou por qualquer um que se infiltre no sistema), porque o DNA pode ser deixado onde quer que uma pessoa vá – por exemplo, num copo de café em uma reunião política ou num copo usado em um bar. As pessoas que têm seus perfis de DNA e outras informações que as identifiquem retidas em bases de dados de DNA são, de fato, tratadas como suspeitas por um eventual crime futuro: seu perfil de DNA poderá encaixar-se com um perfil obtido em uma cena de crime futuramente adicionado à base de dados. As pessoas também podem ser categorizadas e estigmatizadas pelo simples fato

de estarem na base de dados (mesmo que sejam totalmente inocentes). Por exemplo, registros de prisões que permaneceram associados à base de dados de DNA no Reino Unido foram usados para negar vistos para os Estados Unidos a pessoas que apenas haviam sido detidas, sem terem de fato sido condenadas à prisão. Isso significa que regras sobre que perfis de DNA (bem como quaisquer registros associados) podem ser retidos são necessárias, juntamente com salvaguardas para prevenir o mau uso dos dados.

Amostras biológicas contêm informação genética ilimitada (por exemplo, informações relacionadas à saúde) que podem ser acessadas de maneira imprópria, se as amostras são armazenadas. Perfis de DNA, mantidos em uma base de dados computadorizada, são uma série de números baseada em partes da sequência do DNA que não são portadoras de códigos, nas quais não se espera que estejam contidas informações relacionadas a saúde. Mesmo assim, perfis de DNA podem ser usados para rastrear pessoas (por exemplo, analisando-se a saliva em uma xícara usada em uma reunião), e para identificar seus parentes (através de correspondências parciais com os perfis de DNA de outras pessoas). A não-paternidade pode ser revelada ao comparar-se perfis de DNA; e indivíduos relacionados geneticamente podem ser identificados.

A nova lei brasileira requer que os perfis de DNA sejam armazenados com confidencialidade na base de dados, de acordo com regulações a serem expedidas pelo Poder Executivo. A lei também determina que os perfis de DNA obtidos de suspeitos serão excluídos da base ao final do período estabelecido em lei para a prescrição do crime do qual a pessoa é suspeita. Entretanto, não está claro se na definição destes períodos de tempo será feita diferença entre pessoas que foram condenadas, e as absolvidas ou não acusadas – bem como não está claro o período de permanência na base de dados, nestes casos. A exclusão automática de perfis de DNA de suspeitos que são posteriormente considerados inocentes, dentro de um período de tempo razoável após o fim da investigação, é essencial para proteger a privacidade das pessoas, seus direitos humanos, e para manter a presunção de inocência diante da lei.

A lei que cria a base de dados de DNA no Brasil não inclui qualquer provisão para a destruição das amostras biológicas dos indivíduos (geralmente mucosa da boca) armazenadas em laboratórios, após o perfil de DNA necessário para investigação ter sido obtido. Esta é uma salvaguarda importante que está faltando na lei - e que é necessária para que seja evitado o acesso a informação genética pessoal, que poderia ser obtida se as amostras fossem reanalisadas.

No Reino Unido, uma investigação feita em 2006 revelou que pelo menos um laboratório privado estava guardando cópias de todos os dados que eram analisados ali e que depois eram enviados para a *National DNA Database* numa mini-base de dados.[16]

16. "Police DNA database 'is spiralling out of control'." *The Observer*. 16 de julho de 2006. Ver em http://www.guardian.co.uk/uk/2006/jul/16/ukcrime.immigrationpolicy

Novos processos estão sendo implementados agora, de forma que os laboratórios recebam amostras com um código de barras único e sem qualquer informação pessoal sobre o indivíduo do qual a amostra foi retirada. Isso é necessário para proteger a privacidade das pessoas envolvidas e prevenir contra o mau uso dos dados – por exemplo, o rastreamento de indivíduos e de suas famílias, ou a identificação de doenças genéticas, ou identificação de paternidade por pessoas que possam se infiltrar no sistema do laboratório.
A nova lei na Inglaterra e no País de Gales também requer que todas as amostras biológicas sejam destruídas em até seis meses após analisadas: esta garantia também já existe em outros países, como a Alemanha.

As transferências de quaisquer dados de perfis de DNA e outros dados pessoais associados dos laboratórios e delegacias de polícia para a base de dados de DNA também devem ser seguras.

A governança de bases de dados de DNA é um elemento importante para que se mantenha a confiança da população. A regulação também deve estabelecer que um organismo independente seja responsável por monitorar e oferecer informações sobre como a base de dados é operada: por exemplo, publicando um relatório anual contendo informações sobre quantos perfis estão armazenados, quantos foram excluídos, os custos envolvidos e o número de crimes solucionados com a base de dados.

:: ERROS DA JUSTIÇA

Enquanto as provas obtidas com exame de DNA podem ajudar a condenar culpados e exonerar de culpa os inocentes, erros e equívocos com o uso do DNA podem levar a injustiças. Quanto mais as bases de dados de DNA se expandem, mais aumentam os riscos de erros nesta área.

Os perfis de DNA forenses não são únicos, porque eles baseiam-se em análise de apenas algumas partes do DNA da pessoa. Embora a probabilidade de que ocorra uma falsa correspondência entre um perfil de DNA completo de uma pessoa e um perfil de DNA completo de uma cena de crime seja muito baixa (menos de uma em um milhão), correspondências errôneas podem acontecer. O número de correspondências erradas depende do sistema de construção do perfil de DNA e do número de comparações que são feitas (o número de correspondências erradas por ano é o resultado do número de perfis armazenados, multiplicado pelo número de perfis adicionados e comparados com os armazenados naquele ano, multiplicado pela probabilidade de correspondência).
Na Europa e nos EUA, novos sistemas de construção de perfis de DNA com melhor capacidade estatística estão sendo desenvolvidos porque crescem as preocupações de que correspondências falsas ocorram ao acaso, à medida que as bases de DNA se ampliam e mais comparações entre perfis são feitas, cruzando as

fronteiras nacionais.[17,18,19,20] Entretanto, é difícil e caro implementar novos sistemas uma vez que as bases de dados já tenham sido estabelecidas: é, portanto, importante que o Brasil adote o melhor sistema de construção de perfis de DNA possível antes de criar sua base de dados.

O risco de falsas correspondências aumenta em países onde as famílias são grandes, porque parentes compartilham partes de seu DNA. Além disso, muitos perfis de DNA obtidos em cenas de crimes não são completos, porque o DNA pode ser degradado ou encontrado apenas em quantidades mínimas. Pequenas quantidades de DNA podem ser transferidas para uma cena de crime inadvertidamente (por exemplo, o DNA transmitido num aperto de mãos pode ser transferido posteriormente para uma faca). Assim provas baseadas em DNA podem ser plantadas e misturas de DNA podem ser muito difíceis de interpretar. No Reino Unido, entre maio de 2001 e abril de 2006, 27,6% do número total de relatórios de correspondências da base de dados nacional de DNA envolvia uma lista de possíveis suspeitos da qual nenhum sequer foi entregue à polícia – porque foram feitas correspondências com múltiplos registros, provavelmente devido ao fato de que várias correspondências foram feitas com perfis parciais obtidos de cenas de crimes.[21]

As falhas em prevenir contaminação em laboratórios também trazem sérias consequências. Na Inglaterra, um adolescente recentemente passou três meses na cadeia depois de ter sido acusado de um estupro cometido numa cidade que ele jamais havia visitado, por causa da contaminação em um teste de DNA no laboratório.[22] No ano passado, nos Estados Unidos, a polícia de Las Vegas admitiu que um homem inocente passou quatro anos na prisão depois de uma mistura equivocada de DNA num laboratório.[23] Outras misturas de DNA em laboratórios dos Estados Unidos acabaram mandando pessoas inocentes para a prisão, no passado.[24]

Processos de extradição também deveriam requerer outras provas que corroborem a prova oferecida pelo DNA, bem como o direito de refazer os testes das amostras. Por exemplo, o caso Peter Hamkin, no Reino Unido, envolveu um indivíduo falsamente acusado de um crime na Itália devido a uma correspondência de DNA.[25]

17. "FBI's DNA database upgrade plans come under fire." *BBC*. 17 de outubro de 2011. Ver em http://www.bbc.co.uk/news/science-environment-15311718
18. Geddes, L (2011). "DNA super-network increases risk of mix-ups." *New Scientist*. 5 de setembro de 2011. Ver em http://www.newscientist.com/article/mg21128285.500-euro-dna-treaty-risks-false-positives.html?DCMP=OTC-rss&nsref=online-news
19. van der Beek, CP (2011). "Forensic DNA Profiles Crossing Borders in Europe (Implementation of the Treaty of Prüm)." Ver em http://www.promega.com/resources/articles/profiles-in-dna/2011/forensic-dna-profiles-crossing-borders-in-europe/
20. Schneider PM (2009). "Expansion of the European Standard Set of DNA Database Loci – the Current Situation." Ver em http://www.promega.com/~/media/Files/Resources/Profiles%20In%20DNA/1201/Expansion%20of%20the%20European%20Standard%20Set.ashx <http://www.promega.com/%7E/media/Files/Resources/Profiles%20In%20DNA/1201/Expansion%20of%20the%20European%20Standard%20Set.ashx>
21. *The National DNA Database Annual Report 2005-2006*. Ver em http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/DNA-report2005-06.pdf?view=Binary
22. "DNA database in doubt after teenager spends three months behind bars for rape in city he has never even visited because gene samples were mixed up." *Daily Mail*. 18 de maio de 2012. Ver em http://www.dailymail.co.uk/news/article-2114252/Teenager-spends-months-bars-DNA-blunder-fingers-rape-city-visited.html
23. "Las Vegas police reveal DNA error put wrong man in prison." *Las Vegas Review Journal*. 7 de julho de 2011. Ver em http://www.lvrj.com/news/dna-related-error-led-to-wrongful-conviction-in-2001-case-125160484.html
24. "DNA Testing: Foolproof?" *CBSNews*. 11 de fevereiro de 2009. Ver em http://www.cbsnews.com/2100-500164_162-555723.html
25. "Cleared murder accused victim of DNA blunder." *Liverpool Daily Post*. 10 de março de 2003. Ver em http://icliverpool.icnetwork.co.uk/0100news/0100regionalnews/page.cfm?objectid=12718961&method=full&siteid=50061

É uma boa prática usar laboratórios que sejam independentes das autoridades policiais para evitar potenciais análises tendenciosas (ou a acusação de que o sejam) pelos especialistas, particularmente as análises de amostras do DNA obtido em cenas de crimes (que podem estar degradadas ou misturadas, e assim abrir espaço para múltiplas interpretações).

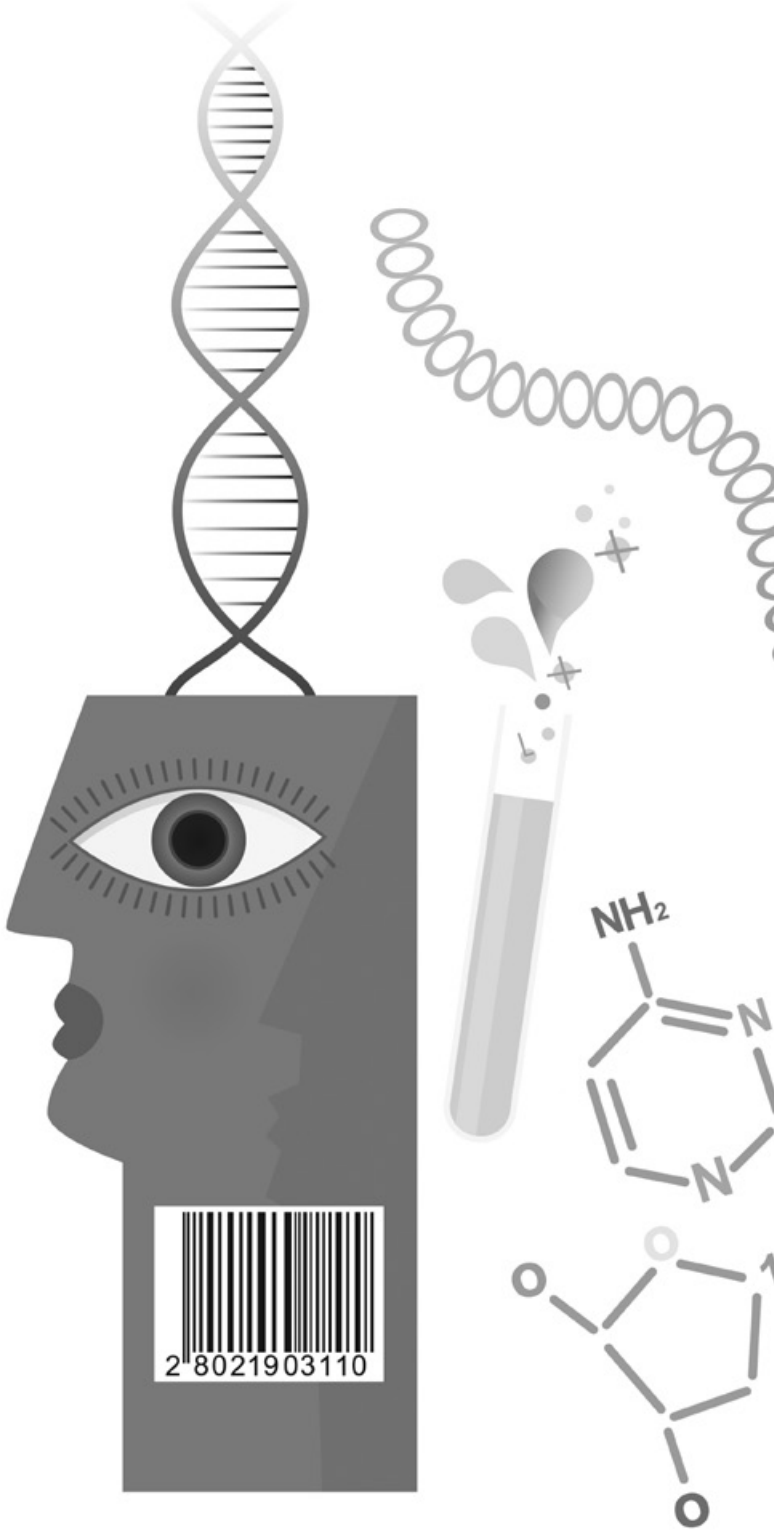
A nova lei que cria a base de dados de DNA no Brasil requer que a informação obtida de uma correspondência de DNA deva ser registrada em um relatório técnico, assinado por um especialista oficial devidamente autorizado para isso. Medidas adicionais importantes, necessárias para prevenir erros por parte da justiça incluem:

1. Um requerimento expedido por juiz para solicitar provas corroboradoras, de modo que indivíduos não possam ser condenados ou extraditados com base unicamente na prova obtida com análise de DNA;

2. Requerimentos que assegurem controle de qualidade dos laboratórios;

3. Medidas para prevenir contaminação nas cenas dos crimes e nos laboratórios, de forma que o DNA de pessoas inocentes não seja misturado com DNA obtido em cenas de crimes;

4. O direito de todos os acusados de que sejam feitos novos testes usando-se uma outra amostra de DNA antes do julgamento ou extradição;



5. Seleção de um sistema de construção de perfis de DNA com capacidade estatística suficiente para efetuar o número de comparações que espera-se que sejam feitas, levando-se em conta o risco aumentado de correspondências entre familiares;

6. Restrições do número de perfis de DNA de indivíduos e de cenas de crimes coletados e armazenados nas bases de dados e compartilhados com outros países, de forma que o sistema de construção de perfis utilizado tenha capacidade estatística suficiente para minimizar a probabilidade de falsas correspondências que possam acontecer por puro acaso;

7. Retenção cuidadosa de provas obtidas em cenas de crimes e o direito de que novos testes sejam feitos com estas provas em caso de suspeita de erro judicial.

> as salvaguardas incluídas na lei são inadequadas para prevenir o mau uso dos dados para fins de vigilância

No Reino Unido, um Regulador de Ciência Forense foi criado para investigar erros ocorridos em análises de DNA e em outros métodos de testagem, bem como para supervisionar a garantia de qualidade dos laboratórios.

:: CONCLUSÕES

A nova lei brasileira 12.654 cria a base de dados nacional de DNA , com o objetivo de solucionar crimes. Entretanto, as salvaguardas incluídas na lei são inadequadas para prevenir o mau uso dos dados para fins de vigilância, para proteger a privacidade das pessoas e outros direitos humanos, e para prevenir erros da justiça. Grandes bases de dados de DNA não ajudam a resolver mais crimes: os benefícios são menores e os custos e riscos envolvidos são maiores, conforme as bases de dados aumentam em tamanho. Lobistas do setor privado têm interesses em encorajar o Brasil a criar uma das maiores bases de dados de DNA do mundo, mas os interesses comerciais conflitam com o interesse público, porque grandes bases de DNA não são uma maneira efetiva, em termos de custos, de combater crimes. Se o Brasil vai estabelecer um precedente para a América Latina, salvaguardas melhores devem ser introduzidas antes que se crie a base de dados. A sociedade civil tem um papel importante de assegurar que estas salvaguardas sejam devidamente debatidas. ●

> **Kelli Angelini** assessora jurídica do NIC.br

SACI

o Sistema Administrativo de Conflitos de Internet implementado para domínios no ".br"

Os primeiros registros de nomes de domínio utilizando o .br foram realizados em meados de 1994. Porém, foi em 1999 que as empresas efetivamente passaram a buscar o registro de domínios compostos por nomes idênticos ou semelhantes às suas marcas, nomes empresariais ou nomes artísticos.

Isso acabou gerando uma verdadeira corrida por nomes no .br – uma vez que muitas empresas, principalmente as multinacionais, ao verificarem o que acontecia em muitos países do mundo quanto à divulgação de produtos e serviços através da Internet, manifestavam seu desejo em estender essa divulgação aqui no Brasil por meio de domínios registrados no .br e, para isso, buscavam registrar domínios compostos por nomes idênticos à sua marca ou à denominação de seus produtos e serviços.

Foi nesse momento de euforia, em que praticamente havia uma corrida para o registro de nomes, que alguns usuários de Internet, já sabendo do que ocorria em outros países, acabaram percebendo que o registro de nomes notórios no .br acabaria por transformar-se em uma atividade lucrativa com a posterior venda desses domínios aos titulares de marcas ou nomes notórios.

Seguiu-se, então, uma fase de negociação de nomes de domínio sob o .br – e quando esta restava infrutífera, o que na maioria das vezes acontecia devido ao expressivo valor requerido por aqueles "usurpadores de nomes", os litígios eram submetidos ao Poder Judiciário. Porém, devido à morosidade na tramitação de ações judiciais em nosso país, as empresas que litigavam frequentemente para obter a titularidade de nomes de domínios semelhantes às suas marcas, apoiadas por grandes escritórios de advocacia especializados em marcas e patentes, pleitearam ao Comitê Gestor da Internet no Brasil – CGI.br –, a adoção de uma medida alternativa para a solução destes conflitos.

O Comitê Gestor da Internet no Brasil resolveu então desenvolver estudos para a solução deste tipo de disputa. A primeira opção encontrada foi a de aderir ao sistema da UDRP – *Uniform Dispute Resolution Policy*[1], ou, em português, Política Uniforme para Resolução de Disputas. Porém, depois de analisar minuciosamente esta política, o CGI.br entendeu que adotá-la não seria o caminho mais adequado – mesmo levando-se em consideração o prestígio que a UDRP já havia conquistado em diversos países, devido à sua eficácia e celeridade na solução de conflitos que envolvem nomes de domínios.

Neste momento o CGI.br percebeu que as reais necessidades para a solução de conflitos de nomes de domínio no país eram:

a) dar a opção das partes escolherem a entidade que administraria esse procedimento, incluindo entidades nacionais;
b) assegurar que o procedimento fosse realizado exclusivamente em nosso idioma;
c) que fosse julgado apenas por especialistas brasileiros;
d) que abrangesse também questões envolvendo nomes empresarias e nomes artísticos;
e) e seguisse as regras já adotadas para domínios registrados no ".br".

Diante da conclusão pela não adesão à UDRP, outra opção que surgiu naquela época foi a instituição da arbitragem para esses conflitos. Entretanto, ao aprofundar-se nos estudos sobre a implementação desse método alternativo de solução de conflitos – apesar de não ter sido encontrada nenhuma proibição legal ou doutrinária para implementação da arbitragem para os conflitos referentes a domínios registrados no ".br" – o CGI.br decidiu (devido à formalidade estabelecida pela Lei Arbitral e ao seu custo) pela não implementação da via arbitral para estes conflitos naquele momento, em que a sociedade buscava uma solução alternativa ao Poder Judiciário.

Uma vez afastada a possibilidade de adesão à UDRP, bem como a implementação da arbitragem para os conflitos envolvendo nomes de domínios registrados no ".br", o CGI.br implementou, em outubro de 2010, através da Resolução CGI.br/RES/2010/003/P[2],

1.http://archive.icann.org/en/udrp.htm 2.http://cgi.br/regulamentacao/resolucao2010-003.htm – acessado em 27/12/2011

o Sistema de Administração de Conflitos de Internet, denominado "SACI-Adm".

O SACI-Adm tem por objetivo a solução de litígios entre o titular de um nome de domínio no .br e qualquer terceiro que conteste a legitimidade do registro do nome de domínio feito pelo titular - sendo que o titular do domínio adere ao SACI-Adm através do contrato firmado para registro de domínio no .br e o terceiro o faz quando da solicitação de abertura do procedimento no SACI-Adm. O escopo dos procedimentos do SACI-Adm limita-se aos pedidos de cancelamento e transferência de domínio - portanto, qualquer pretensão relativa à obtenção de indenizações não poderá ser tratada nesse âmbito.

A administração dos procedimentos decorrentes do SACI-Adm é realizada por instituições credenciadas pelo NIC.br, o que significa que o NIC.br apenas implementou o Sistema, porém jamais participa da administração dos procedimentos, tampouco interfere no julgamento do conflito.

É importante informar que até o presente momento o NIC.br credenciou três instituições. A primeira delas foi a Câmara de Comércio Brasil Canadá - CCBC-, que é uma das entidades mais reconhecidas nacional e internacionalmente, em função das atividades de seu centro de mediação e arbitragem. Desde o princípio a CCBC manifestou total apoio à implementação do SACI-Adm.

A segunda entidade credenciada foi a OMPI (Organização Mundial de Propriedade Intelectual), que é a implementadora da Política UDRP e possui vasta experiência nestes procedimentos administrativos. Esta decisão de aderir ao SACI-Adm deu-se pelo fato de o CGI.br ter decidido, por razões já mencionadas nesse texto, que as regras da UDRP não seriam as mais adequadas para os conflitos no .br, apesar de haver uma grande semelhança entre os sistemas UDRP e SACI-Adm.

A terceira entidade, credenciada em agosto de 2012, foi a ABPI, que através de seu Centro de Solução de Disputas, Mediação e Arbitragem em Propriedade Intelectual (CSD-PI), passou também a administrar os procedimentos do Saci-Adm.

A opção por uma dessas três entidades para administrar o procedimento do SACI-Adm é feita pelo reclamante (aquele que contesta o registro do domínio), ao requerer a abertura do procedimento. Um dos fatores que podem ser decisivos na escolha da instituição credenciada (além, é claro, da idoneidade da instituição e da capacidade de seus especialistas) é o valor das custas do procedimento, que são divulgados pelas instituições e estipulados em valor fixo independente do status das partes, da importância do nome do domínio ou do tempo dispendido para a solução do conflito.

É importante observar que as custas do procedimento do SACI-Adm são pagas por quem solicita a abertura do procedimento (o Reclamante), salvo se o titular do domínio (o Reclamado) optar por um painel composto por três especialistas, nos casos em que o Reclamante decide pelo julgamento

do procedimento feito por apenas um especialista. Nesse caso, o Reclamante arcará com os honorários de um único especialista e o Titular arcará com honorários dos outros dois especialistas.

Com relação à abertura do procedimento, cabe ressaltar que, ao fazer essa solicitação, o reclamante deverá expor as razões pelas quais o nome de domínio contestado foi registrado, se está sendo usado de má-fé (de modo a causar prejuízos a ele, reclamante) e ainda comprovar que o nome de domínio é idêntico ou similar o suficiente para criar confusão com uma marca de titularidade do Reclamante, ou com um título de estabelecimento, nome empresarial, nome civil, nome de família ou patronímico, pseudônimo ou apelido notoriamente conhecido, nome artístico singular ou coletivo.

As circunstâncias que constituem indícios de má-fé na utilização do nome de domínio objeto do procedimento do SACI-Adm (as quais o reclamante deverá comprovar), estão dispostas no parágrafo único do Art. 3º do Regulamento do SACI-Adm[3]:

"**a)** ter o Titular registrado o nome de domínio com o objetivo de vendê-lo, alugá-lo ou transferi-lo para o Reclamante ou para terceiros; ou

b) ter o Titular registrado o nome de domínio para impedir que o Reclamante o utilize como um nome do domínio correspondente; ou

c) ter o Titular registrado o nome de domínio com o objetivo de prejudicar a atividade comercial do Reclamante; ou

d) ao usar o nome de domínio, o Titular intencionalmente tente atrair, com objetivo de lucro, usuários da Internet para o seu sítio Web ou para qualquer outro endereço eletrônico, criando uma situação de provável confusão com o sinal distintivo do Reclamante."

Uma vez atendidos estes requisitos iniciais pelo reclamante, o procedimento é instaurado, seguindo sob a administração da instituição escolhida, a qual estabelece as regras para escolha do (s/as) especialistas que irá (ão) julgar o conflito. Os conflitos submetidos ao SACI-Adm serão decididos por especialistas escolhidos/as exclusivamente entre profissionais integrantes do corpo de especialistas da instituição credenciada que administra o procedimento.

Um fator importante a destacar — que foi uma das razões que levaram o CGI.br a decidir-se por um sistema próprio e não pela adoção à UDRP —, é a previsão no Regulamento do SACI-Adm de que o NIC.br não permitirá a transferência do nome de domínio em conflito desde o início do procedimento no SACI-Adm até o seu término. Isso significa que, iniciado o procedimento, não é possível alterar o polo passivo e ativo da relação, a menos que as partes concordem neste sentido. Nos casos de cancelamento do domínio durante o procedimento do SACI-Adm, o NIC.br não permitirá que esse domínio seja colocado disponível para novo registro, mantendo-o reservado até que seja encerrado o procedimento correspondente.

3.http://registro.br/dominio/SACI-Adm.html – acessado em 17/12/201 4. O registro de domínios no ".br" é realizado através do site www.registro.br e nesse site é possível consultar os dados do titular de um nome de domínio e o endereço eletrônico indicado para o cadastro.

> o procedimento do SACI-Adm prevê a possibilidade de apresentação de defesa pelo titular do domínio, e este o fará se assim desejar.

O regulamento do SACI-Adm assegura ao Reclamante e ao titular do domínio a opção por ter o procedimento do SACI-Adm julgado por um ou três especialistas. As partes, na primeira oportunidade de manifestação, deverão informar sua opção por um procedimento singular ou por um procedimento acompanhado por um painel de especialistas. Os Regulamentos Suplementares das Instituições Credenciadas prevêem a forma de nomeação dos especialistas, sendo que nas instituições até o momento credenciadas (OMPI, CCBC e ABPI) a indicação é feita pela própria instituição.

É importante ressaltar que a maioria dos casos de impedimento e suspensão de juízes e árbitros elencados em nossa legislação processual e utilizados nos processos arbitrais, também foram assegurados nos procedimentos do SACI-Adm. As instituições credenciadas prevêem a obrigatoriedade de o/a especialista firmar declaração e compromisso de independência e, ainda, a possibilidade de qualquer das partes arguir o impedimento ou suspeição da pessoa especialista.

Assegurando o princípio da ampla defesa e do contraditório, o procedimento do SACI-Adm prevê a possibilidade de apresentação de defesa pelo titular do domínio, e este o fará se assim desejar. É necessário destacar que a falta de apresentação de defesa não acarreta nenhum prejuízo ao procedimento, uma vez que este prosseguirá à revelia da parte que manteve-se inerte.

> o conflito decidido pelo SACI-Adm pode ser levado à apreciação do Poder Judiciário ou do Juízo Arbitral.

Porém, isso em hipótese alguma garante a procedência dos pedidos do Reclamante, eis que o/a especialista ou o painel de especialistas deverá decidir o conflito baseado nos fatos e nas provas produzidas durante procedimento do SACI-Adm. A decisão jamais poderá ser fundamentada na falta de apresentação de defesa. É importante destacar que, se o titular do domínio deixar de apresentar defesa, caberá à instituição credenciada que administra o procedimento comunicar o fato ao NIC.br, para que este congele[5] (suspenda) o nome de domínio objeto do conflito. O objetivo desta medida é alertar o titular do domínio sobre a existência de alguma pendência (assim como ocorre quando há falta de pagamento), uma vez que suspendendo-se a utilização do domínio é provável que o seu titular se manifeste para averiguar os motivos da suspensão. Por cautela, antes mesmo do congelamento do domínio, o NIC.br encaminha um comunicado ao titular do domínio informando que sua não manifestação sobre a existência do procedimento ocasionará o congelamento.

O Regulamento do SACI-Adm estipula o prazo de noventa dias para término do procedimento, que pode ser prorrogado, a critério da Instituição Credenciada, por até doze meses[6]. A decisão do procedimento, conforme o regulamento do SACI-Adm, conterá o relatório, os fundamentos da decisão, o dispositivo, data e local em que a decisão é proferida e assinada pelo/a especialista. Esta decisão se dará por maioria de votos, caso o procedimento tenha sido conduzido por um painel de especialistas. A decisão final poderá determinar que o domínio permaneça em nome do reclamado, e isso se dará quando os/as especialistas entenderem que o domínio foi registrado e utilizado sem qualquer violação a direitos daquele que requereu a abertura do procedimento do SACI-Adm. Ou determinará a transferência do domínio ao reclamante ou o seu cancelamento[7].

5. O termo congelamento é utilizado para indicar a suspensão de um nome de domínio, o que pode ocorrer, por falta de pagamento da manutenção anual, por ordem judicial ou nesse caso de falta de apresentação de defesa no SACI-Adm. O congelamento de um nome de domínio acarreta a suspensão provisória da utilização do domínio, ou seja, a suspensão abrange todo o conteúdo divulgado no domínio, os endereços de e-mails correspondentes, as páginas e os subdomínios ligados a ele. 6. Os procedimentos do SACI-Adm já instaurados tiveram sua conclusão no prazo médio de 100 dias, contados da data de seu início até a execução da decisão pelo NIC.br. Fonte: http://registro.br/dominio/decisoes-SACI-Adm.html - acessada em 15-12-2011 7. O artigo 1º § 1º do Regulamento do SACI-Adm limita o escopo do procedimento ao requerimento de manutenção do domínio, transferência ou cancelamento. Fonte: http://registro.br/dominio/SACI-Adm.html - acessado em 18-12- 2011

Nos casos em que a decisão proferida determinar que o domínio seja transferido ou cancelado, o cumprimento dessa decisão poderá se dar espontaneamente pelo reclamado. Se isso não acontecer, o regulamento do SACI-Adm prevê que, uma vez sendo fixada a transferência ou o cancelamento do domínio, o NIC.br aguardará o decurso do prazo de quinze dias úteis para que, nesse período, qualquer das partes ingresse com ação judicial ou processo arbitral, se assim desejar – ou seja, o conflito decidido pelo SACI-Adm pode ser levado à apreciação do Poder Judiciário ou do Juízo Arbitral. Porém, se as partes mantiverem-se inertes nesse prazo, o NIC.br implementará a decisão prolatada.

É importante destacar aqui duas particularidades dessa etapa do processo. A primeira é a de que a previsão do prazo de quinze dias para comprovação de ingresso de ação judicial ou processo arbitral não exclui a apreciação posterior do conflito pelo Poder Judiciário, uma vez que o prazo é fixado apenas para cumprimento da decisão pelo NIC.br, - do contrário, estaríamos diante de um caso nítido de afronta ao art. 5º, XXXV, da Constituição Federal.

A outra particularidade refere-se ao peso que terá a decisão prolatada pelos/as especialistas no procedimento do SACI-Adm, se o conflito for levado ao Poder Judiciário. É fato que o juiz deve valer-se do princípio do livre convencimento motivado da causa, embasando sua decisão não somente no formalismo da lei, mas também nas provas existentes nos autos e em sua livre convicção pessoal. Assim, a decisão prolatada pelo especialista, sem sombra de dúvidas, servirá para, no mínimo, aclarar os fatos, podendo ser seguida – ou não – pelo magistrado.

Além dos casos de encerramento do procedimento do SACI-Adm pelo cumprimento da decisão do (s/as) especialista (s), ou pelo resultado do ingresso de ação judicial ou processo arbitral, o procedimento também poderá ter o seu término se as partes assim concordarem, amigavelmente. Postas em prática essas regras, alguns conflitos já foram solucionados através do Regulamento do SACI-Adm, de forma bem-sucedida. As decisões dos procedimentos do SACI-Adm já julgados estão disponíveis no site: http://registro.br/dominio/decisoes-SACI-Adm.html ●

alguns conflitos já foram solucionados através do Regulamento do SACI-Adm, de forma bem-sucedida.

Retomando de onde o IGF começou:

nosso papel no futuro da governança da Internet

Jeremy Malcolm Coordenador de Projetos em Propriedade Intelectual e Comunicação da Consumers International

A governança da Internet chega a um ponto de crise. Políticas públicas relativas à Internet estão sendo construídas por alguns governos a portas fechadas, estimulando protestos globais – nas ruas e online - sobre acordos tais como o Acordo de Parceria Transpacífica (TPPA)[1] e o Acordo de Comércio Antifalsificação (ACTA)[2]. Outros governos, excluídos desses fóruns, recorrem à União Internacional de Telecomunicação (UIT)[3], ou ameaçam criar seus próprios guetos na Internet[4] governados em um processo mais fechado e liderado por governos. Estados empregam softwares nocivos (*malwares*) para desfechar ciberguerras[5], enquanto o uso desses mesmos *malwares* por criminosos é tomado como justificativa para novas incursões sobre as liberdades pessoais[6]. Governos também estão propondo novas leis e regulamentos, tais como SOPA (Stop Online Piracy Act) e PIPA (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act)[7] nos EUA, e a legislação de responsabilização de intermediários na Índia (Internet Intermediary Guidelines)[8], que parecem contradizer suas próprias declarações públicas sobre liberdades na Internet - e que poderiam prejudicar seriamente os fluxos globais de informação.

As corporações também têm tomado decisões de caráter político sem qualquer prestação de contas ou supervisão pública - como o bloqueio financeiro contra o Wikileaks[9] e os acordos entre provedores de Internet e representantes de proprietários de conteúdos para bloqueios de acesso dos usuários a conteúdos ou à própria Internet a partir de um número arbitrário de avisos prévios (*three strikes*[10] ou *five strikes*[11]). Isto não significa que boas decisões não sejam tomadas - por exemplo, recentemente tem havido uma profusão de relativamente boas declarações de princípios da Internet por parte de vários grupos de interesse[12]; empresas tais como Google e Twitter têm adotado algumas boas práticas internas para reagir a governos e a indústrias por conta de seus ataques sobre a privacidade do usuário e a liberdade de expressão[13]. Mas essas declarações e políticas individuais não encontram respaldo em um marco de política pública comum que poderia dar coerência através dos diferentes setores e áreas de atividade, bem como oferecer um padrão para avaliação e prestação de contas.

1. Ver http://tppwatch.org 2. Ver http://www.guardian.co.uk/technology/2012/jul/04/acta-european-parliament-votes-against?newsfeed=true
3. Ver http://www.theregister.co.uk/2012/06/22/itu_plans_internet_regulation 4. Ver http://tools.ietf.org/html/draft-diao-aip-dns-00
5. Ver http://arstechnica.com/security/2012/06/flame-malware-created-by-us-and-israel 6.Ver http://www.bbc.co.uk/news/uk-politics-17576745
7. Ver http://www.pcworld.com/article/248298/sopa_and_pipa_just_the_facts.html 8.Ver http://cis-india.org/internet-governance/chilling-effects-on-free--expression-on-internet 9. Ver http://wikileaks.org/Banking-Blockade.html 10.Ver http://www.bbc.com/news/technology-14294517 11. Ver http://www.techdirt.com/articles/20110707/10173014998/major-us-isps-agree-to-five-strikes-plan-rather-than-three.shtml 12.Ver http://igcaucus.org/links
13. Google Transparency Report: http://www.google.com/transparencyreport. Twitter Transparency Report: https://support.twitter.com/articles/20170002#

A natureza transnacional (transfronteiras) da Internet requer a habilidade de desenvolver políticas globais consistentes sobre temas que têm impacto sobre direitos e liberdades online, e a democracia requer que isso seja feito de um modo que inclua indivíduos e os grupos de interesse transnacionais afetados por essas políticas. Já que nem a aplicação dessas políticas nem os grupos de interesse afetados por elas estão claramente delimitados por fronteiras nacionais, o arbítrio dessas políticas não pode ser deixado apenas aos governos. Do mesmo modo, ao evitar a imposição de uma solução intergovernamental imposta de cima para baixo (mesmo que existisse uma, o que não é o caso), não se pode cair na armadilha de aceitar o *status quo* - em que governos e corporações desenvolvem suas próprias políticas de modo isolado e descoordenado, sem referência a padrões comuns de transparência, participação ou normas online baseadas nos direitos humanos.

Enquanto o problema de incoerência regulatória acima descrito é amplamente reconhecido, há pouca clareza sobre as possíveis soluções. De fato há pouco mais que uma frase de efeito, "cooperação aprimorada" (*enhanced cooperation*), surgida na Cúpula Mundial sobre a Sociedade da Informação (CMSI/WSIS) em 2005 para caracterizar o que deveria ser feito para preencher o vazio que o Grupo de Trabalho sobre Governança da Internet (GTGI/WGIG) descreveu como "um vácuo no contexto das estruturas existentes, já que não há um fórum pluralista global para tratar dos temas de política pública relacionados à Internet."[14] Essa frase de efeito tem significados distintos para pessoas distintas, como demonstrado em uma consulta sobre o assunto em maio de 2012[15]- variando basicamente de sugestões de maiores esforços de cooperação entre fóruns existentes e grupos de interesse até a criação de um novo comitê da ONU sobre políticas relacionadas à Internet.

Esta última opção despertou temores compreensíveis (e provavelmente insuperáveis), especialmente no setor privado, na comunidade técnica e nos governos da OCDE[16], mas também em muitos usuários comuns da Internet. Eles temem em primeiro lugar a absorção por governos das funções de governança da Internet já existentes exercidas por organismos como a Corporação para Nomes e Números Designados (ICANN)[17] e a Força-Tarefa de Engenharia da Internet (IETF)[18], que atualmente operam através de processos liderados pela comunidade técnica e o setor privado, com uma leve supervisão (no caso da ICANN) do governo dos EUA[19]. Eles também temem que fora dessas áreas técnicas a regulação das políticas da Internet (especialmente por parte de governos repressivos) prejudicaria ou desafiaria a natureza inovadora, flexível e adaptável da rede.

14. Ver http://www.wgig.org/docs/WGIGREPORT.doc 15. Ver http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=61 16. Ver http://www.oecd.org
17. Ver http://www.icann.org 18.Ver http://www.ietf.org 19.Ver http://news.cnet.com/8301-1009_3-57444629-83/u.n-takeover-of-the-internet-must-be-stopped-u.s-warns

Se esses temores têm razão de ser, há por outro lado uma crescente aceitação que a primeira opção – manter o *status quo* – não será melhor no longo prazo. Juntando-se a acadêmicos, entidades civis e ativistas no campo do desenvolvimento que vêm dizendo a mesma coisa há vários anos, os grupos de interesse da indústria começam também a reconhecer que há necessidade de um novo tipo de organismo pluralista para políticas públicas da Internet que possa atuar como contraparte e complementar as funções de corpos técnicos como a ICANN e a IETF. O analista Paul Budde, por exemplo, escreveu em julho de 2012 na revista online CircleID que essa "organização da comunidade Internet" poderia, se "apropriadamente financiada e constituída pelas pessoas internacionais apropriadas para gerenciar o que é necessário para supervisionar a governança da Internet," ser "uma excelente parceira no conjunto da comunidade de organizações internacionais."[20]

Portanto, essa é a chave. É necessário um novo organismo, mas nenhum ainda foi proposto. Este organismo não deveria ser baseado na ONU, não deveria afetar os papéis da ICANN e IETF, e não deveria prejudicar os fundamentos da Internet aberta, orgânica e desenvolvida pelos seus usuários. Seguindo os critérios de processos da CMSI, sua operação deveria ser transparente, participativa e inclusiva. Deveria ser capaz de desenvolver (mas não de impor, já que este não é o modo da Internet) propostas de normas e princípios para guiar os formadores de políticas de modo congruente com o consenso básico de todos os grupos de interesse participantes, em áreas onde um consenso é possível. Deveria também ser capaz de avaliar (de novo, sem imposições) a aderência de outros processos políticos a essas normas e princípios - por exemplo, oferecendo um padrão pelo qual julgar as negociações do ACTA ou TPPA.

Além de desenvolver e avaliar aderência a essas normas gerais de alto nível, esse organismo poderia também formar grupos de trabalho para trabalhar em assuntos específicos, tais como as partes do ACTA e do TPPA que relacionam-se à Internet, como uma alternativa às negociações *ad hoc* somente de governos sobre estes assuntos tal como ocorre atualmente. Outro exemplo de caso poderia ser o desenvolvimento de princípios de privacidade online para orientar entidades de padronização como a IETF e o W3C no desenvolvimento de especificações técnicas. Atualmente estas entidades (e também a ICANN com relação a nomes de domínio e endereços IP) tentam conduzir suas próprias discussões de políticas, mas em razão da participação limitada por parte dos usuários não técnicos, seu êxito é definitivamente relativo[21]. Além de grupos de trabalho temáticos, a nova organização poderia formar grupos de trabalho regionais para tratar de assuntos cujo tratamento mais amplo não é prático ou relevante.

20. Ver http://www.circleid.com/posts/20120620_is_the_future_of_the_internet_at_risk 21. Ver http://www.w3.org/2011/tracking-protection

O que a nova organização *não* faria? Naturalmente, não assumiria as funções de administração de nomes e números da ICANN. Sequer exerceria supervisão sobre essas funções - como organismo voluntário, não teria mandato para isso. Ela poderia recomendar processos pelos quais a supervisão política das funções da ICANN poderia ser internacionalizada no futuro (e talvez até sugerir um papel para si mesma nessa transição), porque este é um assunto de política pública de considerável importância política para muitos grupos de interesse, que não pode ser conduzido com êxito no interior da própria ICANN. Mas a entidade não teria poder de impor qualquer mudança nas funções da ICANN, ou qualquer outro poder decisório. Suas recomendações seriam puramente de aconselhamento, como as Solicitações de Comentários (*Requests for Comments*, RFC) da IETF.

A questão óbvia agora é: deveria o Fórum de Governança da Internet (IGF) fazer tudo isso? Sim, sem dúvida deveria. A Agenda de Túnis aprovada na CMSI[22] especifica claramente que o papel do IGF deveria incluir a formulação de recomendações sobre assuntos emergentes bem como promover e avaliar de modo permanente a realização dos princípios da CMSI em processos de governança da Internet. Estes são exatamente os dois papéis de fixação de normas e avaliação que atribuo acima à nova organização (claro está que o IGF também faz outras coisas, e algumas delas bem, mas esses dois elementos de seu mandato foram completamente postos de lado).

Mesmo que o IGF devesse fazer isso, não podemos esperar que o faça. Por que não? Porque o IGF é um ente das Nações Unidas e portanto, mesmo com seu mandato original inovador tanto na forma como nas funções, na prática ele foi rapidamente atrelado às limitações de agir por consenso (essencialmente pleno), no estilo da ONU. Se qualquer dos grupos de interesse apresenta objeções a que o IGF faça recomendações de políticas - no que alguns deles certamente sempre insistem - este simplesmente não as fará. Para a "cooperação aprimorada" funcionar, deve haver um mecanismo voluntário ao qual os grupos de interesse que queiram colaborar no desenvolvimento de políticas possam aderir, e os que não queiram simplesmente ignorem. O IGF tal como se desenvolveu não é esse mecanismo.

Isso não significa que o IGF jamais poderia ter funcionado - poderia, se tivesse sido projetado adequadamente para tomar decisões por consenso básico (*rough consensus*), desenvolvido através de um processo deliberativo democrático usando discussões online moderadas e interações em pequenos grupos. Mas isso nunca foi tentado, e o IGF acabou engessando-se em torno das linhas

22. Ver http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

mais tradicionais determinadas no seu início por sua equipe executiva (Nitin Desai e Markus Kummer) e pelos que tinham influência decisiva sobre ela. Que uma reforma significativa não é mais possível é demonstrado pelo fato que mesmo uma recomendação de melhora mínima não foi proposta pelo Grupo Assessor Pluralista (o *Multi-Stakeholder Advisory Group*, ou MAG), mas sim por um grupo de trabalho da Comissão sobre Ciência e Tecnologia para o Desenvolvimento (CSTD) da ONU[23]. Mesmo sendo um organismo intergovernamental operando na base do consenso pleno, a CSTD não conseguiu sequer recomendar a formação de grupos de trabalho para o IGF, e ainda menos as reformas que o mesmo precisaria para levar adiante a "cooperação aprimorada".

Com tudo isso, a nova organização teria que trabalhar em estreita colaboração com o IGF. Os IGFs global, regionais e nacionais terão que ter uma capacidade relevante (de fato provavelmente a mais relevante) de definição da agenda e de seu papel de formação de capacidades para a comunidade que desenvolverá recomendações de políticas através da nova organização. O IGF, neste papel, com sua estrutura completamente aberta e sem formalismos, poderia de fato tornar-se mais importante do que nunca. Mas em razão desses mesmos aspectos, o IGF em sua forma atual não terá condições de fazer recomendações de políticas

o IGF em sua forma atual não terá condições de fazer recomendações políticas

ou avaliar a aderência de outros organismos de governança da Internet a normas de procedimento.

Todavia, se o IGF não está qualificado para ser essa organização, isso não necessariamente significa que precisamos de um novo organismo - certamente deve haver alguma outra entidade que poderia desenvolver e promulgar normas globais de políticas para a Internet? Se a resposta é sim, onde está essa entidade? Não é a ICANN - temas de políticas públicas fora do escopo técnico das funções de administração de nomes e números estão fora do seu mandato. A Assembléia de Governança da Internet da Sociedade Civil (o Civil Society Internet Governance Caucus, IGC)[24]

23. Ver http://www.unctad.info/en/CstdWG 24. Ver http://www.igcaucus.org

não está à altura do desafio - além de não ser pluralista, não tem uma estrutura suficientemente formalizada. A Internet Society (ISOC)[25] e a UIT[26] não são organismos pluralistas e negam a necessidade de qualquer processo de "cooperação aprimorada," insistindo que já estão fazendo isso. A Global Network Initiative[27] exclui governos, e de qualquer modo tem seu próprio papel independente e mais restritivo (que deve continuar, informado pela nova organização). A OCDE tem uma estrutura consultiva razoável, mas é um clube dos países ricos que as nações em desenvolvimento não aceitariam. O mesmo ocorre com o Conselho da Europa[28] (mesmo que sua Convenção de Cibercrime tenha sido aberta a Estados não membros).

Conclui-se que temos que começar de novo. Ao fazer isso, há quatro características essenciais em torno das quais a nova organização teria que ser concebida.

Em primeiro lugar, ela precisa ser voluntária, tanto em sua participação quanto na força que suas recomendações terão. Esta é uma estrutura familiar para os que acompanham a governança da Internet, já que a IETF opera dessa maneira. De fato, a IETF foi o modelo que eu tinha em mente quando iniciei a pesquisa de doutorado que posteriormente tornou-se meu livro[29]. Propostas similares para uma entidade de políticas baseadas na IETF - tal como a Força Tarefa Societária (ISTF)[30] proposta pela ISOC - datam de mais tempo, e outras continuam a ser feitas hoje. No entanto, a estrutura que eu acabei propondo para uma rede pluralista de governança da Internet difere da IETF em vários aspectos importantes, dos quais os mais críticos estão refletidos nos critérios abaixo comentados.

Em segundo lugar, se o organismo não é vinculado à ONU (o que, além de ser inaceitável para muitos usuários da Internet, é também agora politicamente improvável, uma vez que a CSTD recusou-se a convocar um grupo de trabalho para considerar os mecanismos de cooperação aprimorada), não há razão para que não seja levado adiante pela comunidade. Em resumo, usuários da Internet têm que tomar a iniciativa de propor esta agenda positiva para a governança da Internet, tal como o fizeram ao derrotar as propostas SOPA, PIPA e ACTA. Na verdade, neste ponto, se a sociedade civil não liderar este processo (talvez com o apoio de um grupo de empresas ou governos progressistas), é provável que ele nunca aconteça.

Terceiro, é preciso ter um papel definido para os governos nessa nova organização. É possível para os governos participarem de uma organização privada de governança? Certamente - pensemos na própria ICANN, na qual governos participam através do Conselho Assessor de Governo (GAC)[31].

25. Ver http://www.isoc.org 26. Ver http://www.itu.int 27. Ver http://globalnetworkinitiative.org 28. Ver http://hub.coe.int 29. Ver http://press.terminus.net.au/igfbook 30. Ver http://web.archive.org/web/20050209065808/http://www.istf.isoc.org 31. Um exemplo muito relevante do Brasil é o Comitê Gestor da Internet no Brasil, CGI.br. Ver http://cgi.br [N.E.]

De fato, a ideia de uma organização privada levar adiante a governança de um bem comum global, com a participação e apoio de governos através do sistema internacional, já tem séculos, pelo menos a partir da formação em 1863 do Comitê Internacional da Cruz Vermelha. Como a participação de governos ainda alarma alguns ativistas da Internet, torna-se ainda mais crítico o segundo critério - que a organização seja estabelecida pela comunidade.

Quarto, de acordo com a Agenda de Túnis da CMSI - que destaca as distintas contribuições que os grupos de interesse têm a oferecer em seus respectivos papéis -, a estrutura da organização deveria refletir isso, através de um corpo executivo com representação formal de membros de governos, setor privado, comunidade técnica e sociedade civil. Muito embora a estrutura do IGF não faça isso, a de outras redes pluralistas o faz - bons exemplos incluem o Forest Stewardship Council[32] e a Fair Labor Association[33]. Em termos práticos, isto deveria significar que decisões do organismo, tal como a adoção de princípios, deveria ser feita por consenso básico em cada categoria de membros, bem como no seu conjunto.

Um corolário adicional é que cada grupo de interesse retenha um certo grau de independência em sua própria esfera de competência. Assim, por exemplo, membros de governos podem responsabilizar-se por converter os princípios adotados pela organização em um acordo intergovernamental. Basicamente foi isso que o Conselho da Europa fez em 2001, com a adoção de uma declaração sobre princípios da Internet pelo Comitê de Ministros[34], desenvolvida num processo pluralista. Por outro lado, há boas razões para restringir o desenvolvimento de normas a instrumentos legais flexíveis, para evitar disputas dispersivas sobre a linguagem dos tratados.

Tal organização, com uma estrutura que reconheça os papéis de governos mas não os privilegie em relação a outros grupos de interesse, e uma constituição que assegure a prestação de contas e a transparência que a comunidade da Internet espera, a distinguiria tanto do inócuo IGF como das negociações não representativas do tipo ACTA e TPPA. Ela preencheria o vácuo na governança da Internet que o WGIG observou em 2005, e terminaria com a recorrente disputa sobre cooperação aprimorada que continua até hoje. E o melhor de tudo é que se este novo organismo for estabelecido pela comunidade, não temos que esperar pela aprovação de ninguém - podemos começar agora mesmo. ●

Este artigo foi publicado originalmente no blog do autor: http://igfwatch.org/discussion-board/picking-up-where-the-igf-left-off-our-role-in-the-future-of-internet-governance

32. Ver http://www.fsc.org 33. Ver http://www.fairlabor.org 34. Ver https://wcd.coe.int/ViewDoc.jsp?id=1835773

Carlos A. Afonso Diretor executivo do Instituto Nupef e conselheiro do Comitê Gestor da Internet no Brasil

Espectro e novas tecnologias de rádio digital – oportunidades e desafios

:: UMA FICÇÃO INTRODUTÓRIA

O ano é 2013. A história é hipotética. A cidade é Presidente Prudente – um município de 210 mil habitantes no oeste paulista. Poderia ser qualquer outra cidade média ou pequena do Brasil, mas temos que escolher uma entre as 5.565 municipalidades brasileiras para nosso exemplo – e escolhi o lugar onde nasci, a 90 km do Rio Paraná. Neste município, dos 45 canais de TV definidos para a TV digital brasileira, foram designados os canais 19 (Rede Bandeirantes), 26 (Rede Vida), 31 (Rede Globo), 43 (Rede Record) e 57 (MTV Brasil) – sendo que os dois últimos ainda não estão em operação (este é um dado real, nesta história hipotética).

A prefeitura municipal, em conjunto com a comunidade (volto a lembrar que este é um exemplo hipotético), decidiu construir uma rede municipal para prover acesso à Internet nos domicílios ao menor custo possível, com qualidade - e também fornecer uma variedade de serviços públicos que

Nota: esta é uma versão de trabalho sobre o tema, como parte de uma linha de pesquisa em andamento do Instituto Nupef relacionada a aplicações comunitárias do espectro aberto. Correções e comentários serão muito bem-vindos.

incluem conectividade para a segurança da cidade (por exemplo, para veículos dos serviços públicos, câmeras de monitoramento etc.) e vários serviços de e-governo local. A prefeitura fez um acordo com a Telebras, que fornece o trânsito da rede municipal com a Internet a um preço que os gestores da rede municipal podem pagar, via um ponto de presença de fibra óptica no município. Combinando rádios cognitivos operando nas faixas de 700 MHz e utilizando os canais do dividendo digital (uma vez que dos 45 canais definidos para a TV digital, somente cinco estão ocupados no município por designação do agente regulador), com dispositivos wi-fi para distribuir conectividade nos domicílios, a rede municipal é um sistema de referência de inclusão digital em municípios brasileiros.

Seria possível tornar esta história real? No Brasil, (ainda) não. Nossos agentes reguladores parecem ignorar algo que nos EUA vem sendo planejado em sucessivas consultas públicas e executado desde 2004 – o aproveitamento das faixas liberadas da TV analógica e dos "espaços em branco" entre os canais para uso comunitário e para serviços de Internet no âmbito dos municípios, com o emprego de transceptores digitais avançados conhecidos como "rádios de software" ou "rádios cognitivos".

Rádios cognitivos? Espaços em branco? Faixas em torno de 700 MHz?? Para que isso, se já há tantos municípios que resolvem suas necessidades de rede municipal com redes wi-fi, cuja legalização já é sacramentada e a tecnologia já é bem conhecida?

Este texto pretende oferecer uma explicação introdutória sobre o que são espaços em branco, rádios cognitivos, como estas tecnologias podem ser utilizadas, que vantagens podem trazer, e os obstáculos e oportunidades para que um município como Presidente Prudente (ou qualquer outro município brasileiro) possa pensar em um projeto integrado de Internet para a comunidade como alternativa às ofertas dos conglomerados de telecomunicações e de mídia.

:: A FALÁCIA DO "ACESSO MÓVEL"

No debate sobre os caminhos da democratização ampla do acesso à Internet, há uma forte presença das operadoras de telefonia móvel, que procuram convencer-nos que a conectividade móvel (via redes celulares) será a solução "definitiva" para esta democratização. Para reforçar essa visão, apresentam estatísticas de acesso global à Internet na ponta somando números de celulares vendidos e conexões reais de banda larga fixa sem distinção de qualidade, preços e disponibilidade. Para piorar, as operadoras priorizam áreas de mercado que geram mais ingressos, e no Brasil vêm praticando os preços mais altos do mundo.

A grande maioria da população brasileira considerada pelas telefônicas como "conectada à Internet" usa celulares em contratos pré-pagos, muito raramente navegam na Internet, e a opção pela rede celular sem uma efetiva estratégia de universalização do acesso no domicílio significa

perpetuar uma estrutura de castas – as que podem pagar terão o melhor serviço móvel em seus *smartphone*s e uma boa banda larga fixa em casa, e as que não podem pagar terão uma banda pseudolarga em casa e uma forte restrição econômica de uso da Internet pelo celular pré-pago. E essa tendência pode agravar-se com as propostas do lobby das grandes operadoras (manifestando-se fortemente no processo de definição dos novos Regulamentos Internacionais de Telecomunicação – ITRs)[1] para que estas decidam os termos dos contratos de interconexão com provedores de conteúdo e com os usuários na ponta, violando princípios básicos de neutralidade e isonomia de acesso.

No entanto, isso não significa que transceptores digitais (o telefone celular é um transceptor ou rádio digital – na verdade um *smartphone* hoje pode conter vários rádios digitais para diferentes funções) não têm futuro na ponta. Pelo contrário, além do que já é bem conhecido em inúmeras aplicações domésticas e comunitárias (as técnicas de conexão via wi-fi), novas técnicas de comunicação via rádio que utilizam de modo cada vez mais eficaz o espectro eletromagnético têm progredido muito e podem avançar ainda mais – ao ponto que espaços do espectro que eram considerados "esgotados" podem ser muito melhor aproveitados.

Por outro lado, para tornar um sonho como o descrito na abertura deste artigo em realidade para todos os nossos municípios, é preciso reconhecer a necessidade de investimentos maciços em redes troncais (espinhas dorsais) de transporte de dados, através das quais transitam dados de milhões de celulares e conexões fixas. Dados apresentados pela Cisco[2] estimam um crescimento global de tráfego de dados de 26 vezes entre 2010 e 2015 em redes móveis, quando estarão trafegando 230 petabytes[3] por dia (ou 26,7 terabits por segundo) – especialmente devido à crescente demanda por vídeo móvel e acesso às "nuvens" da Internet.

Além do aumento do número de estações de radiobase (as estações ou "antenas de celular" que vemos no topo de alguns edifícios) para desafogar as existentes (no Brasil há até dez vezes mais celulares por estação que nos EUA ou Europa), é preciso investir nas redes troncais que transportam as chamadas e dados dessas estações entre si e para a Internet. Os ramos de fibra óptica dessas redes troncais precisam chegar a todos os municípios, com capacidade abundante e à prova de futuro, oferecendo um ou mais pontos de presença da rede com garantia de acesso isonômico e a custo acessível para redes comunitárias, redes de pesquisa, redes municipais, bem como para empreendedores locais de serviços Internet. Essas garantias são essenciais para viabilizar o aproveitamento amplo das novas tecnologias de rádio nos bairros, nas cidades, nas comunidades urbanas esparsas e no meio rural.

1. Ver http://www.itu.int/ITU-T/itr 2. Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015, fevereiro de 2011.*
3. Um Petabyte equivale a 1048575,86 Gigabytes.

:: DE QUE ESPECTRO FALAMOS?

O espectro eletromagnético usado para radiocomunicação em geral, sob a supervisão da União Internacional da Telecomunicação (UIT/ITU)[4], tipicamente cobre o intervalo entre 3 kHz (três mil Hertz ou "ciclos" por segundo) e 300 GHz (300 bilhões de Hertz). É uma imensa faixa de espectro de frequências que vão desde o equivalente ao espectro sonoro audível até a radiação infravermelha, próxima à luz visível. Em várias formas, há hoje operações de rádio em porções de toda essa faixa de frequência.

É uma propriedade da radiação eletromagnética que, conforme a frequência aumenta, a propagação torna-se mais direcional e mais vulnerável a obstáculos físicos e condições atmosféricas. Enquanto as transmissões de rádio em ondas médias (AM, normalmente entre 535 kHz e 1,65 MHz) ou faixas tradicionais de rádio em ondas tropicais ou ondas curtas podem chegar a milhares de quilômetros, rádios em FM e televisão nos canais VHF ou UHF mal ultrapassam a linha do horizonte sem a ajuda de estações repetidoras.

Certas faixas bem estreitas de frequência são definidas em tratados internacionais como de uso livre restrito (com alcance limitado a alguns metros) para comunicação de rádio de vários tipos. Alguns exemplos do cotidiano hoje são o telefone caseiro sem fio, os dispositivos de controle remoto e *bluetooth*. As faixas denominadas "não licenciadas" na verdade têm uma autorização de operação sem licença dentro de limitações rigorosas quanto ao uso (comercial ou não), ao alcance e à potência de transmissão – é o caso das estreitas faixas onde operam os dispositivos conhecidos como wi-fi, em torno de 2,4 GHz e 5,8 GHz. Para operação nessas faixas com alcance e/ou potências maiores (por exemplo, redes comunitárias, redes municipais, provedores locais de serviços Internet), é preciso obter uma licença da Anatel.[5]

No outro extremo estão faixas licenciadas e rigorosamente controladas exclusivamente para uso primário (ou seja, de uso exclusivo permanente de uma concessionária – as frequências não podem ser compartilhadas na região de autorização, ao contrário, por exemplo, das faixas wi-fi), cedidas a operadoras para prestação de serviços específicos através de leilões ou autorizações de vários tipos usualmente a preços muito altos, ao alcance apenas das grandes empresas de telecomunicação e mídia.

No Brasil as faixas de espectro não são vendidas – o que se faz, no caso de faixas licenciadas, é a cessão de porções do espectro para uso primário em determinada região por tempo limitado, sujeito ou não a renovação. Pelo menos na lei, ninguém pode ser "dono" de faixa de espectro no Brasil – este é (ou deveria ser) um bem comum do povo brasileiro. Mesmo no caso de frequências de uso livre, os equipamentos (telefones, controles remotos, dispositivos wi-fi ou *bluetooth*, entre outros) têm que ser certificados pela agência reguladora, a Agência Nacional de Telecomunicações (Anatel)[6].

4. Ver http://itu.int 5.Ver Há dois tipos de licenças "leves" no Brasil para operação de redes sem fio, requeridas mesmo que utilizando dispositivos não licenciados nestes casos: para operação comercial, deve-se obter uma licença de Serviço de Comunicação Multimeios (SCM) – uma autorização única de R$9 mil. Para uso sem finalidade lucrativa, como uma rede municipal ou comunitária, há a licença de Serviço Limitado Privado (SLP), ao custo simbólico de R$400. 6. Ver http://www.anatel.gov.br

:: AS NOVAS TECNOLOGIAS DE TRANSCEPÇÃO DIGITAL

De especial interesse para aplicações comunitárias são os rádios wi-fi e equipamentos similares que operam com a tecnologia de espalhamento de espectro (*spread spectrum*), uma técnica de mudança automática de canais que permite compartilhar as estreitas faixas não licenciadas com dezenas de outros rádios em cada localidade. Estes hoje são os dispositivos mais usados para o acesso na ponta em redes comunitárias e redes municipais, e, em vários casos, mesmo em serviços comerciais locais de acesso à Internet. Os rádios wi-fi operam comumente faixas de frequência em torno de 2,4 GHz e 5,8 GHz. Rádios *spread spectrum* digitais podem ser considerados os primeiros rádios digitais para comunicação de dados operados por software embarcado, também conhecidos simplesmente como "rádios de software".

Avanços recentes que combinam poder de computação, logística de informação e técnicas avançadas de rádio digital levam a uma nova tendência na radiocomunicação: os rádios cognitivos. Trata-se de rádios de software especialmente concebidos para operar em várias frequências de modo automático programável, seja através da consulta a um banco de dados remoto de frequências disponíveis em sua região de operação (logística de informação), seja através de sofisticados algoritmos de sensoriameno de frequências em uso (poder de computação), permitindo até o uso secundário (ou seja, coexistindo com o uso formalmente cedido pelo agente regulador) de faixas sem afetar o serviço primário respectivo nessas faixas. Por exemplo, uma operadora pode ter uma licença na faixa de 700 MHz mas usar apenas algumas porções da faixa em cada região – um rádio cognitivo pode identificar por algoritmos que porções não estão sendo utilizadas a cada microssegundo e operar nessas porções, prestando outros serviços.

Um rádio cognitivo pode ser capaz de operar em diversas porções de espectro sem uso simultaneamente, ampliando em muito sua capacidade de transmissão de dados. Há rádios em teste que são capazes de operar em qualquer frequência entre 100 Mhz e 7,5 GHz com uma capacidade de transferência de dados de até 400 Mbits/s.[7]

:: O FIM DA TV ANALÓGICA, O DIVIDENDO DIGITAL E OS ESPAÇOS EM BRANCO

A tabela de atribuições do espectro de um país é muito longa e em geral inclui as atribuições propostas pela UIT e as efetivamente adotadas no país. O "filé mignon" do espectro atualmente está entre 50 MHz e 6 GHz – isso inclui todas as faixas de rádio FM, TV analógica e digital, bem como as inúmeras faixas de frequência de telefonia móvel e enlaces ponto a ponto de alta velocidade, entre outras.

As faixas de televisão nas Américas em geral vão de 54 MHz a 88 MHz e 174 MHz a 216 MHz para os

7. "Frequency-Hopping Radio Wastes Less Spectrum", Technology Review, June 13, 2012, http://www.technologyreview.com/news/428182/frequency-hopping-radio-wastes-less-spectrum

canais VHF (canais 2 a 13) e de 470 MHz a 890 MHz para os canais UHF (canais 14 a 83). O intervalo entre 88 MHz e 174 MHz é ocupado por canais de rádio FM, de radionavegação aérea e canais de radiomadores. A distribuição de canais analógicos no Brasil segue exatamente a dos EUA, já que adotamos uma variação do sistema NTSC de televisão – em que a única diferença é a forma de modulação para as cores, para a qual o Brasil adotou a norma europeia PAL, dando origem ao padrão brasileiro conhecido como PAL-M. As faixas de frequência para os canais de FM e TV portanto são idênticas às dos EUA, e os canais de TV têm, do mesmo modo, uma largura de faixa de 6 MHz. O canal 37 está reservado a radioastronomia, e os canais 52 a 83 (698 a 890 MHz) são atribuídos a serviços móveis terrestres e estão em disputa para uso com novas tecnologias (4G/LTE).

A UIT considera como "dividendo digital" as porções do espectro originalmente designado à TV analógica que não serão utilizadas na TV digital. Com a migração para a TV digital, estas porções estão ou estarão em disputa. Ademais, na transmissão analógica de rádio e TV, é necessário sempre deixar em cada localidade um canal vazio para evitar interferências entre canais adjacentes – estes são os "espaços em branco" (*white spaces*). Por exemplo, em uma mesma localidade podem coexistir os canais 2 e 4 de TV analógica, mas o canal 3 tem que permanecer vazio. Na TV digital essa separação perde o sentido, uma vez que a tecnologia permite o uso de frequências adjacentes sem interferência. No dividendo digital e nos espaços em branco estão as novas oportunidades de uso do espectro de forma ampla para uso comunitário, bem como para uso por governos e empreendedores locais, especialmente com o emprego de rádios cognitivos.

No Brasil a introdução da TV digital foi regulamentada pelos decretos 4901/2003 e 5820/2006, com a criação do Sistema Brasileiro para Televisão Digital (SBTVD)[8]. Estão definidos 45 canais (canais 14 a 69) operando entre 470 MHz e 806 MHz.[9] A regulação não estabeleceu esta plataforma como um novo serviço. Os atuais detentores de autorizações de canais receberam uma faixa de frequência com a mesma largura dos atuais canais analógicos (6 MHz), e os canais comerciais não podem operar com multiprogramação. A regulação permite o uso de multiprogramação somente para serviços públicos, o que foi reafirmado pela Portaria 106 de 03 de março de 2012: "permite o compartilhamento não-oneroso das faixas de programação entre órgãos da União – que tenham canais de 6 MHz consignados para transmissão digital – e órgãos, autarquias e fundações públicas dos estados, do Distrito Federal e dos municípios... devem ser respeitadas as finalidades educativas, artísticas e culturais; divulgação de programações locais e regionais; de estímulo a produções independentes; divulgação

8. Informação detalhada sobre o SBTVD está em http://pt.wikipedia.org/wiki/SBTVD 9. A lista completa dos canais e cidades já definidos no Brasil pode ser consultada na Wikipedia: http://pt.wikipedia.org/wiki/Anexo:Lista_de_canais_da_televis%C3%A3o_digital_brasileira

de atos, sessões etc de interesse dos órgãos e, ainda, aplicações de serviços públicos."[10]

O SBTVD é uma versão modificada da plataforma japonesa ISDB-T, e é conhecida internacionalmente como ISDB-Tb. Esta versão modificada é também adotada pela Argentina, Chile, Peru, Venezuela, Equador, Paraguai e Costa Rica. Outros países que em 2011 consideravam a adoção do sistema brasileiro eram a Bolívia, Jamaica, República Dominicana, Belize, Guatemala, Honduras, Nicaragua, Suriname, Moçambique, Tanzânia, Malawi e África do Sul. O padrão utiliza o sistema de compressão de vídeo H.264 (MPEG-4 AVC) e um *middleware*[11] desenvolvido no Brasil – o Ginga. Em abril de 2009 a UIT certificou o módulo Ginga-NCL e sua linguagem de programação associada NCL/LUA como a primeira recomendação internacional para ambientes multimeios digitais interativos para TV digital e IPTV (recomendação H.761).

Cada canal permite transmissão em alta definição plena (1080p) ou a transmissão simultânea de um canal em alta definição (720p) e um canal em definição padrão (480p) – esta última forma é a que está sendo utilizada pelas principais emissoras que já operam em modo digital. A má notícia é que o prazo para que as emissoras completem a transição foi adiado pelo Ministério das Comunicações de 2016 para 2020 – mas não é preciso esperar pela transição para começar a utilizar os espaços em branco com rádios cognitivos, desde que os entes reguladores percebam a urgência de definições neste campo.

:: OS AVANÇOS NOS PAÍSES DESENVOLVIDOS

Em janeiro de 2012, a primeira rede comercial utilizando os espaços em branco da TV UHF foi ativada nos EUA, na cidade de Wilmington, Carolina do Norte, culminando um processo regulatório iniciado pela Federal Communications Commission (FCC) em maio de 2004 (quando foi iniciada uma consulta pública sobre o uso de dispositivos não licenciados em canais de TV sem uso). O resultado dessa consulta foi o anúncio, em setembro de 2006, pelo Escritório de Engenharia e Tecnologia da FCC, de um "cronograma projetado para efetivar a operação não licenciada nos canais de transmissão de TV."[12]

Dadas suas características de propagação muito melhores que as do wi-fi, a rede de Wilmington permite o posicionamento muito mais fácil de certos dispositivos e serviços, como a rede municipal de câmeras de monitoramento, comunicação de veículos dos serviços públicos, bem como a ativação de pontos de acesso sem fio (combinando, por exemplo, a rede da cidade com distribuição local via wi-fi). Como emprega rádios cognitivos, a rede não interfere nas transmissões

10. "TV Digital: Minicom permite compartilhamento de multiprogramação," SINRAD-DF, 13/março/2012, em http://www.radialistasdf.com.br/noticia2.php?id=758
11. Middleware é o neologismo criado para designar camadas de software que não constituem diretamente aplicações, mas que facilitam o uso de ambientes ricos em tecnologia da informação. A camada de middleware concentra serviços como identificação, autenticação, autorização, diretórios, certificados digitais e outras ferramentas para segurança. Ver em http://www.rnp.br/noticias/2006/not-060926.html 12. US Federal Communications Commission, "Office of Engineering and Technology Announces Projected Schedule for Proceeding on Unlicensed Operation in the TV Broadcast Bands", DA 06-1813, ET Docket No. 04-186, 11-setembro-2006.

de TV. No caso de nosso exemplo hipotético do começo deste texto, o município de Presidente Prudente poderia interligar seus quatro distritos (Ameliópolis, Eneida, Floresta do Sul e Montalvão) utilizando rádios cognitivos na faixa de 700 MHz com bem menos estações repetidoras que seriam necessárias se usasse redes de malha wi-fi.

Do mesmo modo, a FCC tem apoiado desde 2009 (através de medidas regulatórias e experimentos concretos) o uso da mesma tecnologia em redes municipais e comunitárias. Isso tem estimulado a indústria de equipamentos de rádio a avançar no lançamento de rádios cognitivos disponíveis comercialmente para essas aplicações. As estratégias de projeto trabalham com uma combinação de rádios cognitivos nos canais em torno de 700 MHz com rádios wi-fi nas faixas de 2,4 GHz e 5,8 GHz, formando uma espinha dorsal integrada municipal.

Os EUA estudam a reatribuição do espectro nas faixas de TV analógica desde 2002. A FCC concordou no final de 2008 em abrir os espaços em branco (conhecidos no jargão técnico como TVWS) para uso não licenciado ou licenciamento "leve". Em setembro de 2010 aprovou as regras para operar rádios nos espaços em branco e nos canais livres onde a transição para a TV digital já foi concluída, com a adoção do método de geolocalização de frequências livres por base de dados, para proteger o uso primário do espectro de possíveis interferências. Um conjunto de faixas equivalentes a 48 canais de TV analógica, totalizando 288 MHz, foi liberada para uso não licenciado ou para licenciamento leve. Um novo padrão para rádio cognitivo para essas aplicações foi desenvolvido pela IEEE (802.22)[13] e publicado em 2011.

No Canadá, em agosto de 2011 o Ministério de Indústrias do Canadá (Industry Canada) fez uma consulta para o possível uso de dispositivos cognitivos não licenciados nos espaços em branco ou livres das faixas abaixo de 698 MHz. Desde setembro de 2010 o Canadá segue a política de licenciamento leve para essas faixas, em faixas similares às dos EUA. Para aplicação em áreas rurais, também com licenciamento leve, estão reservadas as faixas 512-608 MHz e 614-698 MHz. Outros exemplos de países que avançaram com regras similares são a Finlândia, a Inglaterra[14] e o Japão. A União Europeia trabalha para definir regras comuns similares.

:: AS PERSPECTIVAS NO BRASIL E EM NOSSA REGIÃO

O avanço das tecnologias de rádio cognitivo viabiliza inúmeras aplicações de uso secundário do espectro. Utilizando transmissão digital com tecnologias avançadas de modulação (como as empregadas nas atuais redes 4G/LTE) pode-se alcançar densidades de dados de mais de 15 bits por Hertz.

13. Ver http://www.ieee802.org/22 14. Na Inglaterra, as seguintes faixas são consideradas disponíveis para uso não licenciado ou licenciado "leve": 566-590 MHz (atuais canais de TV UHF 33 a 35); 806-854 MHz (atuais canais de TV UHF 63 a 68). As faixas 470-550 MHz, 790-806 MHz e 630-790 MHz são reservadas à TV digital, totalizando 259 MHz de espectro, ou 34 canais de 8 MHz. Algumas variações menores devem ocorrer com a relocação de faixas atualmente usadas para radar e radioastronomia.

Em um canal de 6 MHz dos espaços em branco, por exemplo, com essa densidade se poderia transmitir teoricamente a 90 Mbits/s (comparados aos cerca de 20 Mb/s do broadcasting da TV digital). Como já visto, pode-se combinar várias faixas para aumentar a capacidade de transmissão.

Em torno da frequência de 450 MHz (em que as condições de uso são muito similares às faixas em torno de 700 MHz) já há tecnologias comerciais e exemplos concretos de uso do rádio cognitivo para redes de grandes empresas, que tradicionalmente usam essa banda para suas redes internas.[15] Aqui também há espaço a considerar para uso secundário, especialmente no meio rural e em áreas de comunidades esparsas.

Enquanto nos EUA e em outros países desenvolvidos tem havido um forte avanço das estratégias regulatórias associadas às tecnologias de rádio cognitivo para permitir seu uso na otimização do espectro e também na ponta, no Brasil e em outros países da América do Sul essas iniciativas têm sido tímidas - na melhor das hipóteses. Comunidades e governos locais, sem informação qualificada, não têm como demandar dos agentes reguladores normas adequadas de licenciamento, e estes agentes por sua vez estão quase que exclusivamente concentrados em responder às demandas comerciais dos grandes conglomerados de mídia e telecomunicações.

O dividendo digital é um caso especialmente delicado, já que os atuais detentores dos canais de TV (basicamente grandes conglomerados de mídia) pensam em ocupar um espaço como provedores de serviços de rede usando os atuais espaços em branco, bem como os canais que serão liberados pela TV digital. Por outro lado, sob o argumento do esgotamento do espectro, as grandes empresas de telefonia móvel pressionam na disputa da faixa de 700 MHz. Um relatório da AHCIET (uma associação de empresas de telecomunicação atuantes no mercado ibero-americano)[16] argumenta que a cobertura da chamada "banda larga móvel" poderia aumentar de 75% para 95% na Argentina e Brasil, de 53% para 90% na Colômbia, de 39% para 94% no México e de 65% para 89% no Peru.[17] Mas os resultados desta disputa ainda não estão claros. Tal como as empresas de telecomunicações buscam avançar na oferta de serviços multimeios (IPTV e outros), as atuais empresas de mídia querem também atuar na faixa de 700 MHz para oferecer serviços móveis.

Comunidades e governos locais não têm como demandar dos agentes reguladores normas adequadas de licenciamento

15. Ver o exemplo de Petrobras no Brasil em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27950&sid=17&utm_medium=twitter&utm_source=twitterfeed 16. Ver http://www.ahciet.net 17. Estudo contratado com a Telecom Advisory Services LLC (TAS) pela GSMA e AHCIET. Ver http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27781&sid=17&utm_medium=twitter&utm_source=twitterfeed

Na disputa pelas faixas de 700 MHz, os conglomerados de mídia argumentam que é muito cedo para decisões sobre designação desses canais, e que as empresas de telecomunicações já têm uma grande quantidade de espectro disponível que usam de modo ineficiente. De acordo com os cálculos de uma das associações empresariais de mídia (ABERT)[18], as empresas de telecomunicações no país já detêm um total de espectro equivalente a uma largura de 795 MHz, enquanto para o mesmo setor nos EUA essa largura é de 574 MHz (onde há um uso muito mais intenso) – e em ambos os países há evidências de uso ineficaz do espectro.[19] A mesma ABERT afirma que a alegada necessidade de 1280 MHz adicionais para uma amostra de 14 países não se confirma na prática.

Já o Ministério das Comunicações (MiniCom) afirma que a atribuição dessas faixas só ocorrerá depois da desativação da TV analógica. Entidades civis que monitoram as políticas de uso do espectro no Brasil insistem que a atribuição e distribuição do espectro tem que ser decidida com base em consultas públicas com a sociedade e não somente com base em modelos de negócios. A Constituição do Brasil prevê um sistema público de TV com alcance amplo, mas isso até hoje não avançou a contento, em parte pela alegada "falta de espectro". Agora existe a oportunidade, com a TV digital, de avançar muito.[20]

Enquanto na América do Norte e Europa praticamente toda a regulação para uso comunitário já foi definida ou está sendo concluída, com instalações comerciais concretas já em operação em algumas municipalidades, no Brasil a Anatel está concentrada apenas na definição do licenciamento para possível uso de serviços móveis 4G/LTE na faixa de 698 MHz a 806 MHz.[21] Para a Região 2 da UIT (Américas), a Recomendação 224 da entidade indica as frequências de 698 MHz a 806 MHz para serviços móveis. As recomendações da UIT foram discutidas pela Comissão Interamericana de Telecomunicações (CITEL, vinculada à OEA)[22] em 2006, que recomendou as frequências de 698 a 764 MHz e de 776 a 794 MHz para serviços móveis, reservando as frequências de 764 a 776 MHz e de 794 a 806 MHz para uso governamental – mas não ocorreu adoção formal explícita desta recomendação por parte dos países membros até agora.

Cabe especialmente a governos e empreendedores locais, bem como a entidades comunitárias e movimentos pela inclusão digital, manifestar-se ativamente por uma política em defesa do uso não licenciado ou com licenciamento leve do espectro não utilizado em cada região (ou passível de utilização secundária) empregando rádio cognitivo na ponta. Estas oportunidades requerem também uma política de acesso às espinhas dorsais com uma relação benefício/custo que viabilize essas iniciativas locais. Espera-se que os "planos de banda larga" do governo federal contemplem essas garantias para estimular a inovação e a inclusão digital, diversificando as oportunidades na ponta, que é onde todos nós vivemos. ●

18. Ver http://www.abert.org.br. 19. Luís Osvaldo Grossman, "Teles e radiodifusão afiam disputa pelo 700 MHz", *Convergência Digital*, 25-nov-2011, em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28199&sid=17&utm_medium=twitter&utm_source=twitterfeed 20. Entre estas entidades estão Intervozes (http://www.intervozes.org.br) e o Nupef (http://www.nupef.org.br). 21. Anatel, Portaria 681, 6-agosto-2012. 22. Ver http://web.oas.org/citel/en/Pages/default.aspx

Danilo Doneda Coordenador-Geral de Supervisão e Controle no Departamento de Proteção e Defesa do Consumidor do Ministério da Justiça.

Marta Mourão Kanashiro Pesquisadora e professora do Laboratório de Estudos Avançados em Jornalismo da Unicamp.

O Novo Sistema Brasileiro de Identificação traços exclusivos de uma transformação geral

A adoção de uma nova carteira de identidade no Brasil, mais conhecida como RIC (Registro de Identidade Civil), tem história longa, começando com os dispositivos da lei 9.454, aprovada em 1997. No entanto, a implantação da nova carteira de identidade é muito mais recente. Podemos dizer que o início do processo se deu quando houve a aquisição do equipamento necessário para digitalizar a identificação biométrica, ocorrida em 2004. Porém, nem a lei nem seu processo de implantação foram visíveis o suficiente para causar um debate público acerca do assunto. Deve-se acrescentar neste quadro brasileiro a falta de um debate teórico e acadêmico sobre essa mudança na identificação das pessoas e sobre as tecnologias envolvidas em tal transformação.

Esse processo é influenciado por discursos e práticas que merecem uma análise mais detalhada, especialmente porque ele também aponta para mudanças extensas bem como específicas, marcadas por diversas mudanças de significado, conforme detalharemos neste artigo. Vale destacar que o aspecto tecnocrático do processo praticamente impossibilita qualquer tentativa de oposição, como se esse sistema de identificação já viesse isento de quaisquer características obscuras ou negativas.

Esse fato por si só justifica a importância de uma análise mais minuciosa de um sistema cujas consequências se farão sentir para todos os brasileiros num futuro próximo.

O fato de não ter sido implantado um sistema análogo em outros países que, antes do Brasil, já tinham as possibilidades técnicas e econômicas para fazê-lo é nossa principal questão. Iniciativas dessa ordem já foram propostas algumas vezes, e, algumas vezes, devidamente contestadas. Nessas ocasiões, é importantíssimo o entendimento geral de que tais sistemas prejudicariam um certo equilíbrio de poder informacional entre cidadãos e o Estado ou empresas privadas – enfraquecendo os cidadãos, ao levá-los a abrir mão de meios para o controle de suas vidas e atividades. A oposição a iniciativas desse tipo tem contribuído para uma maior proteção dos dados pessoais como um direito fundamental na sociedade da informação.

:: NOVAS FORMAS DE IDENTIFICAÇÃO

No Brasil, o RIC vai substituir o documento nacional de identificação civil, a atual Carteira de Identidade, também conhecida como RG (Registro Geral). O Brasil é um dos países com tradição em dar carteiras de identidade aos seus cidadãos como forma de possibilitar ou facilitar sua identificação em instâncias tanto públicas quanto privadas. Destaque-se que essa tradição se contrapõe a outra, igualmente forte, muito presente em países de cultura anglo-saxônica, onde tal documento não se faz necessário por si só.

O RG no Brasil é emitido pela Secretaria de Segurança Pública de cada Estado da União e, na falta de um sistema de cadastro centralizado entre esses órgãos, toda pessoa pode conseguir mais de uma carteira de identidade, cada qual oriunda de um estado diferente e com distintos números de identificação.

Os principais argumentos do Governo Federal a favor da adoção do RIC são: a ideia de modernização e coordenação nacional desse sistema, o combate a fraudes ou duplicidade da identidade, bem como a promoção da cidadania e da democracia.

A instituição do RIC conta com o apoio da lei 9.454 de 7 de abril de 1997, que diz ser a exclusiva numeração desse documento a principal forma de identificação para todos os cidadãos brasileiros, em todas as suas relações com a sociedade e com organizações privadas ou governamentais. Com vistas a isso, o RIC vai confluir vários outros documentos, como a carteira de identidade (RG), a carteira de habilitação, o Cadastro de Pessoa Física (CPF), o título de eleitor, a Carteira de Trabalho e Previdência Social (CTPS), o cadastro do indivíduo no PIS/PASEP (Programa de Integração Social / Programa de Formação do Patrimônio do Servidor Público) e o número de registro no INSS (Instituto Nacional do Seguro Social). Assim, será possível estabelecer conexão com a maioria dos bancos de dados de maior relevância para a vida de um cidadão normal num único documento e num único banco de dados.

A lei 9.454 foi sancionada pelo presidente do Brasil na ocasião, Fernando Henrique Cardoso . Sua entrada em vigor deveria ter ocorrido 180 dias após sua publicação e sua implantação deveria ter começado no prazo de 360 dias. No caso do RIC, a entrada em vigor da lei é fundamental para determinar sua eficácia real . Entretanto, isso só foi ocorrer em 2010. Como no Brasil o prazo para entrada em vigor desse tipo de legislação vence a cada 5 anos, já houve solicitações no Congresso para estender o prazo (RQS 190 de 2001 e projeto de lei 5.297, de 2005) . Durante o processamento dessas solicitações, houve ocasiões em que a atual carteira de identidade (RG) e o CPF ficaram sem validade legal no país.

Na verdade, o processo de implantação da nova carteira de identidade – incluindo dados biométricos – vai além da esfera jurídica. Como a lei não tinha entrado em vigor, também ficaram faltando mecanismos jurídicos para serem aplicados especificamente ao processo e capazes de estipular formas externas de controle e supervisão da própria carteira. Da mesma forma, não foram desenvolvidas regras normativas quanto ao acesso e utilização dos dados pessoais que vão constar no novo documento e em seu respectivo banco de dados. É importante destacar que os grupos mais engajados na implantação do RIC são basicamente órgãos de segurança pública.

Entretanto, a lentidão para aprovar a lei, a falta de um debate público e de mecanismos jurídicos de supervisão, até mesmo a obscuridade das regras para o acesso aos dados não devem ser entendidos como uma implicação de que o projeto esteja longe de ser efetivamente implantado. Conforme o sítio Web mantido na Internet pelo governo do Estado de Rondônia, este estado é um dos pioneiros na implantação do novo documento, devido à população de pequenas proporções. O Instituto de Identificação Civil e Criminal da capital PortoVelho deu início ao processo de digitalização de quase 1.100.000 carteiras de identidade em dezembro de 2008, como uma das fases de implantação do RIC. O mesmo processo teve início também em outros quatro estados brasileiros, ao mesmo tempo em que se ampliaram as estruturas de identificação e treinamento para o uso do novo sistema. No sítio Web do governo, o Secretário de Segurança garantiu que Rondônia tinha adotado o melhor sistema para fazer o RIC: "Enquanto outros estados estão construindo seus sistemas junto a empresas privadas, investindo cerca de 20 milhões de reais, nós estamos trabalhando em parceria com a Polícia Federal." (Identificação, 2009).

Assim, apesar de não haver regras, transparência, nem debate público, o projeto está sendo implantado devagar e de forma quase invisível, principalmente em regiões distantes dos grandes centros, onde notícias como esta teriam imensa repercussão. Apesar destes procedimentos terem começado em 2008, é possível datar o início do processo em 2004, ano em que o governo federal investiu 35 milhões de dólares para adquirir o sistema AFIS (*Automatized Fingerprint Identification System*), necessário para informatizar a identificação no país.

Agora sob a responsabilidade do Conselho de Justiça Federal, o sistema possibilita o cadastramento eletrônico das impressões digitais em bancos de dados eletrônicos, bem como o cruzamento dessas informações com outras.

O novo documento de identidade lembra um cartão de crédito: uma plaqueta de policarbonato rígida o suficiente para permitir a inserção de chips de memória para armazenamento de dados pessoais, inclusive aqueles já escritos no documento (também chamados de dados biográficos, como, por exemplo, o nome próprio, o dos pais, a data do nascimento e o sexo do indivíduo), e outras informações pertinentes a outros documentos, como o número da carteira de trabalho. A carteira de identidade também poderá ser usada como um cartão de crédito.

No verso do documento, há uma reprodução digital do polegar direito, preferivelmente obtida com o sistema AFIS. A gravação eletrônica é feita posicionando-se o dedo sobre uma superfície de vidro enquanto a leitora ótica projeta uma luz sobre a impressão digital, que é assim "fotografada", gerando uma imagem digital, uma sequência de números zero e um que representam pontinhos (pixels) para formar uma imagem. Uma vez capturada, essa imagem pode ser guardada num banco de dados ou comparada com outras para fins de identificação.

Essa verificação é feita através da análise dos detalhes ou traços característicos da impressão digital por um algoritmo matemático. Para verificar a correspondência entre um par de impressões digitais, por exemplo, o sistema busca padrões comuns, cuja quantidade pode variar conforme a configuração do sistema. Aqui é importante destacar que a utilização da tecnologia biométrica e do AFIS não deve ser compreendida como a mera aplicação de uma tecnologia mais sofisticada para a realização de tarefas que já são realizadas quando se identifica alguém com base no seu RG. Este sistema novo que essencialmente cria um imenso banco de dados e permite a referência cruzada dessas informações, além de muitos outros procedimentos, também está relacionado a uma série de transformações típicas dos nossos dias.

Conforme o primeiro projeto do RIC, elaborado em 1998 pelo atual diretor do Instituto Nacional de Identificação, Marcos Elias de Araújo, a parte inicial do banco de dados seria alimentada com as imagens eletrônicas geradas por varredura ótica dos cadastros criminais que já têm impressões digitais arquivadas em papel, um banco de dados chamado Cadastro Inicial (CIN), que contém cerca de 8 milhões de registros.

Após essa primeira fase, o projeto continua com a construção de um único banco de dados para arquivar as informações de 150 milhões de brasileiros no Cadastro Nacional do Registro de Identidade Civil (CANRIC), que vai conter os dados biográficos e detalhes de todos os cidadãos. O Ministério da Justiça é responsável pela implantação, coordenação e controle do cadastro, que será executado através da interação de algumas organizações estatais, inclusive os Departamentos de Segurança Pública ligados à Secretaria de Segurança Pública, o Instituto Nacional de Identificação, o Departamento de Polícia Federal, bem como outras agências regionais e organizações locais responsáveis pela identificação, como os

cartórios. O sistema, então, será capaz de verificar a correspondência entre impressões digitais tomadas pela própria pessoa (no processo conhecido como *scan*) e dados digitalizados pelo CIN, e poderá também verificar se uma pessoa tentou tirar mais de uma carteira de identidade sob nomes diferentes.

Durante esse processo, todos deverão comparecer a uma agência regional de identificação para se registrar no novo sistema. Depois, serão coletadas a fotografia (imagem digitalizada do rosto), a assinatura e as impressões digitais de cada cidadão. Todos esses dados podem ser considerados biométricos. Neste procedimento, as imagens do polegar e de todos os outros dedos da mão serão colhidas pelas agências de identificação e enviadas eletronicamente para o Instituto Nacional de Identificação, que por sua vez, fará a verificação e comparação, através do sistema AFIS, com dados dos agora digitalizados arquivos criminais e com aqueles já incluídos a partir do Cadastro Nacional.

O protocolo pretende confirmar a exclusividade das impressões digitais de cada cidadão, antes de atribuir-lhe um número de RIC, que poderá ser o mesmo do PIS/PASEP, para quem já o tem. Caso não se confirme essa exclusividade, o INI tornará a fazer a análise, através dos seus especialistas em impressões digitais. Os dados serão transmitidos pela Internet, ou arquivos magnéticos serão enviados por email.

É preciso enfatizar outra característica bastante importante, comum a todas as modalidades mais recentes de implantação de sistemas de identificação: o fato de que o documento de identificação, por si só, tornou-se pouco mais que o componente visível de um sistema que é, de fato, muito mais intricado que seus antecessores. O que podemos considerar como coração do sistema é o banco de dados, que vai permitir vários novos usos para as informações pessoais dos indivíduos. E esses novos usos podem configurar-se como os riscos potenciais mais sérios para os cidadãos registrados.

:: TRAÇOS EXCLUSIVOS DO CASO BRASILEIRO

Além do RIC, há outros três projetos em andamento no país que somam-se ao franco esforço que faz o Estado brasileiro para identificar as pessoas através de tecnologia biométrica inserida em documentos – e a consequente criação de bancos de dados sobre a população. São eles o da Carteira Nacional de Habilitação (CNH), o do Título de Eleitor e o do Passaporte. Todos estes documentos já incluem tecnologia biométrica e seus próprios bancos de dados também já estão sendo criados.

À primeira vista, pode parecer que eles se sobrepõem ou se anulam, no sentido de que um único documento dispensaria mudanças nos demais, como a CNH ou o título de eleitor. Contudo, por causa da meta explícita de integrar o Cadastro de Eleitores num único sistema de identificação de cidadãos, é razoável assumir que este processo seja a última instância da consolidação de bancos de dados num único sistema. Estes projetos se completam em muitas esferas com vistas a cobrir toda a população, em suas várias relações com o Estado e com as organizações não governamentais. A sobreposição de vários projetos faz bastante sentido quando leva-se em conta a área, a população e a diversidade de um país como o Brasil.

A multiplicidade de projetos de identificação no Brasil também destaca uma série de discursos fundamentadores subjacentes. A promoção da cidadania, da democracia, da modernização e da luta contra a fraude são algumas das noções lançadas como justificativas para as mudanças na forma de identificação no país. Esses projetos pegam essas ideias e as redefinem ou deslocam; ao mesmo tempo, conectam-nas com novas tecnologias que permitem vigiar e identificar as pessoas. Entretanto, no exterior, as noções não são as mesmas. Em outras palavras, é importante observar a presença, ou as tentativas de implantar tecnologias de identificação que já são comuns nas sociedades contemporâneas, mas há também as particularidades que caracterizam este processo em vários outros lugares do mundo.

Nesse sentido, as alterações relativas a essas tecnologias podem ser observadas em dois níveis (um geral e um específico), que não estão claramente separados, e, consequentemente, às vezes se interceptam e reforçam. No nível geral é possível observar que as tecnologias que permitem identificar e vigiar as pessoas, como os telefones celulares, os aparelhos de GPS, os *smartcards*, as redes sociais na Internet, documentos com chips e dados biométricos, dentre outros, estão relacionados com noções de individualidade, privacidade, subjetividade, público e privado etc. que estão em transformação. Por outro lado, existe um nível mais específico de mudanças e deslocamento de conceitos que está associado a noções lançadas como justificativas para os projetos que usam essas tecnologias.

No caso de documentos de identificação (como passaportes), é possível observar que, fora do Brasil, em lugar da modernização, do combate à fraude ou da promoção da cidadania, é mais comum encontrar justificativas relacionadas a ideias de combate ao terrorismo e à imigração clandestina, que estão ligadas a questões tais como a globalização, a garantia de mobilidade internacional, soberania e assim por diante. É, portanto, nesse nível que podem ser observadas as particularidades do processo.

Os elementos acionados no caso brasileiro para justificar os projetos supracitados também são específicos de uma pretendida transição tecnológica no país, ligada a uma certa noção de modernização. Além da simples ideia de incorporar novas tecnologias – como no caso da biometria no RIC – que traz à tona certa sensação de modernidade, apesar da continuidade das assimetrias e desigualdades que caracterizam o país, também é necessário repensar essa noção permanente de déficit, ou modernização compreendida como superação de atraso, que permeia a constituição da identidade brasileira e também marca o projeto do RIC.

Não obstante o fato de que nos países europeus ou norte-americanos o uso de tecnologias biométricas e a incorporação de um único documento sejam assuntos amplamente discutidos e combatidos, permanece no imaginário brasileiro a noção de que a presença da tecnologia está relacionada com o próprio progresso. Essa característica está ligada a uma aceitação mais ampla (ou mesmo a um desejo) das tecnologias, sejam quais forem, no cotidiano das pessoas.

Outra especificidade do caso brasileiro é o lançamento da ideia de cidadania como algo a ser promovido pela implantação do projeto do RIC. Essa cidadania não é a mesma que vem sendo definida por movimentos sociais desde a década de 1970, como uma "nova cidadania", ou uma "cidadania mais ampla", que inclui a noção do "direito a ter direitos" e que se caracteriza pela criação, invenção e definição de novos direitos pelos sujeitos enquanto agentes políticos ativos. A cidadania, portanto, não significa a mera inclusão das pessoas num sistema previamente dado e definido, determinado através de um processo de cima para baixo.

A cientista política Evelina Dagnino discute a noção de cidadania mais ampla contrastando-a com: 1) cidadania enquanto conceito liberal, ou seja, "alegação de direito a acesso, inclusão, participação e pertencimento a um dado sistema político", 2) as concepções de cidadania tradicionalmente adotadas no Brasil, ou seja, "uma estratégia de classe dominante e Estado incorporando politicamente, e de maneira gradativa, os setores excluídos, com vistas a uma integração social maior, ou como uma condição política e jurídica necessária para a instalação do capitalismo", 3) a cidadania compreendida em sua conexão neoliberal com o direito a consumir no mercado, ou enquanto solidariedade com os pobres. Com essa definição em mente, a cidadania promovida pelo novo documento RIC parece deslocada de uma cidadania mais ampla por causa de elementos relacionados com a noção liberal ou tradicional, ou por sua ligação com a ideologia neoliberal.

Cabe acrescentar a este quadro o fato de que a identificação dos cidadãos pelo Estado brasileiro já é historicamente favorável à maioria da população por tratar-se de uma pré-condição para a inclusão e o acesso a serviços e benefícios possibilitados pelo Estado. A identificação civil no Brasil não é vista pela mesma ótica de desconfiança atávica com que é tratada em alguns países, especialmente os de cultura anglo-saxônica.

Mas ainda há outros elementos que também caracterizam a particularidade da situação brasileira. Numa entrevista realizada em abril de 2006 com parte de uma pesquisa sobre a tecnologia biométrica em documentos brasileiros, um empresário envolvido com pesquisa e desenvolvimento no setor da segurança eletrônica disse que a maioria dos países ligam a coleta de impressões digitais ou o fornecimento de dados pessoais a criminosos e à ideia de suspeita, mas que isso não acontece no Brasil. Segundo ele, o RG brasileiro já contém impressões digitais, fato que por si só já reduz o potencial de uma oposição popular a tal coleta. Da mesma forma, exigir que brasileiros forneçam dados pessoais é normal em todo tipo de transação cotidiana para conseguir acesso a serviços e bens de primeira necessidade. O empresário em questão declarou ainda que a oposição comparativamente menor dos brasileiros era um fato considerado importante para aqueles que investem em tecnologias biométricas no país.

Devemos acrescentar a este quadro marcado pela aceitação por parte da maioria da população a falta de normas jurídicas ou ausência de movimentos sociais

preocupados com as novas tecnologias de vigilância e identificação, que possibilitam caracterizar o país como imenso campo de testes para a biometria e outras tecnologias de vigilância e para a implantação de bancos de dados sobre a população.

Também é importante destacar que o caso brasileiro está marcado pelo fato de que poucos são os equipamentos de segurança desenvolvidos ou fabricados no Brasil; a maioria é importada e apenas montada no país. Empresários do setor apontam uma saturação no mercado da segurança eletrônica em lugares como o Japão, a Europa e a América do Norte, e a expansão de novos mercados no Brasil, na China, na Rússia e na Índia. Segundo outra entrevista para a pesquisa mencionada: "Não temos aqui as máquinas capazes de reconhecer o rosto de uma pessoa. Elas precisam ser trazidas de fora. Trata-se de mais uma grande vantagem, pois isso significa que temos muitas coisas a construir por aqui."

Num nível mais geral, vale destacar que a aceitação da tecnologia biométrica em documentos também está relacionada à ideia de que as novas tecnologias facilitam as coisas e trazem conforto e velocidade, além de modernização e segurança. Neste sentido, a introdução dessas transformações no país deve ser vista também em conexão com o uso lugar-comum da tecnologia biométrica que acionam essas noções no Brasil. Hoje, o uso da identificação biométrica já é realidade em escolas e universidades, planos de saúde (como a Unimed Paulistana) e também para o acesso a computadores e prédios comerciais. Noutros espaços, como academias de ginástica e locadoras de vídeo, também é possível ver a participação voluntária de usuários, muitas vezes atraídos por promessas de agilidade, segurança e conforto.

É como se numa série de espaços as pessoas tivessem começado a querer a tecnologia biométrica, que é uma transformação dos procedimentos de identificação, no seu cotidiano. São exatamente esse conforto e essa agilidade que acabam incorporados por projetos como o RIC, quando seu texto declara que os brasileiros não mais precisarão carregar vários documentos diferentes. A participação da população é promovida nos vários usos da tecnologia biométrica e as pessoas indicam que desejam tais facilidades, o conforto, a agilidade e a sensação de ascenção à modernidade, ou a superação do atraso através da tecnologia. As novas formas de identificação não são, portanto, apenas uma imposição do Estado; tampouco são imposições vindas de fora. Pelo contrário; contam com a participação da população e parecem capturar seu desejo.

Em suma, se há elementos que diferenciam o processo de implantar um único documento de identificação e de usar a biometria no Brasil daquilo que aconteceu em outros países e que pode ser rastreado até o nível particular, também é necessário conectar esses elementos àqueles mais gerais vistos em outros países, pois trata-se de um fenômeno contemporâneo global que resulta em mudanças profundas nas sociedades. Há vários fatores interconectados, que reforçam a si mesmos e precisam ser separados para que os analisemos.

:: CONSTITUIÇÃO DE BANCOS DE DADOS E PERFIS

Para examinarmos este cenário, precisamos olhar para as mudanças feitas no sistema de passaportes no Brasil, que, diferente dos demais casos brasileiros de uso da identificação biométrica mencionados até o momento, foi impulsionado por fatores externos. Nos outros países, as mudanças nos passaportes resultaram numa reação em defesa da privacidade por parte de movimentos sociais e de intelectuais – tanto na América do Norte quanto na Europa. Por exemplo, em 2003 e 2004, houve intenso debate político nos Estados Unidos sobre tentativas de implantar um programa que incluísse nos passaportes uma nova tecnologia e uma forma de cruzar informações com outros bancos de dados, inclusive os comerciais.

O Departamento de Segurança do Transporte (*Transportation Security Administration*) dos Estados Unidos promoveu o CAPPS (*Computer Assisted Passenger Pre-Screening System* – Sistema Informatizado para Triagem Prévia de Passageiros), cujo objetivo era identificar passageiros que representassem maiores riscos e selecioná-los para procedimentos de segurança adicionais antes do seu embarque nos aviões. A verificação da identidade dos passageiros envolvia avaliação de risco usando bancos de dados comerciais bem como informações de inteligência do Estado. Em outras palavras, os dados contidos nos passaportes eram cruzados com aqueles contidos em outras instâncias de armazenamento para que fosse avaliado o potencial de ameaça que alguns passageiros poderiam representar.

A Electronic Frontier Foundation (EFF), uma ONG estadunidense, tentou dar maior visibilidade à questão:

"O Departamento de Segurança do Transporte dos Estados Unidos divulgou plano de implantar o CAPPS II, um polêmico sistema para vigiar e traçar o perfil de passageiros que passaria a exigir a data de nascimento, telefone e endereço residencial antes de a pessoa embarcar num vôo no país. Na vigência do CAPPS II, as autoridades competentes verificariam a veracidade desses detalhes e de outros mais a partir das informações coletadas nos bancos de dados do governo e nos comerciais, "rotulando" em seguida o indivíduo com uma pontuação e um código em cores para indicar o nível de risco à segurança que ele pareça apresentar. Com base na pontuação/cor, ele pode ser detido, interrogado ou revistado. Caso lhe atribuam uma cor/pontuação errada, o indivíduo pode ficar proibido de tomar o avião." (cf CAPPS II)

Curry (2004) destacou que sistemas que traçam perfis para identificar passageiros que possam ser perigosos só podem existir se criados estereótipos de grande abrangência e se a população for divida em grupos, neste caso, fiando-se não apenas em atributos definidos como também na probabilidade estatística de cada um desses indivíduos engajar-se em atividades consideradas perigosas. O uso da biometria nos passaportes, a maior capacidade para armazenar informações de que dispõem esses documentos e a construção de sistemas de identificação dos perfis das pessoas podem ser vistas da mesma maneira. Para Curry, a vigilância das mobilidades também requer uma busca por dados mais detalhados de forma a construir narrativas

sobre as atividades das pessoas. Ele também destaca a maneira como as técnicas de pesquisa de mercado estão sendo usadas nos sistemas de identificação de perfis, por exemplo, por empresas de transporte aéreo. O autor sustenta que é construído um sofisticado sistema nessas conexões do pessoal e do comercial a partir de narrativas que incorporam opiniões sobre uma série de comportamentos e padrões móveis definidos como aceitáveis ou suspeitos. Argumenta também que esses perfis não visam identificar o viajante no qual se pode "confiar" mas sim naquele que apresenta "risco".

Este caso está ligado ao problema com os bancos de dados, cruzamento de informações e uso de dados pessoais, conforme o caso do projeto RIC no Brasil. Continua em aberto para debate no Brasil um assunto em particular: fora do país, uma carteira de identidade que incorpora biometria, apoia-se num amplo banco de dados e concentra-se na mobilidade – contudo promove a seleção de passageiros. Será que o RIC promoveria coisas semelhantes?

:: CONCLUSÃO

Neste artigo pretendemos destacar alguns elementos que caracterizam a implantação da nova carteira de identidade (RIC) no Brasil, visando dar início a debates acadêmicos e políticos sobre o assunto. A mera implantação de uma carteira de identidade assim aponta para uma distribuição de poder desigual entre o Estado, as empresas e os cidadãos, enfraquecendo a alavancagem cidadã enquanto propicia para Estado e empresas mais meios de controlar a vida e as atividades do cidadão. No Brasil, esta situação é ainda pior devido ao fato de a implantação do RIC praticamente contornar a esfera jurídica e não ter sido visível o suficiente para incitar o debate público. E, fora a regulação jurídica básica, é óbvia a falta de mecanismos legais para o controle e supervisão do uso de uma nova carteira de identidade e das informações de cunho pessoal nela incorporadas.

Quanto à implantação do RIC, há pelo menos dois pontos que denotam falta de padrões de conduta democráticos: em primeiro lugar, a ausência de uma regulação específica relativa à lei 9.454/97, que fornece a base normativa para a implantação do RIC (e isso poderia também estar sujeito a um controle judicial prévio); e o fato de que o sistema proposto implica uma mudança concreta e qualitativa na distribuição de poder entre indivíduo e Estado (bem como certas entidades privadas) em relação ao controle efetivo de seus próprios dados pessoais. Esse desequilíbrio não pode ser compensado por soluções tecnológicas menos invasivas. Tampouco compensaria uma solução normativa, como um conjunto de leis de proteção de dados, que municiasse o indivíduo com instrumentos para o controle efetivo de suas próprias informações.

Aqui também tentamos identificar as particularidades que marcam o projeto de um único documento de identificação que incorpore tecnologia biométrica. Elas baseiam-se em noções tais como cidadania e modernização, que se encontram respectivamente conectadas à proposição de inclusão social (através da conexão entre a identificação dos cidadãos pelos estados brasileiros e os projetos de inclusão social), e a

representação do uso de tecnologias avançadas no imaginário brasileiro (em conexão com a ideia de ascenção à modernidade). Estes elementos são a base para uma aceitação mais ampla dessas tecnologias no Brasil, incorporadas de maneira irracional e não crítica.

Tal aceitação se fia noutro elemento importante: o uso das impressões digitais na atual carteira de identidade e a exigência de que os indivíduos forneçam dados pessoais em diversas situações do cotidiano. Essas características e a falta de leis ou movimentos sociais que visem discutir ou limitar a implantação do RIC criaram uma grande oportunidade para empresas especializadas em tecnologias eletrônicas de vigilância e identificação. Esse nível de particularidade, contudo, é constantemente influenciado e reforçado por um nível mais amplo, relacionado ao uso de novas tecnologias de vigilância e identificação em vários países. Nesse outro nível, podemos ver o uso da tecnologia biométrica em sua forma cotidiana como forma de capturar o desejo e a participação ativa das pessoas. E isto está relacionado com uma esfera mais ampla de mudança que inclui subjetividade.

Alguns países atribuem um número de identificação nacional aos seus cidadãos. Mas o RIC vai além disso ao propor a unificação de alguns sistemas de identificação que foram originalmente separados e seguiam lógica e regras próprias. Portanto, a nova carteira de identidade brasileira unifica não apenas o número de identificação mas também outros documentos, como o CPF, o título de eleitor e outros.

O cruzamento ou fusão dessas informações, desses bancos de dados, é visto por muita gente como um forte argumento para a implantação do RIC, mas, na verdade, trata-se de um dos seus aspectos mais questionáveis e a principal razão para a oposição a sistemas semelhantes noutros países. Ao mesmo tempo, um sistema informatizado facilita a obtenção de dados sobre uma pessoa em particular e torna essa pessoa mais suscetível à categorização por perfis e a uma classificação baseada exclusivamente nas suas informações pessoais. Esses dados também podem ser deslocados ou usados indevidamente, resultando em toda uma gama de problemas e complicações, desde a identificação equivocada até o "roubo de identidade".

Finalmente, apontamos para o aumento de possibilidades de controle e monitoramento dos cidadãos no Brasil, enquanto os de outros países podem contar com normas e sistemas de identificação que lhes propiciam proteção contra os riscos concretos de um único sistema de identificação, além de outras garantias relativas aos seus dados pessoais. Nesse sentido, o chamado "abismo digital" pode aumentar entre os cidadãos de um país e os de outro, não exatamente por conta do acesso à informação e a serviços, mas por causa da facilidade de acesso a informações pessoais, o que permite controle intenso dos cidadãos de alguns países. No Brasil, parece que o projeto do RIC tomou uma via de mão única e apresenta o risco concreto de colocar o país decisivamente neste último grupo. ●

Este texto foi publicado originalmente na revista Surveillance & Society: http://www.surveillance-and-society.org. O artigo completo em português com referências bibiográficas está em www.politics.org.br

poliTICs

COORDENAÇÃO DO PROJETO GRACIELA SELAIMEN

EDITORES GRACIELA SELAIMEN, CARLOS A. AFONSO

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN

DISTRIBUIÇÃO VIVIANE GOMES

TRADUÇÕES RICARDO SILVEIRA

Esta é uma publicação do Instituto Nupef.

Versão digitalizada disponível em www.politics.org.br e no sítio do Nupef - www.nupef.org.br

Para enviar sugestões, críticas ou outros comentários: graciela@nupef.org.br

instituto nupef

Rua Sorocaba, 219 | 501 - parte | Botafogo | 22271-110

Rio de Janeiro RJ Brasil | telefone +55 21 2527-0294

Apoio:

FORD FOUNDATION

Strengthen democratic values, reduce poverty and injustice, promote international cooperation and advance human achievement

Google

nic.br

Núcleo de Informação e Coordenação do Ponto BR

Os originais foram compostos com OpenOffice 3.X e GNU/Linux

ISSN: 1984-8803

A poliTICs procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp

O Instituto Nupef é uma organização sem fins de lucro dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a poliTICs, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – provedor de serviços internet voltado exclusivamente para instituições sem fins lucrativos – resultado de um trabalho iniciado há 21 anos, com a criação do Alternex (o primeiro provedor de serviços internet aberto ao público no Brasil). O Tiwa é um provedor comprometido prioritariamente com a privacidade e a segurança dos dados das entidades associadas; com a garantia de sua liberdade de expressão; com o uso de software livre e de plataformas abertas não-proprietárias.

instituto nupef

Rua Sorocaba 219, 501 | parte | Botafogo | CEP 22271-110 | Rio de Janeiro | RJ | Brasil
telefone +55 (21) 2527-0294 | fax +55 (21) 3259-0370 | www.nupef.org.br