ABERTURA E CONTROLE NA GOVERNAMENTALIDADE ALGORÍTMICA

Henrique Parra

Este artigo surge como desdobramento de uma apresentação realizada no Seminário Informação e Internet, organizado pelo Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) em Brasília, agosto de 2015. Com o título "Abertura e Controle", o debate contou também com a participação dos pesquisadores Sarita Albagli e Sergio Amadeu.

O tema proposto (Abertura e Controle) permite abordar algumas questões que estão na interface de dois projetos que estou conduzindo neste momento: Ciência Aberta e Desenvolvimento Local (1); Tecnopolítica e Saberes Situados. Este artigo é também um desdobramento das proposições lançadas num pequeno ensaio "Privacidade como bem comum" (2) e das reflexões provocadas pela leitura recente de dois textos: um artigo de Antoinette Rouvroy (3) e um ensaio de Amador Fernández-Savater (4).

Esta introdução se faz necessária apenas para indicar a tomada de uma perspectiva em que abertura e controle são fenômenos interconectados e interdependentes quando falamos em comunicação digital em redes cibernéticas.Os sentidos utilizados para esses dois termos neste texto são: abertura: capacidade de acessar, interpretar, difundir informação (seja para fins de produção de conhecimento ou para garantir a funcionalidade técnica de softwares, hardwares etc); e controle: capacidade de regular um conjunto de funções, eventos, variáveis com vistas à obtenção de algum resultado desejado (por exemplo, ter o controle da situação, controle do sistema etc). Mas também como uma capacidade de exercício de poder.

No caso da comunicação em meios digitais, abertura e controle podem se combinar e se efetivar através da implementação de protocolos. Segundo Alexander Galloway (5) podemos definir "protocolo" das seguintes maneiras: padrão que governa a implementação de uma tecnologia específica; ou formas de governo para obtenção de controle num dado sistema. Mais especificamente, o protocolo para os cientistas da computação pode ser entendido como: regras convencionadas que governam um conjunto de comportamentos possíveis dentro de um sistema heterogêneo; ou ainda técnica para alcançar regulação voluntária dentro de um ambiente contingente.

ABUNDÂNCIA INFORMACIONAL E OS PARADOXOS DA ABERTURA Já é senso comum falar que vivemos uma revolução dos dados (6). Com o crescente uso das tecnologias de comunicação digital, um novo universo de informações passa a ser produzido, registrado, analisado, sobre cada aspecto de nossas vidas (7), às vezes com nosso consentimento, muitas vezes com nossa cumplicidade e adesão voluntária (p.ex. Facebook), mas na maioria das vezes, sem termos a menor noção do que de fato ocorre com nossas informações (8).

Este novo manancial informacional é, por vezes, referido como o "petróleo do século XXI" (9), fazendo alusão à sua importância para as atividades econômicas e criação de riqueza monetária. Nesta dimensão, quanto mais informação disponível, quando maior o fluxo informacional, melhor para o dinamismo da economia. Paradoxalmente, tal entendimento caminha lado a lado com a defesa seletiva da expansão do sistema de propriedade intelectual sobre informações consideradas estratégicas para a inovação tecnológica. Nesta perspectiva, o livre fluxo informacional (apoiado no discurso da abertura e transparência) combina-se à expansão de novos *enclousers* informacionais.

O importante aqui é estar no melhor lugar da cadeia produtiva informacional (camada física, aplicativos, harwares etc) de forma a poder modular a membrana que regula os fluxos entre abertura e fechamento estratégico sobre a informação "que conta". Como podemos observar nos recentes acordos comerciais do Trans Pacific Partenership (10), ao mesmo tempo que promovem a expansão da propriedade intelectual sobre o conhecimento e a cultura, sob pressão das grandes corporações, as regulamentações que protegem os dados pessoais dos cidadãos europeus são atacados como inimigos do livre fluxo informacional, impedindo assim o desenvolvimento econômico dessas nações (11).

Mas esse novo universo de dados é também encarado como um recurso fundamental para o avanço da ciência em inúmeras áreas do conhecimento. Como afirmou um dos diretores de uma agência de saúde norte-americana, "as informações disponíveis sobre pacientes, tratamentos, condições de saúde, efeitos de drogas etc, organizadas como *big data* terão um efeito sobre a medicina do século XXI maior do que teve a penicilina no século XX". Não apenas na área médica, esse volume infinito de dados inaugura o *big data* em diversas disciplinas.

Mesmo as humanidades que sempre deram preferência à dimensão qualitativa e significativa das informações, e se aproximavam com suspeita tanto das tecnologias como dos dados quantitativos, abraçaram as novas possibilidades oferecidas pelas tecnologias da informação e comunicação (TICs). As chamadas humanidades digitais não trabalham exclusivamente com *big data*, mas fazem uso intensivo das novas informações produzidas através das mediações digitais presentes em nossa vida social.

Do ponto de vista estatal, seja para o acompanhamento e avaliação de suas ações, para a criação de novas formas de participação cidadã e controle social, mas principalmente para o monitoramento e controle sobre os cidadãos sob uma lógica securitária, as informações digitais produzidas e recolhidas constituem um novo recurso fundamental para o poder gestionário. Participação, transparência, acesso à informação e controle social são palavras que passaram a compor um vocabulário comum de militantes, cientistas e gestores governamentais.

Indiquei rapidamente três eixos – econômico, ciência/conhecimento e governo estatal – apenas para destacar a forma como essa

nova produção e disponibilização de dados situa-se sobre uma arena conflituosa de profunda reconfiguração social, onde as fronteiras entre público-privado, trabalho e não-trabalho, abertura e controle ganham novos contornos, e onde o surgimento de novas formas de conhecer vem acompanhado por novas formas de exercício do poder (a principal referência aqui é, evidentemente, Michel Foucault).

Os exemplos são infinitos:

i) nota fiscal eletrônica: coleta de dados sobre o consumo do cidadão que contribui para combater a evasão fiscal e, ao mesmo tempo, produz um conhecimento de alto valor de mercado sobre perfis de consumo. Quais os usos que podem ser feitos dessas informações? Quem são os intermediários e terceiros que têm acesso à ela?;

ii) dados sobre pacientes no sistema público ou privado de saúde: prontuário eletrônico, importante para ampliar nossos conhecimentos tanto sobre a saúde humana como sobre o sistema de saúde. Mas como essas informações podem ser usadas?;

iii) dados que produzimos em nosso uso cotidiano da internet que são importantes para conhecermos mais sobre determinados aspectos da vida social e, ao mesmo tempo, são o insumo básico da vigilância industrial e distribuída (estatal e corporativa).

Portanto, indicamos que essa crescente produção e disponibilização de dados (dimensão da abertura) vem acompanhada de novas formas de controle. Há, portanto, a emergência de novas formas de conhecer que se combinam às novas formas de exercício do poder. E elas não são genéricas e abstratas, mas sim, situadas (ou contextualizadas) e empíricas.

ESSA CRESCENTE PRODUÇÃO E DISPONIBILIZAÇÃO DE DADOS VEM ACOMPANHADA DE NOVAS FORMAS DE CONTROLE

É sob essa perspectiva que gostaria de avançar. Não faz sentido falarmos da abertura e transparência como valores transcendentais que devam ser aplicados genericamente às informações produzidas (uma vez que existe esta possibilidade). As condições e possibilidades de abertura devem sempre ser analisadas nos contextos específicos de sua produção e circulação, bem como nos efeitos sociais e culturais (sistêmicos) que elas podem provocar.

Pensemos, por exemplo, como os efeitos relativos à disponibilização livre e consentida de nossas informações genéticas está além de questões sobre a decisão/escolha individual e, portanto, também terão efeitos que escapam à proteção dos dados pessoais (como veremos ao final deste artigo).

Por um lado, a oferta dessas informações (p.ex. dados biomédicos) pode contribuir para o avanço dos estudos sobre doenças etc. Podemos considerar aqui que essa "abertura" é voluntária e cabe apenas ao indivíduo decidir o que fazer com seus dados pessoais. Todavia, precisamos considerar os efeitos dessa informação num cenário mais complexo em que o campo de forças econômico e político (corporações, Estados etc) é distribuído de forma assimétrica. De partida, temos atores com condições distintas de apropriação e uso dessa informação. Suponhamos que essas informações sejam utilizadas para analisar o perfil genético de um cidadão no momento de sua contratação profissional ou para a contratação de um convênio médico. Neste caso, estamos tratando dos problemas relativos à aplicação dos dados desse indivíduo sobre ele mesmo. Todavia, o simples fato de que alguns indivíduos disponibilizem suas informações genéticas livremente pode criar uma nova situação em que todos aqueles que não disponibilizam suas informações genéticas sejam tratados de forma negativa (pagar um seguro médico mais caro etc).

Por isso, além da proteção dos dados pessoais, temos que pensar em formas de regulação sobre o que é possível fazer, em termos de coleta, organização, sistematização e análise da massa de dados atualmente disponível, mesmo quando anonimizadas, portanto, fora da esfera dos chamados "dados pessoais". Foi neste sentido que escrevi um pequeno ensaio sugerindo que também abordemos o direito à privacidade com um bem comum (12).

Com isso, pode-se apontar para a emergência de um horizonte sociocultural mais amplo, que estamos produzindo com nossas pequenas ações individuais. Não seria essa a política inscrita no protocolo da transparência total pretendida pelo Facebook? A criação de uma cultura da transparência em que a disponibilização voluntária de nossos dados se naturaliza como um imperativo social e moral? É sobre esta configuração cultural mais ampla que se desenvolve o restante deste artigo.

VIGILÂNCIA E ANONIMATO Como promover o acesso à informação, ao conhecimento e à cultura e, ao mesmo tempo, combater os efeitos potencialmente perversos dessa abertura? Quando falamos em revolução dos dados (como bem interrogou o artigo de Jonathan Gray, em 13) precisamos perguntar para quem será esta revolução? Nesse sentido, parece-me importante colocar a questão da abertura num contexto muito assimétrico de distribuição do poder comunicacional, econômico e político.

Recentemente, numa lista de discussão dedicada à tecnopolítica e ao ativismo, chamada Antivigilância (14), tive contato com um documento excelente (15) de um grupo de trabalho em tecnologia da Associação Brasileira de Saúde Coletiva. Com uma percepção aguda, já no início dos anos 1990, alguns médicos e enfermeiros atentos à necessidade de se pensar em formas críticas de gestão dos grandes bancos de dados que começavam a se constituir sobre os pacientes no sistema público de saúde, produziram esse documento que levanta várias questões importantes como, por exemplo, quais são as tecnologias que podem promover a confidencialidade, proteger a identidade dos pacientes e evitar usos indevidos por empresas sobre os bancos de dados?

Da mesma forma como esses atores estavam preocupados com a identidade e a privacidade dos pacientes, hoje enfrentamos questões análogas no debate sobre a nova Lei de Proteção de Dados Pessoais.

É nesse sentido, também, que a comunidade tecnoativista tem organizado eventos, como as Cryptoparties (16), destinados a difundir o uso de tecnologias que promovam a comunicação segura,

a privacidade e o anonimato, como formas de luta contra as ações massivas de vigilância estatal e corporativa. A luta pelo direito ao anonimato na rede é de suma importância num cenário de crescente mediação digital. Na atual conjuntura a defesa do anonimato é uma possível estratégia para a defesa da liberdade de expressão, para resistir à "censura preventiva" ou ainda para combater o "conformismo antecipativo" diante dos mecanismos de *profiling*.

Não à toa, na era pós-Snowden começam a surgir serviços conhecidos como *zero-knowledge* (protocolos computacionais que objetivam eliminar a produção de informação não desejável). Outro exemplo é o esforço de ciberativistas para criar ambientes de interação que tentam recriar a situação de um encontro de duas pessoas numa floresta, numa conversa presencial e sem qualquer registro que não o da memória individual de cada uma delas.

O anonimato na rede também cumpre a importante função de criar espaços de interação que possam efetivamente funcionar como arenas públicas. É uma situação análoga ao efeito provocado pelas cidades modernas na sociabilidade, onde o espaço público se caracteriza pela possibilidade do encontro com pessoas que não conhecemos e, por isso, surgiram códigos de conduta para o bom convívio com aquele ser genérico que desconheço. Tais princípios e códigos formam a base dos direitos de cidadania.

Na medida em que os ambientes digitais produzem uma infinidade de dados sobre os usuários, a garantia do anonimato torna-se um recurso importante (mas não único como veremos adiante) para que possamos evitar a emergência de uma sociedade policial, onde sabemos tudo sobre todos, e onde todas as interações acontecem em cenários onde a possibilidade do imprevisto e do indeterminado estão sob controle.

GOVERNAMENTALIDADE ALGORÍTMICA Contudo, em todos esses casos que listamos, o conflito e as formas de apropriação e expropriação se dão sobre a fronteira dos dados públicos e privados, e também sobre a capacidade de atribuir autenticidade e identidade aos dados.

Com a crescente concentração das informações digitais nas mãos de poucos atores corporativos e estatais, as práticas de abertura e livre disponibilização de dados combinam-se à emergência do *big data,* num contexto de distribuição assimétrica no poder comunicacional (propriedade dos meios, infraestrutura, aplicativos etc). Neste cenário, gostaria de apontar que a forma de exercício de poder adquire outra dinâmica, deslocando, portanto, o conflito político para outras arenas.

Para explorar essa nova configuração entre saberes e poderes no mundo do *big data*, Antoinette Rouvroy, pesquisadora do Research Center Information, Law & Society (Bélgica), toma as ideias de Foucault e Deleuze para desenvolver o conceito de governamentalidade algorítmica, como um desdobramento da governamentalidade neoliberal:

> Eu gostaria de descrever este deslizamento da governamentalidade neoliberal em direção à governamentalidade algorítmica: um modo de governo alimentado essencialmente por dados brutos (que operam como sinais infra-pessoais e a-significantes mas quantificáveis); que afetam os indivíduos sob o modo de alerta, provocando o reflexo, mais do que sob o modo da autorização, proibição ou persuasão, ao se apoiar sobre suas capacidades de entendimento e de vontade; visando essencialmente a antecipar o futuro, a limitar o possível, muito mais do que regulamentar as condutas. Os dispositivos da governamentalidade algorítmica integram o *data-mining*: a exploração das reservas de dados massivos e brutos, que individualmente não possuem nenhum sentido, para a partir deles traçar perfis de comportamento. O *data-mining* permite gerir as pessoas de maneira personalizante, industrial, sistemática e preemptiva, se interessando por elas somente enquanto pertencentes a uma multitude de perfis (de consumidores, de delinquentes potenciais etc) (17).

Nessa perspectiva, o que está em jogo é muito mais a capacidade de produzir e gerenciar uma infinidade de perfis, de criar cenários e produzir futuros. O perfil é supra-individual (é uma categoria estatística) e é criado a partir de informações brutas, infra-individuais. Não é mais o indivíduo que conta, mas o ser dividual. Deleuze já tinha apontado isso naquele pequeno texto *post-scriptum* das sociedades de controle. Mas a governamentalidade algorítmica ocupa-se de um mundo digital muito distinto daquele observado por Deleuze.

Não se trata apenas de gerir permissões de acesso, de modular a existência dividual a partir de controles de variação contínua. É tudo isso também, porém o campo de intervenção com o *big data* cria uma "política da simulação" que é a própria morte da política, uma vez que as ações passam a ser governadas graças ao *feedback* dos parâmetros que indicam os cenários futuros produzidos com base nas predisposições estatísticas de cada perfil, de cada situação. Não se age, não se cria, modula-se.

Galloway aborda esse problema por uma perspectiva complementar que ele chamará de poder protocolar. Não é preciso se preocupar com o sentido da ação, é possível conduzir a ação de outra maneira. Na medida em que toda ação tecnicamente mediada precisa passar pelo protocolo, o importante é que este protocolo produza os efeitos desejados. É uma ação governada no presente graças ao controle sobre os efeitos desejados.

É por isso que estamos além do *big brother*. Claro, Snowden e Assange estão aí para nos lembrar dos inúmeros aparatos de vigilância. Porém, neste cenário trata-se, menos, de impedir que nos expressemos livremente. Sim, isso também acontece no momento de exercício do poder sobre o indivíduo em situações específicas. Todavia, na governamentalidade algorítmica somos convidados a sempre nos expressarmos livremente: "*escreva aqui o que você está pensando*" (Facebook), "*o que está acontecendo*?" (Twitter) entre outros.

Para além do *big brother* – tomo de empréstimo a feliz expressão de Evegeny Morozov – estamos diante da *big mother* (18). Ela sabe o que eu desejo, ela sabe o que eu preciso, ela vai me oferecer o que acha que necessito.

Antoine Rouvroy também chama nossa atenção para a importância de discutirmos o direito a um futuro não-preocupado: será que as informações que eu estou produzindo agora, mesmo que anonimizadas (portanto, não se trata de dados pessoais), não estão a compor um perfil estatístico que será utilizado no futuro para guiar minhas escolhas ou para me incluir em determinadas categorias sociais que ainda sou incapaz de imaginar?

Por tudo isso, é importante pensarmos numa política para a proteção dos dados pessoais e também nas garantias para o anonimato na rede. Porém, isso só dá conta de uma parte do problema. É absolutamente possível manter a governamentalidade algorítmica funcionando dentro do respeito àquilo que entendemos como "dados pessoais". Para enfrentarmos essa nova forma de poder, teremos que pensar em novas formas de regulação sobre a informação que é produzida, para além da dicotomia público-privado. Afinal, trata-se de discutir o que queremos fazer coletivamente com as informações que estão aí? Quais as possibilidades e o que queremos evitar? Talvez, tenhamos mesmo que pensar que a proteção dos dados pessoais não se refere mais ao indivíduo, mas sim à coletividade. Ou seja, com a crescente mediação das tecnologias digitais há toda uma nova partilha do mundo que se faz necessária, afinal a intermediação digital inaugura um novo território comum sob disputa. Uma alternativa seria pensarmos o ecossistema comunicacional de maneira análoga aos bens comuns (diferentemente do *commons* da perspectiva liberal ou neoinstitucionalista), traçando seu usufruto coletivo a partir de uma concepção renovada dos direitos no mundo digital.

***Henrique Parra** é sociólogo e ativista, professor do Departamento de Ciências Sociais da Universidade Federal de São Paulo (Unifesp) e coordenador do Laboratório de Tecnologia, Política e Conhecimento (Pimentalab). É integrante da rede Lavits e realiza pesquisa de pós-doutorado financiado pelo CNPq junto ao Instituto Brasileiro de Informação em Ciência e tecnologia (Ibict) da Universidade Federal do Rio de Janeiro (UFRJ).*

NOTAS E REFERÊNCIAS

1. Ciência Aberta e Desenvolvimento Local é um projeto interinstitucional da Open and Collaborative Development Network, apoiado pelo Internacional Development Research Center – Canadá, coordenado no Brasil pelo Ibict. No momento, o autor deste artigo realiza uma pesquisa de pós-doc no Ibict/UFRJ investigando essa iniciativa. Mais informações: http://cienciaaberta.ubatuba.cc.
2. Parra, H. Z.M.. *Privacidade como bem comum*. Disponível em: http://prototype.pimentalab.net/?p=67. Acesso em 28/10/2015.
3. Rouvroy, A. *Le droit à la protection de la vie privée comme droit à un avenir non pré-occupé, et comme condition de survenance du commun*. (Draft / Version provisoire) Entretiens à propos du droit à la protection de la vie privée (à paraître). Ed. Claire Lobet-Maris, Nathalie Grandjean, Perrine Vanmeerbeek. Paris: FYP éditions, 2014. Disponível em: http://works.bepress.com/cgi/viewcontent.cgi?article=1065&context=antoinette_rouvroy. Acesso em 28/10/2015.
4. Fernández-Savater, A. *La pesadilla de un mundo en red*: Disponível em: http://www.eldiario.es/interferencias/pesadilla-mundo-red_6_412668752.html. Acesso em 28/10/2015.
5. Galloway, A. *Protocol, how control exists after decentralization*, MIT Press, Cambridge, 2004.
6. Veja o projeto United Nations Data Revolution Group. Disponível em http://www.undatarevolution.org/ Acesso em 28/10/2015.
7. Veja o projeto Quantified Self. Disponível em: http://quantifiedself.com/. Acesso em 28/10/2015.
8. As controvérsias em torno da política de privacidade dos usuários do Windows 10.0 é um bom exemplo neste caso. Disponível em http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_and_how_to_plug_them.html. Acesso em 28/10/2015.
9. Sobre o valor econômicos dos dados pessoais para o World Economic Forum, veja http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf . Acesso em 28/10/2015.
10. O Trans Pacific Partenership é um grande acordo comercial entre os Estados Unidos e demais países alinhados à sua política comercial. Desenhado sob forte influência de grupos econômicos e corporações poderosas, ele foi elaborado distante do escrutínio público. Nos últimos meses a organização Wikileaks tem publicado partes importantes desse documento visando interrogar a legitimidade política desse acordo. Veja https://wikileaks.org/tpp/. Acesso em 28/10/2015.
11. E. Morozov desenvolve um argumento interessante sobre este fato: http://www.theguardian.com/commentisfree/2015/jul/12/ttip-your-data-privacy-is-a-barrier-to-economic-growth. Acesso em 28/10/2015.
12. Parra, H.Z.M. *op.cit*.
13. Gray, J. *Data revolution for whom?* Disponível em https://www.opendemocracy.net/ourkingdom/jonathan-grey/data-revolution-for-whom. Acesso em 28/10/2015.
14. Site do projeto Antivigilância - https://antivigilancia.org/. Acesso em 28/10/2015.
15. O documento analisado está disponível online em http://www.abrasco.org.br/site/wp-content/uploads/2015/06/GT_informacao_plano-diretor.pdf. Acesso em 28/10/2015.
16. Na cidade de São Paulo a Cryptorave é um evento anual que tem atraído um grande público - https://cryptorave.org/. Acesso em 28/10/2015.
17. Agradeço a Lilian Sampaio pela ajuda na tradução. A seguir o fragmento original em francês "*J'ai voulu décrire ce glissement du gouvernement néolibéral au gouvernement algorithmique: un mode de gouvernement nourri essentiellement de données brutes (qui opèrent comme des signaux infra-personnels et a-signifiants mais quantifiables); qui affecte les individus sur le mode de l'alerte provoquant du réflex plutôt que sur le mode de l'autorisation, de l'interdiction, de la persuasion, en s'appuyant sur leurs capacités d'entendement et de volonté ; qui vise essentiellement à anticiper l'avenir, à borner le possible, plutôt qu'à règlementer les conduites. Les dispositifs de la gouvernementalité algorithmique intègrent le data-mining: l'exploitation de gisements de données massives et brutes, qui n'ont individuellement aucun sens, pour en faire surgir des profils de comportements. Le data-mining permet de gérer les gens de façon personnalisante, industrielle, systématique, préemptive, en ne s'intéressant à eux qu'en tant qu'ils relèvent d'une multitude de profils (de consommateurs, de délinquants potentiels etc.)*".
18. Morozov, E. *The planning machine*. Disponível em http://www.newyorker.com/magazine/2014/10/13/planning-machine. Acesso em 28/10/2015.