# SURVEILLANCE E ESTADO-NAÇÃO: AS INADEQUADAS TENTATIVAS DE CONTROLAR OS FLUXOS DE DADOS ATRAVÉS DO MARCO CIVIL DA INTERNET E DA CPI DA ESPIONAGEM

## SURVEILLANCE AND NATION STATE: THE INABILITY TO CONTROL DATA FLOWS USING LAWS AND CONGRESSIONAL INVESTIGATIONS

Jose Luis Bolzan de Morais[1]
Elias Jacob de Menezes Neto[2]

**RESUMO**: Este artigo abordará o problema da surveillance e dos fluxos globais de dados. A partir de uma análise bibliográfica da matriz teórica da surveillance studies, irá defender a necessidade de construção teórica da surveillance que, embora já exista na sociologia mundial, ainda não encontrou lugar no cenário jurídico brasileiro. Uma tal teoria deve explicar por quais motivos a surveillance (pós-moderna) não pode ser comparada à vigilância (no sentido tradicional, ou seja, moderna). Em seguida, demonstrará que mudanças na tecnologia causaram modificações no conceito de privacidade, especialmente em virtude da utilização dos metadados e das técnicas de big data. Partindo dos exemplos do marco civil brasileiro da Internet e da CPI da espionagem do Senado Federal, criticará o recebimento equivocado do tema pelo mundo jurídico. Ao tentar controlar fluxos de dados com mecanismos vinculados à ideia de territorialidade estatal, o direito diminui o seu papel na proteção dos direitos fundamentais. Por fim, concluirá que são necessários novos mecanismos jurídicos capazes de lidar com os fluxos globais de dados no contexto das transformações do Estado e da dissolução da sua soberania na modernidade líquida.
**Palavras-chave**: Surveillance; Lei 12.965/2014; CPI da espionagem; Teoria do Estado.

**ABSTRACT**: This paper will analyse the problem of surveillance and global data flows. At first, it will review some bibliography from surveillance studies sociology to explain why we must develop such approach inside the Brazilian legal theory. Such a theory must initially explain how surveillance (post-modern, linked to the concept of liquid modernity) couldn't be compared to simple cloak and dagger surveillance (in the traditional sense, associated with the modern structures of visibility). Through the use of metadata and big data techniques, information technology changed the nature of privacy. These ideas will be linked with two Brazilian events – the recently passed bill to control Internet (Marco Civil) and the investigation by a Senate committee following Edward Snowden scandals involving NSA mass surveillance (CPI da espionagem) – to criticise the common approach of legal scholars to deal with surveillance-related problems. Traditional legal mechanisms are tied to

[1] Bacharel em Direito (UFSM). Mestre em Direito (PUC-RIO). Doutor em Direito (UFSC). Bolsista de Produtividade em Pesquisa do CNPq – Nível 1D. Professor do Programa de Pós-Graduação em Direito da UNISINOS – Mestrado e Doutorado. Procurador do Estado do Rio Grande do Sul. E-mail: bolzan@hotmail.com

[2] Bacharel em Direito (UFRN). Mestre em Direito (UNISINOS). Doutorando em Direito (UNISINOS). Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES. Advogado. Lattes: http://www.eliasjacob.com.br/lattes . E-mail: contato@eliasjacob.com.br

the territorial limit of nation states thus they aren't able to properly solve problems that are intrinsically deterritorialised. It will conclude that legal theory will loose its capacity do protect human rights if legal scholars refuse to engage in new ways to deal with global data flows, especially by taking into account transformations of Nation state's sovereignty in the liquid modernity.
**Keywords**: Surveillance; Law 12.965/2014; Congressional investigations; Theory of the State.

## INTRODUÇÃO

O marco civil brasileiro da Internet tem sido festejado por diversos setores da sociedade, sendo comumente considerado uma "constituição da Internet". O objetivo da Lei 12.965/2014 é disciplinar o uso da Internet no Brasil, assegurando a proteção de diversos direitos fundamentais, inclusive, para fins deste texto, a proteção contra violação dos fluxos de dados e das comunicações privadas armazenadas (art. 7º, incisos II e III). Dessa maneira, pretende garantir a preservação da intimidade e da privacidade, uma vez que esse conteúdo somente poderá ser acessado por ordem judicial. Será mesmo?!

Pouco antes da promulgação do marco civil, Edward Snowden, um analista de segurança que trabalhava para uma empresa contratada pela NSA – *National Security Agency* –, trouxe ao conhecimento geral a existência de alguns sistemas de monitoramento telemático: *PRISM*, *Upstream* e *XKeyscore*, entre outros[5]. Esses sistemas revelaram uma capacidade gigantesca dos órgãos de inteligência dos EUA – e, via cooperação, de outros países – para interceptar, armazenar e catalogar quase que todo o tráfego mundial da Internet, além de todos os dados armazenados em servidores das gigantes empresas de tecnologia da informação (TI). Diversos outros sistemas foram revelados posteriormente. E todos eles possuem um traço comum: ignoram a diferença entre público e privado, nacional e internacional. Assim, eles dissolvem as tradicionais fronteiras, os conceitos e os mecanismos manejados pelo aparato jurídico derivado do Estado-nação, como é o caso do marco civil da Internet no Brasil.

Como resposta a esses eventos, o Senado liberou o relatório final da "CPI da espionagem" (BRASIL, 2014). O próprio nome da CPI expressa a posição adotada em relação às informações divulgadas por Edward Snowden. Apesar dos eventuais avanços – toda pesquisa sobre o uso da SIGINT (signals intelligence) parece ser válida, especialmente se

[5] Os detalhes desses programas estão sendo amplamente divulgados pelos meios de comunicação de massas e pela Internet. Por todos, remete-se ao dossiê realizado pelo jornal "*The Guardian*", uma das fontes originalmente contatadas por Snowden para divulgar os detalhes dos projetos: < http://www.guardian.co.uk/world/edward-snowden>.

considerarmos que pouco se fala sobre o assunto –, será demonstrado que o relatório da CPI é extremamente míope em relação à compreensão do fenômeno que quer discutir e às soluções elencadas para os problemas.

Para aqueles pouco afeitos ao tema, poderia parecer a concretização do cenário distópico imaginado por George Orwell, na obra 1984. No entanto, a utilização das comunicações privadas armazenadas – e, por óbvio, de todos os dados que circulam pelo mundo virtual, inclusive os dados sobre os dados (metadados)[6] – está longe de ser do interesse apenas dos governos, pois constituem o maior trunfo de gigantes empresas de tecnologia – como *Apple*, *Google*, *Facebook*, *Amazon*, *Microsoft*, *WalMart*, dentre outros. Trata-se, assim, de uma mudança no próprio conceito de privacidade, afinal, o uso de metadados permite a violação desse direito fundamental sem transgredir, nos termos do marco civil, as comunicações privadas armazenadas.

No século XXI, tudo é passível de ser transformado em dados analisáveis, inclusive os próprios dados. Como resultado, o acesso ao fluxo de dados e a qualquer tipo de informação armazenada é muito mais do que um problema de privacidade. Passa a ser um problema de violação da igualdade.

A sistemática coleta e processamento dos fluxos de informação possibilita a classificação pouco – ou nada – democrática das pessoas em categorias sociais de seu interesse. Com base na análise das informações de uma troca de e-mails[7], por exemplo, é

---

[6] Para clarificar um pouco, metadados são informações a respeito de outras informações. De modo grosseiro, é possível utilizar a metáfora de uma carta ordinária. Assim, enquanto os dados seriam o conteúdo da correspondência – e, portanto, protegidos contra violação –, os metadados seriam informações sobre aquela carta: tipo do papel utilizado, tamanho do envelope, dados do remetente e destinatário, data e local de postagem, traços de DNA e impressões digital encontrados na carta, tipo e cor da tinta utilizada para escrever a carta, tamanho da correspondência, número de letras e palavras, peso da carta, traços de substâncias impregnadas no papel, informações sobre quaisquer outras correspondências similares no sistema postal, nome do carteiro que fez a entrega etc.

[7] Ressalte-se, aqui, a importância da análise dos metadados. Com uma abordagem estatística adequada, informações como remetente, destinatário, assunto, horário de envio e endereço IP podem ser tão ou mais valiosas que o conteúdo dos e-mails. Simplificando: imagine que um determinado sistema coleta, durante alguns meses, informações sobre todos os contatos realizados – não o conteudo das comunicações – por um indivíduo – frequencia, duração, destinatário, horário –, além de todas as suas movimentações no espaço – com rotas percorridas, velocidade, etc. Qualquer pessoa poderia extrair conclusões interessantes desses dados: quem são as pessoas importantes para esse indivíduo? Quais os meios de transporte que ele utiliza? Qual a sua profissão provável? Afinal, se todos os dias às 03:00 da madrugada ele está no hospital, possivelmente é um profissional da saúde. Se isso ocorre apenas excepcionalmente, provavelmente está doente. Obviamente, um sistema pode tirar conclusões muito mais avançadas com esses dados no atacado: esse indivíduo chama-se João, é médico, número de CPF tal, possui uma esposa e quatro filhos, dirige um veículo de marca tal e, por isso, tem 85% de probabilidade de votar no partido X, possui os traços de personalidade Y, Z, K e, portanto, tem um risco de 75% de desenvolver demência na velhice. A concatenação de dados é quase infinita e pode parecer absurda, mas é

possível – sem sequer ter acesso ao conteúdo da mensagem – classificar indivíduos em grupos específicos, classificações estas que possuem consequências significativas para suas vidas.

A categorização dos seres humanos tem como finalidade a sua inclusão ou exclusão em determinados grupos. E, com isso, uma nova categoria entra em cena, a *surveillance,* a qual levanta barreiras virtuais, capazes, assim, de garantir ou impedir o acesso aos elementos indispensáveis para uma vida digna, como, por outro lado, permitir novas formas de gestão e controle de pessoas, empresas, governos etc. E os critérios para a obtenção e uso dessas classificações, ressalte-se, não se submetem aos tradicionais controles e limites democrático-territoriais, sendo geridos, tratados e utilizados a partir da ideia de segredo: seja de Estado, seja comercial, visto que tais informações e as análises que delas derivam são consideradas propriedade da empresa que as obtêm e oferece o serviço.

É por isso que, conforme será visto, não é possível falar apenas de "vigilância", como parece ser a tentação em muitos setores. A mera tradução da palavra *surveillance* como "vigilância" é inadequada para englobar um fenômeno tão complexo, afinal, não se está falando de um evento específico dirigido contra um sujeito determinado (como é o caso da vigilância), mas de uma característica da vida neste mundo globalizado e interconectado.

Com base nisso, o objetivo deste trabalho é questionar, a partir da distinção entre vigilância e *surveillance*, qual o papel do Estado-nação na proteção dos direitos fundamentais violados a partir do acesso à informações privadas armazenadas. Será mesmo que, como intenta o Estado brasileiro através do marco civil da Internet e da CPI da espionagem, o recurso à lei regulamentadora – instrumento tipicamente vinculado à ideia de territorialidade – é capaz de controlar os fluxos globais de dados? Qual o impacto do marco civil brasileiro no acesso indiscriminado de comunicações privadas por parte de empresas transacionais e entidades de inteligência em servidores localizados do outro lado do planeta?

Essas perguntas são puramente retóricas. O marco civil brasileiro, por óbvio, trouxe diversos avanços – veja-se, por exemplo, a ideia de neutralidade da rede. No entanto, conforme será ressaltado, é ingênuo acreditar que as comunicações pessoais armazenadas passaram a estar protegidas em virtude da promulgação de uma lei no Brasil. Igualmente ingênuo é acreditar – como quer o relatório da CPI da espionagem – que a elaboração de uma nova lei seria capaz de evitar a interferência nos fluxos de dados mundiais. A proteção dos

---

utilizada diariamente no mundo do *Big Data* para determinar riscos, preferências e hábitos das pessoas. A sofisticação desses sistema (vide infra, KOSINSKI *et al*, 2013) parece retirada de filmes de ficção científica.

direitos fundamentais é essencial para proteger os direitos fundamentais das pessoas, mas, sem entender o fenômeno da *surveillance*, nada estará protegido. É como se o direito tentasse obter respostas sem sequer saber fazer as perguntas corretas.

## 2 O QUE É ISTO, A SURVEILLANCE?

Os estudiosos, diz Saskia Sassen (1996), encontram enormes dificuldades para analisar mudanças significativas que lhes sejam contemporâneas. Os câmbios paradigmáticos frequentemente não podem ser "capturados" por eles, uma vez que estão tanto imersos no paradigma antigo quanto confrontados com o ineditismo do novo. Os vocabulários, categorias e modelos disponíveis nessa situação-limite são incapazes de responder suficiente e eficazmente às mudanças fundamentais que causam perplexidade ao pesquisador.

Esse é exatamente o caso que enfrentamos aqui. Por esse motivo, mostra-se essencial explicar a escolha da palavra "*surveillance*" para conceituar um fenômeno que, cotidianamente, tem sido simplesmente traduzido como "vigilância", muito provavelmente na esteira da versão para o português do livro de Michel Foucault – "Vigiar e Punir".

Embora a tradução literal – vigilância – seja linguisticamente adequada, a palavra em língua inglesa – bem como na francesa – possui uma polissemia que não é alcançada pelo termo em português[8]. Isso fica nítido quando os teóricos dos estudos sobre a surveillance fazem a distinção entre "*surveillance*" e "*new surveillance*", respectivamente associadas à modernidade tradicional e à modernidade líquida.

A maturidade do debate no exterior, contudo, permite que os autores anglófonos ressignifiquem a palavra em inglês. Como a carga semântica do vocábulo "vigilância" é demasiadamente forte no Brasil – por vários motivos, inclusive por estar muito mais ligada, etimologicamente, à palavra "*vigilance*" (inglês e francês) –, na ausência de tradução que compartilhe o mesmo sentido, preferimos utilizar o termo diretamente do inglês. Isso não

[8] Aqui vale o alerta de Arthur Schopenhauer. Para o filósofo alemão, "às vezes ocorre também que uma língua estrangeira expresse um conceito com uma sutileza que a nossa própria língua não lhe dá, de modo que o pensamos apenas naquela língua com tal sutileza. Com isso, cada pessoa que busca uma expressão exata de seu pensamento usará a palavra estrangeira, sem se importar com a algazarra dos puristas pedantes. Em todos esses casos, não é exatamente o mesmo conceito que determinada palavra de uma língua designa, em comparação com outra língua, e o dicionário oferece diversas expressões aparentadas que se aproximam do significado, só que não de modo concêntrico, mas em várias direções como na figura precedente, estabelecendo assim as fronteiras entre as quais esse significado se encontra." (SCHOPENHAUER, 2009, p. 149-150).

significa que vigilância e *surveillance* estejam completamente dissociadas, mas que a *surveillance* expressa um fenômeno diferente que pode ou não ter componentes de vigilância.

Com o propósito de fazer uma diferenciação dessa "*new surveillance*", Gary T. Marx (2002) critica a definição dicionarizada – no dicionário: uma observação próxima, especialmente de um indivíduo suspeito. Para o referido autor, o uso de novas tecnologias transforma a *surveillance*, uma vez que tais tecnologias não necessitam da proximidade física, tampouco envolvem apenas indivíduos suspeitos de alguma prática ilícita. Além disso, uma definição tradicional de "vigilância" exige polos definidos de função, uma vez que divide os indivíduos em "observador" e "observado", delimitação bem mais difícil quando tratamos de bancos de dados difusos, análises de padrões de dados, uso de redes sociais etc.

Assim, esse novo conceito de *surveillance* pode ser caracterizado, especialmente, pelo uso de "sentidos estendidos", ou seja, pela utilização de meios técnicos capazes de extrair ou criar informações pessoais. Tais informações não são apenas "sobre indivíduos", dado que também levam em conta o contexto da sua coleta, o que permite afirmar que boa parte da surveillance está ligada ao reconhecimento de padrões relacionais do indivíduo com outros e com o espaço. Dessa maneira, "o significado pode residir na classificação cruzada de distintas fontes de dados (como ocorre com combinação e análise de perfis) que, neles mesmos, podem não ser reveladores. Os sistemas, assim como as pessoas, são de interesse. (MARX, 2002, p. 12, tradução nossa)[9].

De maneira similar, tanto David Lyon (1994, p. 40) fala de uma "new dimension of surveillance", quanto Colin Bennet *et al* (2014, p. 183, tradução nossa) afirmam que "[...] devemos rotular como '*surveillance*' muitas outras práticas além das escutas telefônicas ou da busca por suspeitos da polícia"[10].

Assim, um dos processos-chave para caracterizar a *surveillance* é o atual uso de bancos de dados indexáveis no processamento de informações para diversas finalidades. Entende-se, portanto, que as novas infraestruturas da tecnologia da informação, ao permitirem o processamento em tempo real e o armazenamento ilimitado de dados, não apenas "qualificam" a vigilância, mas introduzem mudanças qualitativas que permitem um "salto"

---

[9] No original: "Meaning may reside in cross classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing. Systems as well as persons are of interest.".

[10] No original: "[...] we must label as 'surveillance' many more practices than just wiretapping or the trailing of suspects by police.".

em direção ao conceito de *surveillance*[11]. Assim, "os computadores, em conjunto com as técnicas avançadas de estatística, ajudam a inaugurar uma nova dimensão da 'surveillance'"[12] (LYON, 1994, p. 40, tradução nossa).

A *surveillance*, muito além de uma "vigilância", é uma das grandes marcas das sociedades contemporâneas e depende intrinsicamente do uso dos bancos de dados pessoais. Dependemos dela para nos movermos pelo mundo cotidiano. Logo, "[...] a surveillance discutida aqui não envolve, usualmente, pessoas de verdade olhando umas às outras. Ao invés disso, busca fragmentos factuais abstraídos dos indivíduos" (LYON, 2001, p. 2, tradução nossa)[13].

Nesse sentido, é possível demonstrar algumas características da "*new surveillance*" capazes de diferenciá-la das formas tradicionais de controle social. Trata-se não apenas de uma "versão eletrônica da vigilância", mas de um fenômeno qualitativamente novo e que possui os seguintes diferenciais:

> Ela transcende a distância, a escuridão e as barreiras físicas. Transcende o tempo, o que pode ser visto, especificamente, na capacidade de armazenamento e recuperação que possuem os computadores; informações pessoais podem ser 'congeladas', para usar a expressão de Goodwin e Humphey. Ela é de baixa visibilidade ou invisível; os indivíduos cujos dados são coletados possuem cada vez menos ciência disso. Ela é frequentemente involuntária, como notamos anteriormente. A prevenção é a sua maior preocupação; pense nas bibliotecas com livros com código de barras ou nos shopping centers com câmeras de segurança que estão lá para prevenir a perda, não para ensinar que roubar é imoral. Ela [a surveillance] faz uso intensivo de capital, não do trabalho, o que faz com que seja economicamente mais atrativa. Ela envolve políticas descentralizadas de autocontrole; mais uma vez, notamos como participamos no nosso próprio monitoramento. Isso leva a uma mudança da identificação específica de indivíduos em direção a uma suspeita de categorias. Ela é, simultaneamente, mais intensiva e mais extensiva. Utilizando a metáfora de Stanley Cohen, a rede é mais fina, mais maleável e mais ampla (LYON, 1994, p. 53, tradução nossa)[14]

---

[11] De maneira similar, ver a justificativa de Manuel Castells (2010, p. 304) para considerar a globalização atual como um fenômeno novo, distinto dos eventos associados à expansão do capitalismo no final do século XIX.

[12] No original: "[...] computers in tandem with advanced statistical techniques help inaugurate a new dimension of surveillance.".

[13] No original: "The surveillance discussed here does not usually involve embodied persons watching each other. Rather, it seeks out factual fragments abstracted from individuals.".

[14] No original: "It transcends distance, darkness and physical barriers. It transcends time, and this can be seen especially in the storage and retrieval capacity of computers; personal information can be 'freeze-dried', to use Goodwin and Humphreys' term. It is of low visibility or invisible; data-subjects are decreasingly aware of it [...]. It is frequently involuntary, as we noted above. Prevention is a major concern; think of bar-coded library books or shopping mall video cameras, which are there to prevent loss, not to teach the immorality, of theft. It is capital – rather than labour – intensive, which makes it more and more economically attractive. It involves decentralized self-policing; again, we noted above how we participate in our own monitoring. It triggers a shift from

Isso não significa, contudo, que o aspecto tecnológico seja o mais importante na análise do fenômeno. Ele não está "descolado" das realidades social, econômica e política. A tecnologia, antes de causa, é instrumento para coletar, armazenar, processar, classificar e transmitir informações. Ao invés de ser um aspecto externo – como nos remete à ideia de "vigilância" –, a tecnologia é parte da textura que compõe a vida nas sociedades contemporâneas.

Assim, o que se busca é diferenciar a vigilância no sentido tradicional – ou seja, como espionagem, controle e investigação sigilosa de atividades individuais – das técnicas facilitadas pela tecnologia da informação que, por sua natureza, são endêmicas nas sociedades contemporâneas. Tais técnicas têm como objetivo a sistemática coleta, armazenamento, processamento, individualização e classificação das informações sobre as pessoas em determinados grupos. Logo, o elemento "líquido" (BAUMAN; LYON, 2012), e, por consequência, de difícil controle que caracteriza o fluxo de dados por sistemas de computadores é um traço essencial do que se quer, aqui, denominar *surveillance*.

A seguinte tabela, trazida por Gary T. Marx (2002, p. 28-29), serve bem para diferenciar a "*traditional surveillance*" (cuja equivalente, no Brasil, é a vigilância) da "*new surveillance*" (que, neste texto, identificamos apenas como "*surveillance*"). A partir dela, é possível verificar algumas dimensões utilizadas como critério para distinguir esses fenômenos.

| **DIMENSON** | **A. Traditional Surveillance** | **B. The New Surveillance** |
|---|---|---|
| Senses | Unaided senses | Extends senses |
| Visibility (of the actual collection, who does it, where, on whose behalf) | Visible | Less visible or invisible |
| Consent | Lower proportion involuntary | Higher proportion involuntary |
| Cost (per unit of data) | Expensive | Inexpensive |
| Location of data collectors / analyzers | On scene | Remote |
| Ethos | Harder (more coercive) | Softer (less coercive) |

identifying specific suspects to categorical suspicion. It is both more intensive and more extensive. In Stanley Cohen's metaphor, the net is finer, more pliable, and wider.".

| | | |
|---|---|---|
| Integration | Data collection as separate activity | Data collection folded into routine activity |
| Data collector | Human, animal | Machine (wholly or partly automated) |
| Data resides | With the collector, stays local | With 3rd parties, often migrates |
| Timing period | Single point or intermittent | Continuous (omnipresent) |
| Time period | Present | Past, present, future |
| Data availability | Frequent time lags | Real time availability |
| Availability of technology | Disproportionately available to elites | More democratized, some forms widely available |
| Object of data collection | Individual | Individual, categories of interest |
| Comprehensiveness | Single measure | Multiple measures |
| Context | Contextual | Acontextual |
| Depth | Less intensive | More intensive |
| Breadth | Less extensive | More extensive |
| Ratio of self to surveillant knowledge | Higher (what the surveillant knows, the subject probably knows as well) | Lower (surveillant knows things the subject doesn't |
| Identifiability of object of surveillance | Emphasis on known individuals | Emphasis also on anonymous individuals, masses |
| Emphasis on | Individuals | Individual, networks systems |
| Form | Single media (likely or narrative or numerical) | Multiple media (including video and/or audio) |
| Who collects data | Specialists | Specialists, role dispersal, self-monitoring |
| Data analysis | More difficult to organize store, retrieve, analyze | Easier to organize, store, retrieve, analyze |
| Data merging | Discrete non-combinable data (whether because of different format or location) | Easy to combine visual, auditory, text, numerical data |
| Data communication | More difficult to send, receive | Easier to send, receive |

Em virtude dessas diferenças, o desenvolvimento tecnológico proporciona o aparecimento de novos instrumentos de violação de direitos fundamentais capazes de atuar em duas frentes: por um lado, através da identificação, rastreamento, monitoramento e análise de informações relativas aos detalhes da vida íntima e da identidade das pessoas; por outro, em razão das práticas de coleta, armazenamento, processamento, individualização e classificação das pessoas em determinados grupos. Como resultado, tais práticas modificam as relações de visibilidade/opacidade, que não devem ser compreendidas apenas como um atributo físico do sentido humano – o olhar –, mas, de maneira mais abrangente, como a

ampla disponibilidade de informações personalizadas e compiláveis sobre indivíduos e grupos.

A coleta, armazenamento e processamento automatizado de diversas informações sobre os indivíduos e grupos – transações financeiras, ligações telefônicas, preferências de consumo, hábitos de uso da Internet etc. – permite, além da territorialidade, transcender também a temporalidade, uma vez que, embora estejam relacionadas ao presente, as novas técnicas de *surveillance* empregam o armazenamento quase ilimitado de informações – passado – e o seu uso por ferramentas de análise estatística e de predições de risco – futuro.

Atualmente, um dos objetivos primordiais da *surveillance* é a previsão de comportamentos futuros, seja por parte do poder público – prever atitudes terroristas, por exemplo[15] –, seja pela iniciativa privada – para prever quais as melhores formas de ganhar dinheiro com anúncios, exemplificativamente[16]. O homem é um animal de hábitos, de maneira que, com a coleta de informações diversas durante período de tempo suficiente, é possível prever padrões de comportamento, deslocamento, preferências e interação social.

Não apenas nossas comunicações privadas, mas nossos "*alter egos virtuais*", ou *data doubles* – conceito sintetizado por David Lyon (2007, p. 22, tradução nossa) como "[...] as várias concatenações de dados pessoais que, queira ou não, representam 'você' dentro da burocracia ou da rede"[18] –, circulam livremente pelas redes de computadores e, embora sejam cada vez mais alimentados por nós mesmos e tenham cada vez mais efeitos concretos nas nossas vidas, temos paulatinamente menos controle sobre os dados que são coletados e sobre as formas como eles são manipulados.

A descentralização das informações – paradoxalmente, protagonizada pela convergência das tecnologias – permite que a capacidade da *surveillance* seja aumentada exponencialmente. Isso requer novas formas de entender esse fenômeno, o que culmina na

---

[15] Nesse sentido, veja-se o FAST (*Future Attribute Screening Technology*) desenvolvido pelo *Department of Homeland Security* dos EUA. Esse sistema pretende, através da análise de atributos físicos dos indivíduos – movimentos corporais, mudanças na entonação e ritmo da fala, movimento dos olhos, alterações na temperatura corporal e frequência respiratória – prever quem é "potencialmente perigoso". Para maiores detalhes: <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf> e <http://epic.org/privacy/body_scanners/EPIC-DHS-FOIA-09-14-11.pdf>

[16] Basta ver, por exemplo, como funciona o mecanismo de sugestões de compras de grandes sites varejistas como a *Amazon*. Ao processar o histórico de compras dos usuários, cliques nas opções "curtir" das redes sociais e itens adicionados às "listas de desejos", a empresa cruza esses dados com aqueles de outros usuários e elabora listas de sugestões incrivelmente precisas sobre produtos que irão despertar o interesse do consumidor.

[18] No original: "[...] various concatenations of personal data that, like it or not, represent 'you' within the bureaucracy or the network.".

necessidade de desenvolver o conceito de *surveillance*, já não mais reduzido às características da modernidade – de maneira ampla, associadas às limitações espaço-temporais e às relações de visibilidade–, mas aos traços líquidos e incertos do mundo contemporâneo, ou seja, ignorando fronteiras físicas, teóricas e técnicas, bem como as distinções entre público e privado ou nacional e internacional.

Mostra-se claro, assim, que *surveillance* significa muito mais do que vigiar a vida de alguém ou grampear telefones. Trata-se de uma prática organizacional (BENNET *et al*, p. 6) que possui como resultado a categorização de pessoas em grupos diferentes com o intuito de tratá-los diferentemente. Da Receita Federal brasileira até o *Google*, passando pela *NSA*, *Amazon*, dentre outras, a classificação de pessoas em categorias é uma das características essenciais da *surveillance*.

Assim, muito além da privacidade, a questão fundamental da *surveillance* é "como – e com base em quais critérios – somos categorizados?". Embora nenhum instrumento jurídico estatal possa fornecer respostas para essa pergunta, a ausência de qualquer proteção no marco civil brasileiro da Internet é o símbolo do atraso do direito em relação à emergência de problemas reais que violam os direitos fundamentais.

## 3 MUDANÇAS NA PRIVACIDADE E AS INSUFICIÊNCIAS DO MARCO CIVIL DA INTERNET NA ERA DA GLOBALIZAÇÃO

### 3.1 – MUDANÇAS DA PRIVACIDADE NA ERA DIGITAL

Como mencionado anteriormente, a utilização de metadados causou uma mudança importante do significado da privacidade. Isso transformou o conceito daquilo que é "informação privada" para muito além das simples "comunicações privadas armazenadas". No mundo atual, somos identificados por processos técnicos de alta complexidade e que são, em grande parte, de baixa visibilidade e *accountability* (BENNET *et al*, p. 74). Os metadados, embora escapem do conceito legal de "comunicação privada armazenada", podem dizer muito mais sobre a vida privada de um indivíduo do que o conteúdo de e-mails, por exemplo.

A coleta, armazenamento, análise e processamento desses metadados permite identificar e fazer inferências sobre os mais íntimos segredos do ser humano. Alguns exemplos desse tipo especial de informação são: endereços IP (*Internet protocol*); números MAC (*media access control*); ESN (*electronic serial number*); SPIN (*service provider*

*identification number*), IMEI (*international mobile equipment identity*), EMSI (*international mobile subscriber identity*); *cookies* com dados de pesquisas em mecanismos de busca; informações de posicionamento por satélite transmitidas para fabricantes de *smartphones* ou *tablets* e inseridas automaticamente como metadados nas fotografias feitas nesses dispositivos; informações de localização das torres de transmissão próximas de terminais móveis de telefone e Internet; origem, destinatário e hora de telefonemas, envio de mensagens e e-mails etc.

Essa lista – incompleta – é apenas um indicativo da quantidade de informações não protegidas pelo conceito de "comunicações pessoais armazenadas" que podem ser utilizadas para associar qualquer indivíduo a um ponto específico no espaço e no tempo. Além disso, permitem estabelecer sua rede de contatos e relacionamentos. Nesse sentido, Bennet *et al* (2014, p. 74, tradução nossa) afirmam que "se você sabe e combina um número suficiente de informações online e offline, você talvez tenha dados suficientes para fazer um palpite muito provável (as vezes quase perfeito) sobre quem estava fazendo o que, quando e onde"[19].

Além disso, os hábitos de navegação e interação de todos, por exemplo, são utilizados pelas grandes empresas de publicidade *online* – como o *Google* e o *Facebook* – para direcionar anúncios "relevantes". Atualmente, grande parte da nossa vida real (lazer, trabalho, educação) tem componentes do ambiente virtual – basta imaginar, por exemplo, uma viagem ao exterior sem uma consulta no *Google*. O uso de redes sociais aumenta ainda mais esse vínculo entre "real" e "virtual". Nenhuma dessas informações, aparentemente, está enquadrada no conceito de "comunicação privada armazenada", o que significa que são menos protegidas, ainda que sejam tão ou mais reveladoras que o tipo de informação referida pelo marco civil da Internet.

Se a finalidade dessa legislação é proteger a privacidade dos indivíduos, é possível afirmar, desde logo, categoricamente que ela falhou em seu objetivo, como será visto.

### 3.2 – AS INSUFICIÊNCIAS DO MARCO CIVIL DA INTERNET NA ERA DA GLOBALIZAÇÃO

Considerando todos esses elementos que compõem o quadro de mudanças da privacidade na era digital, é possível dizer que o marco civil da Internet fracassou. O artigo

[19] No original: "if you knew and combined enough online and offline information, you might have enough data to make a highly probable (sometimes almost perfect) guess about who was doing what, when, and where.".

7º, no conjunto dos seus incisos, é um exemplo claro do que tentamos demonstrar neste trabalho. Isso porque dá início ao capítulo que justamente trata dos direitos e garantias do usuários, mas restringe esses direitos à privacidade. O marco civil da Internet, ao proteger a vida privada (inciso I), o sigilo do fluxo das comunicações (II) e, especialmente, o sigilo das comunicações privadas armazenadas (III) não entendeu que existem outros direitos fundamentais violados pela *surveillance*.

Isso não significa dizer que a proteção da privacidade não seja importante. Entretanto, a partir dos aportes teóricos já referidos, objetiva-se deixar claro, fundamentalmente, dois aspectos: primeiro, a forma reducionista como vem sendo tratada a questão da privacidade, apenas como sinônimo de vida particular, ou seja, de intromissão nas comunicações privadas armazenadas (vide inciso III); segundo, os problemas oriundos da modernidade líquida não são resolvidos a partir de soluções dependentes da territorialidade, como é o caso do marco civil.

Sobre a modernidade líquida, Zygmunt Bauman (2001, p. 8) justifica a metáfora da fluidez como a mais adequada para o mundo atual, pois, distintamente dos sólidos, os líquidos "[...] não mantêm sua forma com facilidade [...] não fixam o espaço nem prendem o tempo [...] não se atêm muito a qualquer forma e estão constantemente prontos (e propensos) a mudá-la [...] o que conta é o tempo, mais do que o espaço que lhes toca ocupar".

Essa habilidade para suprimir o tempo e ignorar com facilidade o espaço é um traço fundamental daquilo que Bauman chama de modernidade líquida. A tecnologia da informação, muito além de mera ferramenta facilitadora dessa liquidez, é uma das suas *clé de voute*.

Com efeito, merece atenção a análise de Saskia Sassen (2006) a respeito das "*assemblages*" na era global digital e os reflexos das tecnologias da informação no Estado. A autora, embora reconheça as transformações de paradigma que envolvem as novas dinâmicas institucionais da globalização, não trabalha com a perspectiva comum de "vitimização" do Estado, uma vez que ele continua sendo o lugar privilegiado de formação jurídico-institucional. Isso não significa o fim do Estado, mas ressalta a importante imbricação entre a pluralidade de instituições globais desnacionalizadas e o próprio Estado, uma vez que aquelas instituições, geralmente, somente são operacionalizadas quando adentram na estrutura estatal. Nesse sentido, Saskia Sassen (2006, p. 8, tradução nossa) afirma que

> [...] as maiores transições que iniciam os novos arranjos [...] podem depender das múltiplas capacidades da ordem anterior. Essa 'dependência' não é necessariamente

> fácil de reconhecer, uma vez que as novas lógicas organizacionais podem e irão tender a alterar a valência de uma determinada capacidade [...] algumas das antigas capacidades são essenciais para a constituição crítica da nova ordem, mas isso não significa que suas valências sejam as mesmas; os sistemas relacionais ou as lógicas organizacionais dentro das quais elas adquirem funcionalidade podem ser radicalmente diferentes. O ponto crítico é a intermediação que as capacidades produzem entre a nova ordem e a antiga; enquanto elas mudam de caminho, tornam-se partes constitutivas e, simultaneamente, podem disfarçar essa mudança vestindo as mesmas roupas de sempre.[20]

Quando se fala nas tecnologias da informação e o seu impacto nas estruturas estatais, um dos pontos centrais é o questionamento a respeito da capacidade regulatória que os modelos de Estado e democracia vigentes possuem sobre essas tecnologias. Elas desestabilizam as estruturas hierárquicas formais, pois estas passam a ser substituídas por novas estruturas ainda não formalizadas, frequentemente apropriadas por poderes privados e imunes aos influxos democráticos.

Do ponto de vista da *surveillance*, isso significa que, embora essas práticas escapem frequentemente da regulação estatal – especialmente quando envolvem a iniciativa privada ou os segredos de Estado –, não estão imunes ao controle, mas, muito pelo contrário, submetem-se à regulamentação dos detentores das tecnologias – ainda que sejam Estados, como no caso dos EUA. Tal situação é problemática, uma vez que impossibilita a análise pública da *surveillance* até mesmo quando ela é utilizada pelo Estado, como, repita-se, ficou claro com as notícias envolvendo Edward Snowden.

Sob essa perspectiva de fluidez e desterritorialização dos fluxos de dados e dos servidores que guardam comunicações privadas, o marco civil da Internet, embora seja um avanço em diversos aspectos, pouco pode fazer[21].

---

[20] No original: [...] major transitions ushering novel arrangements [...] might depend on multiple capabilities of the older order. This "dependence" is not necessarily easy to recognize, as the new organizing logic can and will tend to alter the valence of a given capability [...] some of the old capabilities are critical in the constituting of the new order, but that does not mean that their valence is the same; the relational systems or organizing logics within which they then come to function may be radically different. The critical issue is the intermediation that capabilities produce between the old and the new orders: as they jump tracks they are in part constitutive and at the same time can veil the switch by wearing some of the same old clothes.".

[21] Vale lembrar que, mesmo se tivesse sido aprovada a proposta, que constava no projeto inicial, de obrigar que empresas possuissem servidores em território nacional, de nada adiantaria. Afinal, é próprio da computação na nuvem a existência de múltiplos níveis de redundância. Logo, não existe, por exemplo, somente "um servidor da empresa X, localizado no endereço Y", mas uma infinidade de equipamentos espalhados em diversos pontos do globo. Mesmo, hipoteticamente, com um servidor do *Google* no Brasil, ainda existiriam outras centenas deles em lugares completamente diversos do globo terrestre. Fica difícil, portanto, determinar "onde" está a informação: ela é ubíqua.

Certamente, alguma proteção é melhor que nenhuma, de maneira que há possibilidade de (pouca) efetividade dos trechos da legislação em questão. No entanto, seria ingênuo – embora essa espécie de pensamento seja extremamente comum no imaginário jurídico – acreditar que esse tipo de solução sólida (dispositivo legal) tem condições para lidar com a liquidez da *surveillance*.

Veja-se, por exemplo, que os termos de serviço do *Google* preveem o acesso pela gigante de *Mountain View* a todas as mensagens e conversas dos usuários dos seus serviços de e-mail e bate papo[22]. Se até mesmo os termos de serviço do *Google* – uma empresa com representação no Brasil que provê serviços a milhões de brasileiros, empresas e órgãos da administração pública e que, portanto, está totalmente enquadrada nos critérios do marco civil – "valem mais" que o disposto no art. 7º, inciso III da lei 12.965/2014[23], por qual motivo deveríamos acreditar que essa legislação será respeitada por outras empresas[24] com muito menos vínculos no Brasil ou por agências de inteligência?

Sem entrarmos no mérito de que a igualdade, direito fundamental essencial para sociedades democráticas atuais, foi esquecida pelo marco civil da Internet – embora seja muito mais afetada pelo crescimento da tecnologia da informação do que a privacidade –, pergunta-se: como podemos proteger a privacidade em pleno século XXI se confiamos somente em instrumentos feitos para lidar com problemas inaugurados no século XVI? É possível afirmar, mutatis mutandis, que o imaginário equivocado sobre os limites e possibilidades do marco civil da Internet sofre da mesma miopia da CPI da espionagem realizada pelo Senado Federal.

---

[22] "Nossos sistemas automatizados analisam o seu conteúdo (incluindo e-mails) para fornecer recursos de produtos pessoalmente relevantes para você, como resultados de pesquisa customizados, propagandas personalizadas e detecção de spam e malware. Essa análise ocorre à medida que o conteúdo é enviado e recebido, e quando ele é armazenado.". Para maiores detalhes: <http://www.google.co.uk/intl/pt-BR/policies/terms/regional.html>.

[23] Observe-se que, nos termos dessa mesma lei (art. 8º, inciso I), a referida cláusula do termo de serviço utilizado como exemplo deveria ser nula de pleno direito. E, mesmo assim, o *Google* continua (e, fatalmente, continuará) a analisar e-mails, bate papos e muito mais informações.

[24] Veja-se, também, o caso do *Facebook*. A rede social, alegam os meios de comunicação, analisa – através de sistemas automatizados – o conteúdo das mensagens privadas trocadas pelos seus usuários – grupo que, agora, engloba também aquelas trocadas pelo aplicativo *WhatsApp*, utilizado por milhões de brasileiros. Um dos "resultados" aparentemente positivos dessa prática seria a habilidade de relatar atividades potencialmente criminosas para as autoridades competentes. Veja-se, por exemplo, o fatídico dia em que "o Facebook capturou um pedófilo": <http://www.dailymail.co.uk/sciencetech/article-2173081/Right-wrong-Facebook-monitors-chat-conversations-informs-police-suspicious--privacy-breach-does-catch-paedophiles. html>.

## 3.3 – OS EQUÍVOCOS DA CPI DA ESPIONAGEM

O mesmo tipo de raciocínio equivocado sobre os efeitos da surveillance e a capacidade de regulamentação do Estado permeia o relatório final da CPI da espionagem realizada pelo Senado Federal como resposta aos eventos envolvendo Edward Snowden.

O relatório faz amplo uso da palavra "espionagem" para se referir ao seu objeto de estudo. No entanto, o problema deixou de ser mera "espionagem" ou "vigilância", ou seja, um evento específico e dirigido contra determinados sujeitos, passando a constituir uma das características inevitáveis das sociedades contemporâneas. Não apenas grandes potências militares, como os EUA, mas, especialmente, grandes grupos privados dedicam cada vez mais esforços no desenvolvimento de tecnologia para coleta, análise e processamento de informações.

A análise que permeia o texto da CPI engloba apenas a violação da privacidade como único resultado da utilização de técnicas de coleta e processamento massivo de dados Os perigos da coleta e processamento de dados vão muito além da vida privada individual. Para utilizar a expressão que ficou famosa no imaginário popular após as denúncias de Edward Snowden, pode até ser que o "Obama" não tenha interesse na vida pessoal dos indivíduos, mas só o fato de se imaginar que a surveillance se resume ao olhar de um presidente na vida pessoal de um cidadão já demonstra a ausência de compreensão adequada do fenômeno.

Existe, no relatório, uma mistura entre eventos pontuais de espionagem – como, por exemplo, a invasão de servidores da Petrobrás ou da Presidência da República – e eventos generalizados que de maneira alguma podem ser considerados "espionagem". A coleta massiva de metadados por entidades públicas e privadas para a elaboração de perfis (de uso, risco, preferências pessoais, compras etc.) não pode ser considerada espionagem por dois motivos principais: a) a coleta de dados não é individualizada, mas feita no atacado (salvo casos pontuais – esses sim de espionagem) e b) tais dados fazem parte da própria existência do ser humano nas sociedades contemporâneas.

No mundo atual há um deslocamento da ideia de "espionagem" para um conceito mais amplo de coleta e análise generalizada de quaisquer tipos de dados. Deixou-se de coletar informações específicas e passou-se a armazenar todos os tipos de informações que, individualmente, podem parecer irrelevantes, mas que, conjuntamente, são capazes de dizer muito sobre um determinado indivíduo ou grupo.

Logo, uma das características centrais dessa mudança é a prática da *data mining* pela iniciativa privada. Armazena-se indiscriminadamente todo o tipo de informação não processada com a finalidade de, posteriormente, aplicar algoritmos computacionais para extrair quaisquer conclusões que sejam relevantes. Assim funcionam, por exemplo, os mecanismos de marketing em sistemas de e-mails ou redes sociais: ao armazenarem todo o conteúdo das mensagens trocadas ou das interações realizadas, é possível classificar as preferencias dos usuários, tornando a publicidade cada vez mais direcionada e precisa. Em pesquisa recente (KOSINSKI *et al*, 2013), foi possível determinar com precisão de 95% os traços de personalidade de indivíduos somente através das informações que eles disponibilizam voluntariamente através do ícone "curtir" da rede social *Facebook*. Através do mesmo mecanismo, o Google pode cruzar todas as pesquisas feitas no seu sistema de busca com os dados oficiais sobre surtos de gripe e dengue – sistema conhecido como "*Google Trends Flu/Dengue*" (GINSBERG *et al*, 2009). Como resultado, a empresa de Mountain View é capaz de prever surtos daquelas doenças com precisão e antecedência muito maior que os órgãos governamentais de controle de doenças.

Desfaz-se, assim, a imagem de que o problema é apenas a existência de um "grande irmão" estadunidense que deseja espionar a vida de todos. Muito além disso, todos os movimentos dos indivíduos nas sociedades contemporâneas podem ser coletados, processados e analisados com a finalidade de extrair um sentido daquele conjunto aparentemente caótico de dados – transações eletrônicas, detalhes de chamadas telefônicas realizadas, e-mails enviados, interações em redes sociais, posicionamento no espaço-tempo (através de tecnologias como GPS, *iBeacon* e RFID), dentre outros. Em resumo: a tecnologia da informação destrói não apenas os muros do panóptico, mas todas as tradicionais categorias que buscam contê-la. Ela não é pública, não é privada, não está aqui, não está ali: ela está em todos os lugares como parte inerente da vida em sociedade.

Assim, falha a CPI ao colocar considerar equivalentes eventos intrinsicamente distintos – espionagem de autoridades pela NSA e coleta massiva de dados de todos os indivíduos pela iniciativa pública e privada. A espionagem, conforme o próprio relatório, é a segunda profissão mais antiga da humanidade e agora encontra-se "turbinada" pela assimetria no poder tecnológico de países como os EUA. O segundo, muito mais amplo, é uma novidade viabilizada por uma conjunção de fatores extremamente complexos e que escapam explicações simplistas da ideia de espionagem.

Como consequência, o relatório da CPI torna-se extremamente míope para a violação de direitos fundamentais que não sejam a privacidade, como, por exemplo, a igualdade. Afinal, será que somos realmente iguais se, antes mesmo de pensarmos, todos os nossos passos – aparentemente aleatórios – foram analisados e, através de sistemas com critérios que escapam qualquer ideia de democracia, fomos classificados em categorias que irão ter efeitos reais nas nossas vidas (como "autorizado", "não autorizado", "de interesse comercial ou para segurança", "liberal", "democrata", "judeu", "católico", "ateu" etc.)?

O problema é muito mais amplo e complexo do que a ocorrência de algumas "espionagens". Fossem a mesma coisa, não haveria necessidade de tanto debate – tampouco de uma CPI –, porque a espionagem é tão antiga quanto a própria humanidade. Não haveria novidade exceto do meio utilizado para espionar. Esse, obviamente, não é o caso, o que pode ser confirmado pela simples existência da CPI.

No que diz respeito às soluções propostas pelo relatório da CPI, ele busca – numa espécie de "corrida científica do século XXI" aumentar a capacidade do Estado brasileiro para coletar e processar dados. *Mutatis mutandis*, é como se a solução para o problema das armas fosse comprar mais armas. Em seu item VI. 1.2, o relatório reconhece que

> Se existe uma afirmação que pode ser feita sobre a espionagem internacional é que esta continuará e, de fato, mostrar-se-á mais intensa com o desenvolvimento de recursos tecnológicos que permitam a operação no ambiente virtual. Essa espionagem, feita por governos, empresas e organizações não pode ser objeto de qualquer regulamentação internacional, pois é atividade típica do sistema internacional anárquico. Assim, iniciativas de se propor um regime internacional para regular o recurso à espionagem por parte de governos é, na melhor das hipóteses, utópica e ingênua. O direito internacional dificilmente alcançará o ofício dos espiões. Diante dessa realidade, o que o Estado brasileiro deve fazer é investir em contrainteligência. Isso envolve mais recursos para os serviços secretos, aquisição e desenvolvimento de equipamentos, capacitação de recursos humanos e, ainda, estabelecimento de legislação que dê amparo ao setor de inteligência e permita a seu pessoal atuar em defesa do Estado e da sociedade.

Antes de tudo, é preciso deixar bem claro que, se existe uma coisa que as revelações do Edward Snowden nos ensinaram é que, no que diz respeito à coleta massiva de dados pelo Estado, há pouca ou nenhuma relação entre setores de inteligência e defesa da sociedade. O fortalecimento desses setores no cenário brasileiro vai de encontro àquela pretensão inicial do Snowden – agora muito defendida até mesmo no cenário público dos EUA: a redução da coleta massiva de informações. O Brasil parece caminhar na marcha ré ao propor o fortalecimento de algo que, no mundo inteiro, deveria ser enfraquecido.

Há que se concordar, contudo, com a afirmação de que "o direito internacional dificilmente alcançará o ofício dos espiões". O problema, no entanto, é que o reconhecimento da *surveillance* como fenômeno impede que se fale de mera espionagem, como já se pretendeu deixar claro anteriormente. Por isso, é necessário insistir na ideia de que a compreensão equivocada do problema gera respostas igualmente erradas.

Dentre as soluções propostas pelo relatório estão "investimento em contrainteligência"; "maior dotação orçamentária para a comunidade de inteligência"; "criação de agência brasileira de inteligência de sinais"; "criação de comissão temporária, no âmbito do Senado Federal, para propor reformas na legislação brasileira de inteligência"; "aprovação da PEC 67/2012"; "aprofundamento dos mecanismos de controle externo da atividade de inteligência". Todas elas têm em comum aquele objetivo de fortalecer algo que deveria ser enfraquecido. Como o caso estadunidense mostra, o principal alvo desses serviços é a população. A consequência final desse desenvolvimento terá pouco a ver com uma maior segurança das "informações brasileiras" e estará muito mais direcionada aos próprios brasileiros.

Obviamente, devem ser buscados mecanismos para proteger empresas nacionais estratégicas – como a Petrobrás – ou as informações trocadas pelo alto escalão do poder público. De fato, sem a capacidade técnica para auditar sistemas e equipamentos, é nula qualquer tentativa de proteger essas informações. No entanto, a inserção deliberada de fragilidades é empregada em diversos sistemas, gerando um custo anual para a NSA de duzentos e cinquenta milhões de dólares para concretizar suas "parcerias secretas"[26]. Contudo, é de se questionar se o Brasil possui alguma chance de combater esse tipo de ataque, uma vez que, por mais desenvolvida que seja a tecnologia nacional, ainda dependeremos de processadores, memórias, equipamentos de rede etc., todos eles produzidos com tecnologia estrangeira.

O último – e mais importante – problema diz respeito ao pano de fundo no qual se movem as soluções apontadas tanto pelo relatório da CPI quanto pela crença na capacidade do marco civil da Internet para regulamentar o fluxo de dados. A tecnologia da informação dissolve as fronteiras de espaço e de tempo. Perde qualquer sentido, portanto, sustentar que o

[26] Veja-se, por exemplo, o caso da falha do Dual_EC_DRGB: de acordo com Snowden, a National Security Agency (NSA – EUA) e o Government Communications Headquarters (GCHQ – Reino Unido) teriam pago o valor de dez milhões de dólares para criar um backdoor numa tecnologia de criptografia extremamente importante, tornando vulnerável a ataques grande parte dos sistemas de criptografia da atualidade.

mecanismo "lei" – associado ao Estado vinculado a um território – possa ser capaz de conter um fenômeno marcado pela desterritorialidade.

O art. 2 do projeto de lei contido no anexo I do relatório da CPI determina que "o fornecimento de dados relativos ao fluxo de comunicações, ou de comunicações privadas armazenadas, de cidadãos brasileiros ou de empresas brasileiras, para autoridade governamental ou tribunal estrangeiros, deverá ser previamente autorizado pelo Poder Judiciário brasileiro [...]". Essa afirmação não é nenhuma novidade. Desde a constituição de 1988, a autorização judicial tornou-se indispensável para quebrar o sigilo telemático. Entretanto, pergunta-se: qual a relevância disso no modo de operar das grandes empresas de tecnologia e das poderosas agências de inteligência? Nenhuma, por óbvio.

A mudança espacial da infraestrutura defendida pelo tanto pela CPI da espionagem como pelos debates no anteprojeto do marco civil – através da concentração de servidores e rotas de dados em território nacional – também é de baixa relevância. Pouco importa a localização física de um determinado servidor: os fluxos de dados não conhecem as fronteiras do Estado-nação. Fica claro, assim, que não adianta pensar "o novo" através de proposições "velhas", baseadas todas elas na ideia de territorialidade.

Além disso, é possível afirmar que, sustentado em um pensamento ultrapassado – o que pode ser visto na confusão entre espionagem e coleta massiva de dados (por nós denominada *surveillance*), bem como nas tentativas de resolver tais problemas sempre retomando à ideia de territorialidade –, o relatório final da CPI sofre de uma miopia que, se não ingênua, é maligna. Isso porque o pouco que há de concreto nas suas conclusões é que o Brasil precisa urgentemente investir em agências de inteligência. Tais agências, como ficou claro no caso dos EUA, nada fazem contra inimigos externos – a NSA falhou ao tentar citar um único caso em que seus sistemas impediram um ataque terrorista.

O Estado, pelo menos nos moldes como conhecemos, é uma das primeiras instituições a sentir o distanciamento, típico da modernidade líquida, entre política – entendida como a capacidade de escolher as ações a serem tomadas – e poder – entendido como a capacidade de agir (BAUMAN, LYON, 2013).

## 3.4 – TRANSFORMAÇÕES DO ESTADO E DISSOLUÇÃO DA SOBERANIA NO MUNDO CONTEMPORÂNEO

Ao analisar as transformações do Estado no mundo contemporâneo, entretanto, é insuficiente, senão equivocado, utilizar as categorias que foram desenvolvidas em outros contextos espaço-temporais, ou seja, é preciso "olhar o novo como novo". Isso reforça a necessidade de entender a capacidade que as novas tecnologias da informação têm para liquefazer aquilo que, comumente, não era líquido, ou seja, de atribuir "hipermobilidade" àquilo que é físico.

A perda de diversos componentes da autoridade formal do Estado não significa o desaparecimento das antigas estruturas de poder, mas o seu rearranjo. Nesse sentido, Sassen (2006, p. 346, tradução nossa) afirma que a "a teoria existente não é suficiente para mapear a atual multiplicação de atores não estatais nem as formas transfronteiriças de cooperação e conflito, como as redes globais de negócios, ONG's, diásporas, cidades globais, esferas públicas transfronteiriças e o novo cosmopolitismo"[27].

Por esse motivo, é possível afirmar que o direito internacional, comumente mencionado como possível solução para os problemas desterritorializados das novas tecnologias da informação, também é insuficiente. Isso porque suas categorias foram pensadas para relações interestatais (cujos sujeitos são exclusivamente Estados-nação) e ignora o fato de que, atualmente, os atores globais não são sempre estatais e, portanto, não obedecem a sua lógica.

Em síntese, a proposta de Saskia Sassen demonstra que a soberania estatal – entendida como a capacidade, dentro de um determinado território, de centralizar e legitimar todo o poder e o direito – torna-se instável, uma vez que as manifestações de poder nos territórios deixam de ser mutuamente excludentes. Ainda que o Estado-nação permaneça sendo importante no cenário interno e externo, diversos poderes – associados a determinados territórios ou não – passam a ganhar cada vez mais espaço no cenário atual.

De maneira similar, Jose Luis Bolzan de Morais (2011, p. 35 e ss), ao tratar da crise conceitual do Estado, ressalta que o modelo estatal moderno não consegue lidar com as perplexidades oriundas da multipolarização do mundo globalizado. As categorias tradicionais da teoria do Estado, associadas às estruturas de poder modernas, também são fragilizadas pela descentralização e concorrência de poderes não estatais, tornando-se insuficientes para

---

[27] No original: "Existing theory is not enough to map today's multiplication of nonstate actors and forms of cross-border cooperation and conflict, such as global business networks, NGOs, diasporas, global cities, transboundary public spheres, and the new cosmopolitanisms.".

caracterizar o fenômeno estatal do mundo globalizado. Isso requer a superação do modelo "fechado" do Estado, reconhecendo as inevitáveis transformações associadas à pulverização do poder. Essa pulverização, embora possibilite o deslocamento do poder em direção para outros *loci* , não exclui o poder público, uma vez que "embora fragmentado e fragilizado [...] este foi redefinido, mas não abolido".

É possível, através do mesmo raciocínio que Bolzan de Morais usa para tratar do problema ambiental, afirmar que a compreensão jurídica do fenômeno da *surveillance* não pode ignorar as transformações do Estado no mundo globalizado, que ultrapassam a lógica do modelo de direito moderno, submetido à territorialidade estatal. Muito além de estarem meramente relacionadas, as novas tecnologias telemáticas reestruturam a visibilidade, a territorialidade e a temporalidade.

Assim, talvez seja necessário questionar se o Estado, dentro dessa nova dinâmica, pode, ainda, fazer frente aos diversos *players* globais da tecnologia da informação. Em outras palavras: a teoria do Estado tradicional – que fundamenta o "mito" de que ele pode proteger a os direitos fundamentais dos indivíduos frente à liquidez da *surveillance* – não pode dar todas respostas aos problemas do mundo atual. É necessário, pois, perguntar quais os novos limites e papéis do Estado na contemporaneidade.

Dentro desses novos papeis, é necessário reconhecer a dissolução da soberania como uma consequência do surgimento de novas estruturas não estatais de autoridade e poder. Agora vulnerável aos ataques cada vez menos específicos – e, por isso mesmo, mais inevitáveis – das diversas fontes de poder do mundo contemporâneo, o Estado-nação tem suas funções reformuladas, agindo não mais como centro, mas como "nós" – *nodes* – (CASTELLS, 2010) de uma rede descentralizada de poder. Nesse sentido, Saskia Sassen (1996) entende que soberania e território permanecerão como características fundamentais do sistema internacional. No entanto, elas foram parcialmente desviadas em direção a outras arenas institucionais fora do Estado e do modelo de território nacionalizado. Dado que a exclusividade de soberania e de território, do ponto de vista histórico, são essenciais para o Estado-nação, essa mudança representa uma reviravolta do próprio conceito de Estado.

Assim, o Estado-nação, com sua autoridade soberana, é antagonizado pelos influxos dos diversos poderes que também são nós da rede, como acontece, por exemplo, quando os *data-doubles* dos indivíduos circulam livremente, sem possibilidade de controle pelo Estado-nação, entre empresas quem monetizam as informações (e metainformações) dos indivíduos e das suas atividades cotidianas. Com isso, desconstrói-se a soberania, pelo menos no seu

conceito tradicional, uma vez que ela deveria ser indivisível. Nessa nova função, embora mantenha certo poder decisório em determinados assuntos, o Estado-nação passa a ser também influenciado pelas decisões de uma pluralidade de poderes que integram a rede descentralizada de atores globais. Por isso mesmo, talvez continue a ser necessária, portanto, uma teoria do Estado, visto que as relações de poder, embora não confinadas exclusivamente na esfera estatal, continuam a ser parte de toda a atividade estatal, mas muito mais como uma *teoria do poder*.

As limitações da territorialidade, as transformações da soberania e a desnacionalização são características essenciais da globalização. Tais transformações são tão importantes que "falar em soberania, nos dias atuais, como um poder irrestrito, muito embora seus limites jurídicos, parece mais um saudosismo do que uma avaliação lúcida dos vínculos que a circunscrevem" (BOLZAN DE MORAIS, 2011, p. 28). Muitos dos processos globais, contudo, ainda dependem frequentemente da entrada no âmbito do Estado-nação para serem operacionalizados. Trata-se de um fenômeno complexo, que resiste à simplicidade das explicações duais e que requer que sejam decifradas as "profundas mudanças estruturais por baixo das continuidades superficiais, e, alternativamente, as profundas continuidades estruturais por baixo das descontinuidades superficiais" (SASSEN, 2006, p. 12, tradução nossa)[35].

No caso do marco civil da Internet, a resposta estatal para uma multiplicidade de problemas foi a lei, como expressão da soberania do Estado. Esses problemas, contudo, são tão distintos que dificilmente poderiam ser resolvidos da mesma maneira. Por um lado, a exigência da neutralidade na rede pode, de fato, proteger a liberdade ao impedir que empresas privadas apliquem técnicas de *traffic shapping*[36] desleais, prejudicando concorrentes e filtrando serviços e conteúdos que poderiam ser acessados pelos internautas no Brasil. Por outro, tenta evitar violação da privacidade através da deficiente exigência de uma suposta inviolabilidade das comunicações privadas.

Ao invés de um debate entre os representantes do povo brasileiro, a proteção dos direitos fundamentais violados pela *surveillance* deve ocorrer a partir da consideração dos

---

[35] No original: "[...] deep structural shifts underlying surface continuities and, alternatively, deep structural continuities underlying surface discontinuities.".

[36] A prática de *traffic shapping* viola a neutralidade da rede, uma vez que os detentores da estrutura física – provedores – poderiam utilizar essa ferramenta para controlar quais serviços e *websites* terão prioridade ao trafegar em sua rede. Isso possibilitaria o direcionamento ao acesso somente aos conteúdos por eles aprovados.

fatores aqui mencionados, levando em conta a presença dos grandes *players* globais: Estados e empresas privadas de tecnologia da informação. Afinal, a liquidez cada vez maior dos fluxos de dados leva a um processo de diminuição sistemática da soberania e do poder do Estado-nação como forma de manter sua longevidade.

## CONSIDERAÇÕES FINAIS

Com estas considerações, nossa pretensão foi entender de que maneira a garantia de inviolabilidade das comunicações privadas contida no marco civil brasileiro da Internet serve para proteger os direitos fundamentais, eminentemente o direito à privacidade.

Para tanto, buscamos a perspectiva dos *surveillance studies* como marco teórico para fazer algumas indagações: 1) o que é *surveillance*?; 2) por qual motivo não podemos confundi-la com vigilância?; 3) como a tecnologia da informação modifica o nosso conceito de privacidade?; 4) quais as mudanças que essa mesma tecnologia proporciona ao poder estatal? 5) será que mecanismos vinculados à territorialidade – como é o caso do marco civil da CPI da espionagem – podem, efetivamente, proteger os direitos fundamentais contra violações oriundas da *surveillance*?

Uma perplexidade causada pelos *surveillance studies* é a superação da ideia de que informações pessoais e comunicações privadas dizem respeito apenas à privacidade. Esse lugar-comum no direito faz com que os juristas já comecem a encarar o problema de maneira equivocada, o que pode ser simbolizado pela ausência do enfrentamento, pelo marco civil brasileiro e pela CPI da espionagem, das cruéis violações da igualdade patrocinadas pela *surveillance*.

Desde concessões de benefícios somente para indivíduos caracterizados como "de interesse comercial", até a impossibilidade de utilizar transporte aéreo – veja-se o exemplo das famosas *no-flight lists* – para indivíduos que sofrem as consequências de um sistema que coleta e analisa informações com critérios que não passam por qualquer tipo de controle democrático, é possível afirmar que a *surveillance* viola muito mais que a privacidade.

Por óbvio, se não concordamos com a possibilidade de ampla efetividade do art. 7º, inciso III do marco civil, certamente também não acreditamos que seria efetivo um dispositivo legal que protegesse a igualdade. Não se trata, por enquanto, de efetividade – afinal, como visto, não acreditamos que ela seja possível através de instrumentos vinculados à territorialidade –, mas de um problema simbólico: sequer fala-se disso na lei.

Alguns autores apontam para a desintegração do Estado-nação. Outros, mais otimistas, entendem que a expansão mundial e aplicação em grande escala do modelo estatal seria a forma mais adequada e viável de proteger os direitos fundamentais (FERRAJOLI, 2011). Outros teóricos, como Manuel Castells (2005, 2010), por perceberem que o mundo está passando por um processo de transformação diversificado – mudanças econômicas, políticas, tecnológicas, institucionais e culturais –, acreditam que estamos presenciando o surgimento de uma ordem global multifacetada, cuja característica principal é a sua formatação em redes de cooperação entre Estados e instituições internacionais.

Parece claro que não estamos presenciando o fim do Estado. Ele ainda é importante. O marco civil da Internet, fruto do direito desse Estado, é igualmente importante. Todavia, existem problemas que não podem ser resolvidos por essas vias tradicionais. O papel do jurista é reconhecer esses problemas, deslocando-se do discurso fetichizado da lei que, seguindo a etimologia da palavra, enfeitiça o profissional do direito, fazendo-o acreditar que o direito vinculado à territorialidade estatal é a solução para todos os problemas do homem.

Assim, como juristas, temos que questionar se uma ferramenta tão sólida quanto a lei é capaz de controlar algo tão líquido quanto os fluxos de dados. Por um lado, o marco civil, embora fundamentado em uma ideia equivocada sobre o papel da lei na modernidade líquida, possui enorme importância para o país, sendo sua aprovação, definitivamente, um ganho para a sociedade brasileira e, em muitos pontos, um exemplo a ser seguido por outros países. Por outro, a proposta de lei incluída no relatório da CPI da espionagem é perigosa, visto que busca criar o pânico para criar uma necessidade. Assim como os EUA utilizaram essa tática em relação ao terrorismo, o relatório da CPI busca fazer a mesma coisa, só que com o argumento de que o Brasil não pode ficar para trás. Obviamente, quem perde, com isso, é a democracia, a cidadania e os direitos fundamentais.

O que o direito precisa reconhecer é que o mundo, assim como a vida, é demasiado complexo e caótico para caber no espaço rígido e seguro da lei. Ao invés de tentar simplificar o mundo, o trabalho do jurista é fazer parte desse caos e, dentro dele, encontrar formas efetivas de proteger os direitos fundamentais.

## REFERÊNCIAS

BAUMAN, Zygmunt; LYON, David. **Liquid Surveillance**: A Conversation. Cambridge: Polity Press, 2012. 152 p.

_____. **Modernidade líquida**. Tradução de Plinio Dentzien. Rio de Janeiro: Zahar, 2001. 258 p.

BENNET *et al*. **Transparent lives**: surveillance in Canada. Edmonton: AU Press, 2014. 239 p.

BOLZAN DE MORAIS, Jose Luis . As crises do estado e da constituição e a transformação espacial dos direitos humanos. 2. ed. Porto Alegre: Livraria do Advogado, 2011. 143 p.

BRASIL. Senado Federal. **Relatório final da CPI da espionagem**. Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Disponível em < http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em 21 jul 2014.

CASTELLS, Manuel. **End of millennium**: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, 2010. v. 3. 456 p.

_____. Global Governance and Global Politics. **PS: Political Science & Politics**, p. 9-16, jan. 2005. Disponível em <http://arkkitehtuuri.tkk.fi/YKS/fin/opetus/kurssit/yks_teoria/luennot/Castells/2005Global-Castellas.pdf>. Acesso em 23 ago 2013.

_____. **The power of identity**: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, 2010. v. 2. 538 p.

FERRAJOLI, Luigi. **Poderes salvajes**: La crisis de la democracia constitucional. Tradução de Perfecto Andrés Ibáñez. Madrid: Trotta, 2011. 109 p.

GINSBERG, Jeremy et al. Detecting influenza epidemics using search engine query data. **Nature**, n. 457, p. 1012-1014, 19 fev. 2009

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, Washington, v. 110, n. 15, p. 5802-5805, 9 abr. 2013. Disponível em <http://www.pnas.org/content/110/15/5802>. Acesso em 11 jun. 2014.

LYON, David. Identification, surveillance and democracy. In: HAGGERTY, Kevin; SAMATAS, Minas (orgs.). **Surveillance and democracy**. London: Routledge, 2010. p. 34-50.

_____. Introduction. In:_____ (org). **Surveillance as Social Sorting**: Privacy, risk and digital discrimination. London: Routledge, 2003. p. 1-9.

_____. **Surveillance society**: Monitoring everyday life. Buckingham: Open university press 2001. 189 p.

_____. **Surveillance Studies**: An Overview. Cambridge: Polity Press, 2007. 243 p.

_____. Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies. **International Political Sociology,** Tucson, v. 4, n. 4, p. 325-441, 2010. ISSN: 1749-5679. DOI: 10.1111/j.1749-5687.2010.00109.x.

_____. **The Electronic Eye**: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 1994. 270 p.

_____ (org.). **Theorizing Surveillance**: The panopticon and beyond. Cullompton: Willan Publishing, 2006. 351 p.

MARX, Gary T. What's New About the "New Suveillance"? Classifying for Change and Continuity. **Surveillance and society**, v. 1, n. 1, p. 9-29, 2002. ISSN: 1477-7487.

MCLUHAN, Marshall. Playboy interview: Marshall McLuhan: a candid conversation with the high priest of popcult and metaphysician of media. **Playboy**, Chicago, v. 16, n. 3, p. 53-75, mar. 1969.

SASSEN, Saskia. **Losing control?** Sovereignty in an Age of Globalization. New York: Columbia University Press, 1996.

_____. **Territory, authority, rights**: From Medieval to Global Assemblages. Woodstock: Princeton University Press, 2006. 493 p.

SCHOPENHAUER, Arthur. **A arte de escrever**. Tradução de Pedro Süssekind. Porto Alegre: L&PM, 2009 176 p.