Relatório da CPI da Espionagem é míope em dois pontos: objeto e soluções

Recentemente, o Senado liberou o relatório final da CPI da espionagem[1]. O próprio nome da CPI expressa a posição adotada em relação às informações divulgadas por Edward Snowden, ex-analista da NSA. Apesar dos eventuais avanços — toda pesquisa sobre o uso da SIGINT (signals intelligence) parece ser válida, especialmente se considerarmos que pouco se fala sobre o assunto —, o relatório é extremamente míope em dois pontos essenciais: a) a compreensão do fenômeno que quer discutir e b) as soluções elencadas para os problemas.

O que a CPI deveria discutir? O erro de objeto da CPI

O relatório faz amplo uso da palavra "espionagem" para se referir ao seu objeto. 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 peculiares das sociedades contemporâneas. Não apenas grandes potências militares, como os EUA, mas, especialmente, grandes grupos privados dedicam cada vez mais esforços para o desenvolvimento de tecnologias para coleta, análise e processamento de informações.

A análise que permeia o texto da CPI engloba a violação da privacidade como único resultado da utilização de técnicas de coleta e processamento massivo de dados. Entretanto, as violações 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 esta "nova" *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 da CPI, uma mistura entre eventos pontuais de espionagem — como, por exemplo, a invasão de comunicações de servidores da Petrobras 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 centrais: 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 entanto, 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 "nova" *surveillance* é a prática da *data mining* pela iniciativa privada. Armazena-se indiscriminadamente todo o tipo de informação 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 e interações entre usuários, é possível classificar suas preferências, tornando a publicidade cada vez mais direcionada e precisa. Em pesquisa recente[2], 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" do *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[3]. Como resultado, a empresa de Mountain View, por exemplo, é capaz de prever surtos daquelas doenças com precisão e antecedência muito maior que os órgãos governamentais.

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. Ou de uma "sociedade panóptica". 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 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 nesta sociedade tecnológica de que, as vezes, tanto nos vangloriamos.

Assim, falha a CPI ao 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 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 forma de controle democrático e jurídico, 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.)?

Assim, o problema é muito mais amplo e complexo do que a ocorrência de algumas "espionagens". Fosse a mesma coisa, não haveria necessidade de tanto debate — tampouco de uma CPI —, porque a espionagem é tão antiga quanto a própria humanidade, como concluíram o membros da mesma. Não haveria novidade, exceto no meio utilizado para espionar. Esse, obviamente, não é o caso.

As soluções elencadas pela CPI

Também, no que diz respeito às soluções propostas pelo relatório da CPI, entendemos que 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. Mas, com o final dos trabalhos, tal corrida mais se assemelha àquela dos desenhos

televisivos — a “corrida maluca”. 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. E que, por evidente, não trará resultados.

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 não estamos falando de mera espionagem, como já se pretendeu deixar claro anteriormente. Por isso, insistimos que a compreensão equivocada do problema gera respostas igualmente erradas. Respostas do tipo “senso comum”, ou respostas *prêt-à-porter*.

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 o objetivo de fortalecer algo que deveria ser enfraquecido. De responder questões novas/inéditas com soluções velhas. 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 Petrobras — 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. A inserção deliberada de fragilidades em sistemas é muito comum, gerando um custo anual para a NSA de U$ 250 milhões para concretizar suas "parcerias secretas" [4]. 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 pelo relatório da CPI. A tecnologia da informação dissolve as fronteiras de espaço e de tempo. Perde qualquer sentido, portanto, sustentar que o mecanismo "lei" — associado ao Estado, vinculado a um território — é capaz de conter um fenômeno marcado pela desterritorialidade. Ou seja, o "velho" direito nacional parece que nada pode fazer frente a esta "nova" *surveillance.*

O artigo 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. Sempre foi necessária a autorização judicial para quebrar o sigilo telemático, há uma Constituição que — parece! — protege essas informações! Agora a pergunta: 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 projeto — 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.

Como conclusão, 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 "nova" *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 burra (com perdão pela expressão). 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.

Parece que se quer criar o pânico para produzir uma necessidade, que, por evidente, é falsa: se 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 "não podemos ficar para trás".

Quem perde, com isso, é a democracia, a cidadania e os direitos fundamentais.

[1] http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1

[2] KOSINSKI, Michal et al. 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.

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

[4] Veja-se o exemplo do Dual_EC_DRGB: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Date Created
13/05/2014