Pegasus

Por **SÉRGIO AMADEU DA SILVEIRA***

O software-espião israelense foi encontrado no aparelho celular de ativistas de direitos humanos, jornalistas e autoridades

O filósofo Gilbert Simondon apresentou o conceito de alienação técnica para mostrar o grande equívoco constante na recusa de ver a tecnologia como expressão da cultura. É difícil encontrar uma sociedade que não crie, invente e adote objetos técnicos em seu cotidiano. As técnicas e as tecnologias integram nossa existência social e negar que sejam elementos cruciais de estruturação da vida coletiva faz parte dessa alienação. Milton Santos nos ensinou que "a principal forma de relação entre o homem e a natureza, ou melhor, entre o homem e o meio, é dada pela técnica", mas também constatou que na maioria das vezes tal premissa era desconsiderada.

O capitalismo, em sua fase neoliberal, se alimenta também da alienação técnica para se reproduzir e expandir novas formas de extração de valor. As tecnologias são apresentadas como neutras, meramente "técnicas", distantes de condicionamentos sociais, políticos, econômicos e ideológicos. Tecnologias muitas vezes são naturalizadas e expostas como imutáveis, definitivas. O marketing exibe os objetos técnicos como verdadeiros "passes de mágica", benéficos e distantes das complexas redes de decisões empresariais que o produziram.

As corporações retratam as tecnologias como desprovidas de quaisquer possibilidades de portar interesses escusos, ambientalmente e socialmente prejudiciais. As empresas desenvolvedoras de tecnologia se exibem como incapazes de trazer interesses que extrapolem a melhoria da experiência de seus consumidores ou usuários. "*Don't be evil*" era o lema do Google que foi substituído pelo "*do the right thing*", seja lá o que deva ser considerado certo.

Uma vez ou outra as tecnologias ou os processos tecnológicos causam assombro. Eventualmente uma reportagem mostra que uma determinada tecnologia pode portar efeitos colaterais ou malefícios. Em certos momentos, como agora, uma empresa e seu produto tecnológico é exposto como algo prejudicial à sociedade. Mesmo assim, a alienação é reforçada, pois o caso é apresentado como um ponto fora da curva, como uma exceção. Esses parágrafos iniciais são importantes para chamar a atenção de que existe atualmente a prática tão disseminada quanto perigosa de coleta massiva de dados praticada por insuspeitas corporações que enevoam e obscurecem outras práticas mais nocivas para as democracias e direitos humanos.

Além de um gigantesco mercado de dados pessoais amplamente aceito e que obtém, atualmente, a maior fatia dos gastos em publicidade e propaganda do planeta, existe um mercado também bilionário de espionagem e obtenção ilegítima e ilegal de dados. Quem não se recorda de Edward Snowden? O ex-agente do aparato de inteligência dos Estados Unidos demonstrou que a *National Security Agency*, NSA, espionava cidadãos comuns e autoridades a partir do uso que essas pessoas faziam de redes sociais, e-mail de empresas como Microsoft, Google, entre outras, que atualmente fazem parte do cotidiano das nossas sociedades. As denúncias espetaculares de Snowden geraram uma enorme onda de indignação passageira.

Recentemente, o jornal *The Guardian* publicou o vazamento de informações de uma empresa que integra o mercado de dados bilionários da espionagem industrial e política. O NSO Group, empresa israelense de ciberguerra, que desenvolve e vende um software de espionagem chamado Pegasus, teve 50.000 números de telefones de seus alvos entregues para a imprensa. Por que uma empresa de espionagem iria guardar seus alvos? Como explicou Nicholas Weaver, para monitorar quem está espionando e saber de tudo que o espião obteve dos espionados. É importante destacar que as empresas

© 2025 A Terra é Redonda. Todos direitos reservados. ISSN 3085-7120.

israelenses de espionagem são monitoradas e controladas pela inteligência israelense.

Corporações de ciberguerra e espionagem muitas vezes se apresentam como empresas de segurança digital ou segurança da informação. O NSO Group vendeu o acesso aos seus dispositivos de intrusão em celulares e captação de dados para governos e empresas de aproximadamente 40 países. O software-espião Pegasus foi encontrado no aparelho celular de ativistas de direitos humanos, jornalistas e autoridades. O assassinato do dissidente saudita de Jamal Khashoggi e de jornalistas mexicanos podem estar ligados a aquisição de informações a partir do Pegasus, uma vez que o spyware ou software-espião foi encontrado nos celulares das vítimas.

As informações divulgadas em julho desse ano foram rigorosamente checadas, uma vez que o grupo de jornalismo independente Forbidden Stories e a Anistia Internacional solicitaram ao Citizen Lab, da Universidade de Toronto, uma análise forense do Pegasus com revisão de pares independentes. A análise constatou as práticas de espionagem do NSO Group que são extremamente perigosas para as democracias e para os direitos e garantias individuais.

Por enquanto, sabemos que ditadores, forças de segurança e certos empresários são grandes clientes desse mercado de espionagem. James Bamford, jornalista investigativo, escreveu para a *Foreing Policy*, em 2016, sobre a economia da espionagem. No artigo, Bamford relata que Ricardo Martinelli, ex-presidente do Panamá, usou e abusou da espionagem ilegal de líderes da oposição, jornalistas, juízes, rivais de negócios, entre 150 alvos, graças ao que nomeou de "florescente negócio de empresas privadas que vendem *spyware* de nível militar". Já em 2011, o *Wall Street Journal* estimava o mercado varejista de ferramentas de vigilância e espionagem em US$ 5 bilhões.

Israel é considerado o paraíso dessas empresas. Amitai Ziv, em uma matéria escrita para o jornal *Haaretz*, em janeiro de 2019, esclareceu que Israel possui a renomada unidade de inteligência 8200 das Forças de Defesa do país. Esse serviço é uma fonte de recrutamento de operadores e hackers de alto nível para as empresas de espionagem. Estima-se que esses ex-agentes da unidade 8200 passam a receber, no mínimo, 80 mil shekels mensais, o que equivale a 21 mil dólares norte-americanos. No mesmo texto, Ziv alertava sobre uma nova empresa de ataques cibernéticos: "Candiru, que deve o seu nome a um peixe amazônico conhecido por parasitar a uretra humana, recruta pesadamente pessoas da unidade 8200 e vende ferramentas ofensivas para hackear sistemas de computador".

A empresa chamada Candiru também foi analisada pelo *Citizen Lab*. Trata-se de uma companhia secreta que obviamente possui a proteção das autoridades de defesa. Segundo a investigação, a empresa Candiru também explora falha de celulares com seus *spywares*. Junto com o *Microsoft Threat Intelligence Center* (MSTIC), o *Citizen Lab* constatou pelo menos 100 vítimas na Palestina, Israel, Irã, Líbano, Iêmen, Espanha, Reino Unido, Turquia, Armênia e Cingapura. Foram detectados mais de 750 sites vinculados a infraestrutura de espionagem do Candiru, alguns se passam por organizações da sociedade civil e veículos de imprensa.

Temos um mercado legal de extração de dados que convive ao lado de um mercado de espionagem que viola completamente as legislações de proteção de dados. O primeiro vigia as pessoas com interesses comerciais e de marketing, o segundo espiona para tirar vantagens industriais, geopolíticas e militares. O problema é que governos, incluindo o dos Estados Unidos, utilizam ambos os mercados para manter suas posições geoestratégicas. Há um fluxo de dados entre um e outro mercado. Como Snowden nos mostrou, há um conúbio entre figuras e estruturas desses mercados.

Além disso, existe ainda a disputa entre os agrupamentos burocráticos, o que também estimulam a confusão das fronteiras entre os dois mercados de tecnologias de intrusão e captura de dados. Carlos Bolsonaro, o filho vereador do presidente, queria retirar do controle das Forças Armadas brasileiras e da ABIN a possível aquisição do spyware Pegasus. Articulou para que o Ministério da Justiça, considerado mais aliado aos interesses da sua família, lançasse uma licitação para a compra do dispositivo. O alerta da operação provavelmente veio de militares descontentes com o que consideravam um desvirtuamento burocrático.

Qual seria o objetivo de Carlos Bolsonaro com a aquisição do Pegasus? Instaurado o escândalo, o NSO Group disse que não iria participar da licitação. Mas uma outra empresa de espionagem vencerá a licitação e entregará um dispositivo de contágio de celulares e de e-mails para o governo Bolsonaro. Curiosamente, não temos um levantamento abrangente de quantos *spywares* estão em operação no país, adquiridos com dinheiro público pelo governo federal e pelos governos estaduais.

Por fim, a alienação técnica se apresenta mais uma vez quando consideramos normal ou natural os processos e modelos de

© 2025 A Terra é Redonda. Todos direitos reservados. ISSN 3085-7120.

negócios preponderantes das tecnologias digitais, amplamente utilizadas para a coleta e tratamento de nossos dados, legal e ilegalmente. O nome Candiru do peixe da Amazônia não poderia expressar melhor o que as empresas dos dois mercados fazem ao acumular dados sensíveis sobre nossas vidas. Mas, isso assemelha-se a um roteiro de filme da Netflix. Não gera indignação. Parece que os processos são assim porque não haveria outro caminho, outros modos de viver as tecnologias. Não se renda. Nada nas tecnologias digitais a conduzem inevitavelmente para a vigilância pervasiva e para a espionagem. Precisamos romper com a alienação técnica.

***Sergio Amadeu da Silveira** *é professor da Universidade Federal do ABC. Autor, entre outros livros, de* Software livre – a luta pela liberdade do conhecimento *(Conrad).*

Referências

BAMFORD, James. The Espionage Economy. U.S. firms are making billions selling spyware to dictators. *Foreing Policy*, january,22,2016. Disponível: https://foreignpolicy.com/2016/01/22/the-espionage-economy/

MARCZAK, Bill and others. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus. *Citizen Lab*, July 15, 2021. Link: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

MARCZAK, Bill and others. Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. *Citizen Lab*, July 18, 2021. Link: https://citizenlab.ca/2021/07/amnesty-peer-review/

SANTOS, Milton. *A natureza do espaço: técnica e tempo, razão e emoção*. Edusp, 2002.

SIMONDON, Gilbert. *Do modo de existência dos objetos técnicos*. Rio de Janeiro: Contraponto, 2020.

ZIV, Amitai. Top secret israeli cyberattack firm, reveled. *Haaretz*, jan. 4, 2019. Link: https://www.haaretz.com/middle-east-news/.premium-top-secret-israeli-cyberattack-firm-revealed-1.6805950

A Terra é Redonda

© 2025 A Terra é Redonda. Todos direitos reservados. ISSN 3085-7120.