PEGASUS E A CIBER ESPIONAGEM ISRAELENSE NO MÉXICO

DOLORES GUERRA

MEMO
MONITOR DO ORIENTE MÉDIO

MIDDLE EAST MONITOR

O Monitor do Oriente Médio é um instituto de pesquisa política sem fins lucrativos que fornece pesquisas, informações e análises, principalmente sobre o conflito entre a Palestina e Israel. Oferece, também, informativos sobre outras questões do Oriente Médio. Sua produção é disponibilizada para uso de jornalistas, acadêmicos e políticos com interesse nas regiões do Oriente Médio e Norte da África. O portal em português também inclui informações e análises sobre América Latina.

O objetivo do MEMO é influenciar políticas e pautas públicas a partir da perspectiva da justiça social, dos direitos humanos e da lei internacional. Isso é fundamental para obter igualdade, segurança e justiça, com atenção especial para a Palestina.

MEMO gostaria de ver um Oriente Médio definido por princípios de igualdade e justiça. Promove a restauração dos direitos palestinos, incluindo o Direito de Retorno, um Estado palestino com Jerusalém como sua capital e com direitos democráticos. Defende também um Oriente Médio livre de armas nucleares.

Ao assegurar que os formuladores de políticas sejam melhor informados, MEMO procura causar um maior impacto nos atores internacionais responsáveis pelas decisões-chave que afetam o Oriente Médio. MEMO busca uma cobertura da mídia justa e precisa sobre a Palestina e outros países do Oriente Médio.

Título: Pegasus e a ciber espionagem israelense no méxico
Imagem de Capa: Foto montagem de Antonio Cabrera

Publicado: Agosto 2021
Este relatório está disponível para download no site
do Monitor do Oriente Médio: www.monitordooriente.com

MEMO EDITORA

Monitor do Oriente Médio
Avenida Conselheiro Carrão, 1077
Sala 706, Vila Carrão São Paulo
Estado de São Paulo, Brasil
telefone: +55 (11) 2093-0599
www.monitordooriente.com

PEGASUS E A CIBER ESPIONAGEM ISRAELENSE NO MÉXICO

DOLORES GUERRA
Formada em Letras, pela Universidade de São Paulo e estudante de jornalismo na Universidade Metodista de São Paulo.

Atualmente, não é incomum ligar a televisão no México e se deparar com uma série que retrate alguém sendo espionado através de programas instalados no celular. Seja em tramas políticas, vinganças dramáticas ou *narconovelas*, a vítima não tem como se defender, pois não há indícios da invasão. Poderia ser um medo abstrato da vida contemporânea, mas a representação da ciber espionagem reflete a preocupação com uma ameaça real. Em 2017, surgiram as primeiras denúncias de que o governo mexicano havia comprado um software israelense para monitorar ilegalmente pessoas de seu interesse.

Criado pela *NSO Group*[2], o Pegasus é um software para celulares, tanto Android como iOS, cuja instalação não requer nenhum clique por parte do usuário afetado. Basta receber uma mensagem de texto ou ligação pelo WhatsApp para que o *malware* possa vigiar todas as atividades realizadas com o celular da vítima. Também apresenta a vantagem de se esconder e autodestruir qualquer rastro, caso não consiga se comunicar com seu servidor por mais de sessenta dias ou tenha acessado o dispositivo equivocado.

O consórcio jornalístico coordenado pela *Forbbiden Stories* chamado *The Pegasus Project*[3] divulgou que cinquenta mil dispositivos haviam ao menos sofrido tentativas de invasão por parte do *malware* israelense. Ao contrário da promessa original da NSO de oferecer o serviço de ciber espionagem para "prevenir e combater a criminalidade e o terrorismo", o Pegasus foi utilizado em 21 países para monitorar jornalistas, advogados, ativistas de direitos humanos e dissidentes políticos de diferentes espectros.

Único país latino-americano mencionado, o México contou com a maior quantidade de linhas telefônicas comprometidas: ao menos quinze mil entre 2016 e 2017. Desde jornalistas até o atual presidente da república, a reportagem revela que o México é o maior consumidor do Pegasus em todo o mundo. Nesse sentido, este artigo pretende discorrer sobre os sérios impactos causados no México pelas técnicas de espionagem da ocupação israelense, desenvolvidas às custas da colonização na Palestina.

A SAGA DO PEGASUS NO MÉXICO

A espionagem governamental é um crime grave pela legislação mexicana, cuja pena seria de seis a doze anos de reclusão. Ainda assim, a Secretaria de Defesa Nacional (SEDENA) contratou o *spyware* Pegasus em 2011[4], durante o mandato de Felipe Calderón.

Frustrando a promessa original de ser utilizado apenas para combater o crime organizado, o Pegasus também serviu desde o início como ferramenta de monitoramento político.

Durante o governo subsequente de Enrique Peña Nieto (EPN)[5], o uso do *malware* se ampliou para a Procuradoria Geral da República (PGR), Secretaria de Segurança Pública (SSP) e Centro de Investigação e Segurança Nacional (CISEN).

Ex-presidente do México Enrique Peña Nieto, em 19 de junho de 2013 [Chatham House]

Em julho de 2021, a *Forbidden Stories* revelou que entre 2016 e 2017, o CISEN, a Agência de Investigação Criminal (AIC) e a SEDENA escolheram cerca de quinze mil números em sua plataforma Pegasus, antevendo um eventual ataque. Ou seja, quase um terço do total de registros encontrados pela reportagem[6].

Tomás Zerón de Lúcio era titular de inteligência estatal quando EPN era governador do Estado do México, em 2009. Segundo investigações da antiga PGR, ex-agentes do CISEN e um ex-militar israelense ajudaram a formar um sistema de espionagem naquele período.

Desse modo, Zerón conheceu o empresário israelense Uri Emmanuel Ansbacher Bendrama, dono da empresa *BSD Security Systems*. Quando Peña se tornou presidente do México em 2012, trouxe consigo sua equipe de vigilância. Considerando que os antigos intermediários entre o governo de Felipe Calderón e as empresas israelenses (Azano e Weinberg) haviam se

aposentado, o caminho estava livre para os sócios Uri Ansbacher e Samuel Avishay Neryia.

Oficialmente, Ansbacher é proprietário da Projetos e Desenhos VME[7]. Ainda que o negue, o amigo de Shaley Hulio se tornou o principal distribuidor da NSO no México. Os relatórios da Unidade de Inteligência Financeira (UIF) e da Fiscalizadora Geral da República (FGR) relacionam Uri a uma rede de ao menos trinta empresas sob investigação de irregularidades nos contratos da PGR.

Na condição de diretor da Agência de Inteligência Criminal (AIC), Tomás Zerón fechou contrato com a *Tech Bull* por 32 milhões de dólares em troca do sistema Pegasus[8]. Fontes das agências de segurança mexicanas ouvidas pelo *The Pegasus Project* declararam que Zerón fazia uso do Pegasus na AIC de maneira descontrolada, assim como o CISEN e a SEDENA. Zerón ficou conhecido principalmente por ser o responsável por dois grandes casos: a recaptura do traficante Joaquín "El Chapo" Guzmán e o desaparecimento dos 43 estudantes normalistas de Ayotzinapa.

O então Secretário Técnico do Conselho Nacional de Segurança do México, Tomás Zerón de Lúcio, lança o Fórum Internacional de Segurança Nacional do México: A Perspectiva Multidimensional e os Desafios do Século XXI, realizado na Cidade do México, em 31 de agosto de 2017 [Presidência da República do México]

PEGASUS E O CASO AYOTZINAPA

O diretor da AIC[9] durante o mandato de Enrique Peña Nieto era Tomás Zerón de Lúcio. Ele aspirava equipar todas as forças de segurança estatais com tecnologia de vigilância[10], sob sua coordenação através da PGR. Foi acusado de manipulação de evidências, tortura, desaparecimento forçado e superfaturamento.

O México já era assíduo consumidor da italiana *Hacking Team*, até surgir o primeiro contrato entre a NSO e a Procuradoria-Geral da República (PGR) por 32 milhões de dólares - valor[11] muito superior aos negociados pela *Hacking Team*. Preocupada em manter seu cliente, a empresa italiana tentou investigar mais sobre o produto da concorrente, assim que a própria NSO justificou publicamente que seu diferencial era a infiltração "zero-clique".

Ironicamente, a *Hacking Team* foi hackeada em 2015, fato que a levou à falência, deixando o espaço livre para a criadora do Pegasus.

Zerón era considerado o discípulo do ex-secretário de segurança pública, Genaro García Luna, que tentou pela primeira vez implementar um sistema de espionagem. Através de uma empresa intermediária pertencente a Samuel Weinberg, empresário israelense radicado no México, a Secretaria de Defesa Nacional (SEDENA) adquiriu o sistema *NICE Track*.

A AIC foi criada em 2013 com o propósito de concentrar as tarefas de inteligência e informação, investigação e serviços periciais em um único órgão. Zerón esteve no cargo até 2016, quando foi obrigado a renunciar depois da denúncia de manipular evidências feita pelos pais dos 43 estudantes normalistas desaparecidos.

Em 2014, ele era o responsável por investigar e escrever o relatório oficial do sequestro dos 43 de Ayotzinapa, que foi o elemento detonador de manifestações multitudinárias no país. Em seu documento final, concluiu que os estudantes haviam sido sequestrados pela polícia local de Iguala, no estado de Guerrero, e entregues ao cartel Guerreiros Unidos, que teriam matado a todos e incinerado seus corpos.

A "verdade histórica", como ficou conhecida, foi refutada pela equipe internacional de peritos independentes - GIEI. Segundo a perícia realizada pela *Citizen Lab* em 2017, alguns dos participantes da GIEI foram vigiados pelo *malware* da NSO Group[12].

IRREGULARIDADES NA COMPRA DO PEGASUS

O então diretor da AIC teria superfaturado a compra de veículos equipados com sistema de espionagem, plataformas digitais de inteligência e a construção de um centro da PGR em Querétaro. Em sua defesa, justifica que alguns dos contratos são referentes ao serviço de produção e pós-produção de vídeo dos trabalhos de inteligência na operação que prendeu o narcotraficante Joaquín "El Chapo" Guzmán Loera.

A Unidade de Inteligência Financeira (UIF) detalhou o esquema de compra do *malware*, que custou 32 milhões de dólares aos cofres públicos. A PGR assinou contrato com a intermediária mexicana Tech Bull, revendedora do malware Pegasus da NSO Group. No entanto, surgem duas irregularidades no processo: superfaturamento e lavagem de dinheiro. A diferença recebida pela firma nacional era transferida para uma série de empresas fantasmas.

A principal atividade realizada pela *Tech Bull* era a compra e venda de equipamento de segurança de alto nível. No entanto, nenhum dos acionistas possuía experiência anterior como empreendedor do ramo. Ainda assim, com somente um ano de existência, a *Tech Bull* fechou a compra milionária com a PGR.

JORNALISTAS VIGIADOS PELO PEGASUS NO MÉXICO

O México é o país mais perigoso para ser jornalista do mundo[12], com exceção dos países atualmente em guerra. Muitos perdem a vida ao escrever sobre casos de corrupção e escândalos políticos que ameaçam altas esferas do poder. Os únicos jornalistas latino-americanos que constavam na lista de alvos da investigação eram mexicanos.

Não é um fato inédito a vigilância de ativistas, jornalistas, advogados e opositores no país norte-americano, mas ela nunca esteve tão sofisticada. Os jornalistas que estão mais expostos são os que investigam redes de influência e interesses relacionados com o crime organizado, as forças de segurança e oficiais corruptos.

Entre os 25 jornalistas mexicanos identificados pela pesquisa estão: Cecilio Pineda, Yuriria Sierra, Alejandro Patrón, Carmen Aristegui, Rafael Rodriguez, Jorge Carrasco, Alejandro Sicairos, Alejandra Xanic von Betrab, Marcela Turati, Ricardo Raphael, Luis Hernandez Navarro e Álvaro Delgado.

O telefone do jornalista Cecilio Pineda Birto constava na lista dos quinze mil números dos celulares-alvo do Pegasus no México. Pineda havia sido jornalista d'El Universal, um dos maiores jornais do país, antes de se tornar *freelancer*. Originário de Guerrero, denunciava supostas ligações entre o deputado Saul Beltran com a quadrilha "Los Tequileros".

Sua região é fortemente militarizada com forças de segurança federais e estatais, além das agências de inteligência. Pineda dizia não ter medo, mas sofria de insônia e ataques de pânico, então decidiu procurar o serviço de proteção federal para trabalhadores de direitos humanos e jornalistas. As ameaças que recebia foram consideradas preocupantes, mas o caso foi encerrado em outubro de 2016, pois Pineda se recusou a mudar de estado. Semanas depois, ele foi eleito um possível alvo para ser espiado pelo Pegasus.

Em 2017, as ameaças retornaram. O jornalista realizou sua última transmissão com a divulgação de seu relatório denunciando o governador do estado e elementos da polícia estatal, que supostamente sabiam onde se escondiam "Los Tequileros". Algumas horas depois, Cecilio Pineda foi assassinado enquanto esperava seu carro em um lava-jato. Seu celular desapareceu da cena do crime, não podendo passar por provas forenses.

Existe a possibilidade de que o Ministério da Defesa o havia selecionado como alvo. Considerando que muitas das forças de segurança estatais com acesso ao *spyware* possuem vínculos com o crime organizado e políticos, a informação privilegiada poderia terminar em mãos erradas.

Segundo a investigação da *Forbidden Stories*, a NSO rebateu as acusações sobre o caso de Cecílio Pineda. Em nota, a desenvolvedora do software alega que mesmo se fosse comprovada a invasão do celular do jornalista, isso não relacionaria obrigatoriamente as informações coletadas de seu aparelho com sua morte. Inclusive argumenta que o governo poderia encontrar sua localização de outra forma.

As denúncias referentes a governos espiando jornalistas através do Pegasus não são novas. Em 2016, uma primeira versão do programa foi descoberta. Seu método de invasão era através de *spear-phishing*, ou seja, mensagens de textos ou e-mails que induzem o alvo a clicar em um link malicioso.

Por essa razão, organizações uniram forças para verificar se o governo de Enrique Peña Nieto havia invadido as comunicações. O projeto foi levado pela Escola Munk de Assuntos Globais da Universidade de Toronto, *Citizen Lab* e o *The New York Times* em 2017. Ao final, as suspeitas iniciais foram confirmadas. Desse modo, Carmen Aristegui e outros jornalistas mexicanos registraram uma queixa legal contra a NSO no ano de 2018, em Israel.

Primeiro-ministro de Israel, Benjamin Netanyahu, visita o presidente do México Enrique Peña Nieto, em 14 de setembro de 2017 [Presidência do México]

NSO GROUP: DE PEQUENA STARTUP A LÍDER DO MERCADO

Contando com mais de 500 pesquisadores, a NSO pode identificar as vulnerabilidades dos *smartphones* e aperfeiçoar sua técnica espiã. Em 2014, a empresa dedicou-se ainda mais em desenvolvimento científico após vender setenta por cento de suas ações ao fundo de investimentos privados *Francisco Partners* por 120 milhões de dólares[13]. Nada parecia ser capaz de frear esse sucesso até o jornalista saudita ser assassinado em Istambul[14].

Para recuperar-se do escândalo, o fundo de investimento privado Novalpina comprou a empresa de tecnologia em 2019. Nessa nova etapa, a *startup* de outrora agora estaria comprometida com os princípios da ONU sobre negócios e direitos humanos.

Dois anos depois, a NSO lançou seu primeiro relatório de "Transparência e Responsabilidade", antecedendo em alguns dias a publicação do *The Pegasus Project*. Segundo o documento, mais de 300 milhões de dólares em contratos foram rejeitados, pois os compradores não aderiam aos padrões internacionais de direitos humanos. Mais cinco contratos teriam sido cancelados pelo mesmo motivo.

Diante do relatório exposto pela *Forbbiden Stories*, a defesa da NSO foi o ataque. A nota oficial divulgada em seu site questiona a confiabilidade do documento, pois estaria "repleto de suposições equivocadas e teorias não verificadas"[15].

A NSO declara que vendeu o *malware* para sessenta clientes em quarenta países, porém se recusa a identificá-los. Reitera que não tem acesso às informações extraídas dos alvos por seus consumidores. Também enfatiza que o fato de um número aparecer na lista divulgada não significa que tenha sido vigiado pelo Pegasus.

O Chipre é um dos três países em que a NSO está legalmente instalada. Inclusive, a lista de números sob poder do consórcio jornalístico foi obtida de seus servidores nesse país. Em resposta, a nota oficial da empresa

reportou não possuir nenhum servidor na ilha. Também argumenta que a alta quantidade de alvos potenciais não condiz com o real funcionamento do Pegasus.

"O compromisso da NSO com os direitos humanos está mais para um exercício de relações públicas que qualquer tentativa significativa de mudança de rumos. Seu relatório de transparência atual parece uma propaganda", rebateu Dianna Ingleton, diretora da *Anistia Tech*. "Por que continuam atacando a sociedade civil e tentando silenciar nos julgamentos?", completou.

No dia em que *The Pegasus Project* foi lançado, a *Amazon Web Services* derrubou a conta da NSO. "Nossas tecnologias estão sendo usadas todos os dias para quebrar círculos de pedofilia, tráfico de drogas, exploração sexual, localizar crianças desaparecidas e sequestradas, localizar sobreviventes presos sob edifícios desmoronados e proteger o espaço aéreo contra a penetração disruptiva de drones perigosos. Em suma, o Grupo NSO está em uma missão de salvar vidas, e a empresa executará fielmente esta missão sem se deixar intimidar, apesar de toda e qualquer tentativa contínua de desacreditá-la por falsas razões."[16] rebateu a nota.

A NORMALIZAÇÃO COM ISRAEL ATRAVÉS DA INDÚSTRIA MILITAR

Nas palavras do diretor de Empreendedorismo e Tecnologia do Ministério das Relações Exteriores, Andy David, "o mundo se vira contra nós em alguns momentos e há muitos atores querendo trabalhar contra nós. A tecnologia é uma ferramenta para sobressair-nos e fazer a diferença". O tom de sua entrevista de 2018 demonstra que existe um esforço em consolidar o título de Israel como "Nação de *Startups*" e "Nação da Inovação" por parte do Estado, que há pouco tempo era comandado pelo primeiro-ministro Benjamin Netanyahu. Ele mesmo já havia declarado estar buscando dentro do governo a maneira de que esses sistemas pudessem promover os interesses econômicos e diplomáticos[17].

Porém não é de hoje que Israel realiza intercâmbios de venda de armas por benefícios diplomáticos. Desde os surgimentos do enclave, o primeiro-ministro daquele momento, David Ben Gurion, investiu fortemente na indústria bélica como forma de se proteger. Os negócios expandiram, já não sendo completamente absorvidos pelo mercado local, levando à exportação, inclusive algumas duvidosas. Em 1959, Ben Gurion aprovou vender 250 mil morteiros israelenses para diversas partes, entre eles, a Alemanha Oriental. Diante das críticas, afirmou que "Israel venderia armas para países estrangeiros em todos os casos em que o ministério das Relações Exteriores não tivesse objeção"[18].

Naquela mesma década, os três principais pilares do governo da ocupação israelense possuíam sua própria indústria de armas: as Indústrias Militares Israelenses (IMI), a Indústria Aeronáutica de Israel (IAI) e a Rafael. Posteriormente, as empresas foram se desmembrando entre empresas privadas de alta tecnologia militar e eletrônicos como a Tadiran, El Op, Elbit e outras.

O embargo militar imposto pela França em resposta a guerra de anexação de 1967 incentivou a indústria local a crescer quatro vezes nos três anos subsequentes. Nas décadas de setenta e oitenta, o setor se ampliou e modernizou tornando-se um que mais empregava em Israel.

É importante frisar que os compradores da indústria de armas israelenses não se baseiam apenas no desenvolvimento tecnológico delas, senão também no selo de qualidade "testada em campo pelo exército israelense". Possivelmente, esse configura como sendo o elemento principal que permitiu o sucesso dessa "diplomacia Uzi' – em alusão à submetralhadora israelense que se tornou a favorita entre as forças de segurança ao redor do mundo na década de 60. Com o tempo, conseguiram aperfeiçoar a prática de oferecer materiais bélicos e treinamentos com forma de iniciar uma aproximação com regimes[19] que normalmente se recusariam a manter relações diplomáticas.

Nesse sentido, a NSO recebeu autorização do governo da ocupação israelense para tentar vender seu principal produto aos sauditas em 2017.

O acordo era sigiloso e terminou culminando na compra por 55 milhões de dólares. A revelação do contrato levantou suspeitas sobre as intenções diplomáticas de Israel serem de usar o software para causar tumultos políticos e permitir o acesso de governos antidemocráticos à sua tecnologia.

Naquele ano, Shalev Hulio viajou a Riyadh sem cumprir com os requisitos necessários a qualquer cidadão israelense que vá para aquele país. Mesmo sendo uma falta grave fazer esse trajeto sem prévia autorização, o dono da NSO não sofreu nenhuma punição.

Em resposta, o advogado da empresa declarou que "a NSO é uma companhia privada. Não é uma 'arma da diplomacia israelense", muito menos uma porta dos fundos do serviço de inteligência de Israel e não é conduzida por nenhum líder o governo[20].

O Ministério da Defesa de Israel se defendeu afirmando que comercializa e exporta produtos cibernéticos de acordo com o Decreto de Controle de Exportação da Defesa de 2007. Com base nele, as decisões são tomadas pensando na segurança nacional e em considerações estratégicas que incluem o cumprimento de acordos internacionais. Concluiu enfatizando que "Israel não tem acesso à informação coletada pelos clientes da NSO".

Por outro lado, quando nos perguntamos como o programa foi concebido, devemos notar qual foi a grande escola das *startups* de inteligência de Israel. A Unidade 8200, parte das Forças de Inteligência Israelense, é responsável por coletar sinais de inteligência (SIGINT) e de criptografia. A unidade é composta principalmente por jovens de 18 a 21 anos, mais os cursos livres ministrados para adolescentes. Depois de cumprir o serviço militar, muitos jovens lançam suas próprias empresas.

Em 2014, 43 soldados da reserva escreveram para Benjamin Netanyahu e os chefes das forças armadas denunciando a coleta abusiva de informações de palestinos nos territórios ocupados por parte da unidade. Afirmavam que o uso desse tipo de espionagem servia para planejar bombardeios que terminam em mortes de civis e dividem a sociedade palestina por meio de chantagem.

POSSÍVEIS PERSPECTIVAS

Quanto ao caso da extradição de Tomás Zerón, peça-chave para que as famílias dos 43 desaparecidos possam saber o que aconteceu com seus entes queridos, continua sem avanços. Dias antes que fosse emitida sua ordem de apreensão, Zerón escapou do México. Sua fuga começou no Canadá, porém ele conseguiu voar para Israel em meio à pandemia de covid-19. México e Israel não possuem um acordo mútuo de extradição.

Segundo uma reportagem publicada no *The New York Times*[21], um alto funcionário diplomático afirmava que não estavam empenhados com a extradição de Zerón ao México. O motivo seria a atual postura do país latino-americano na ONU ao criticar a repressão da ocupação israelense contra o povo palestino, principalmente na última guerra de 2021 contra Gaza.

O embaixador israelense no México negou que essa fosse uma resposta oficial ao caso. Alega-se que o pedido de extradição interrompeu a solicitação anterior de asilo feita por Zerón e ambos processos estavam parados. Ao vencer seu visto de turista, Tomás Zerón solicitou asilo político justificando que as acusações eram falsas e se tratava de uma retaliação da atual presidência contra seus predecessores. Também destaca o fato de os dois governos não terem um tratado mútuo de extradição como elemento complicador[22].

Para o subsecretário de direitos humanos do México, Alejandro Encinas, são os múltiplos contatos de Zerón com empresas de segurança israelenses muito poderosas que estariam lançando mão de suas influências para protegê-lo.

Sobre os crimes de espionagem cometidos pelo mau uso do Pegasus no México, as promessas são de garantir que o produto não seja mais adquirido e que os culpados sejam penalizados. Ainda que o nome do próprio presidente do México, André Manuel López Obrador (AMLO) e outras cinquenta pessoas próximas apareçam na lista do consórcio jornalístico, disse não estar surpreendido. Justificou que já era espionado pelos sucessivos governos desde muito antes.

Os resultados ainda são inconclusivos sobre se o monitoramento persistiu no mandato de AMLO ou não. Em 2019, novas denúncias são feitas pelos pesquisadores da *Citizen Lab*, WhatsApp e organizações civis (como a R3D). Nessa nova versão, o ataque acontece com uma simples ligação de WhatsApp, que sequer precisa ser atendida para ser ativada. Muitos dos telefones infiltrados estavam no México[23].

No ano seguinte, a Secretaria de Segurança e Proteção Cidadã (SSPC) corroborou que a licença do software de espionagem havia expirado em 2017 e não havia sido renovada pelo governo federal. Portanto, o Pegasus não deveria estar operando em território nacional. Ainda assim, segundo a peritagem a *Citizen Lab*, oito agências de segurança utilizaram essa tecnologia e duas ainda usam[24].

Primeiro-ministro de Israel, Benjamin Netanyahu, visita o presidente do México Enrique Peña Nieto, em 14 de setembro de 2017 [Presidência do México]

CONCLUSÃO

Se a própria utilização de espionagem para combater ao crime já não demandasse um enorme debate ético, o fato dessa tecnologia ser desenvolvida, testada e aprimorada às custas de uma colonização intensifica a problemática. Sob a proteção oferecida pelo argumento de que Israel precisa investir em segurança porque está cercado de inimigos, sua indústria bélica se desenvolveu a ponto de ser exportada para todo o mundo. Dessa maneira, um círculo vicioso é montado, em que a comunidade internacional consome sua tecnologia e treinamentos, atraídos pelo selo de qualidade de haver sido testado em campo, e que Israel tenha que criar e provar seus produtos ao tentar silenciar pela coerção o direito inalienável de autodeterminação do povo palestino.

Refletir sobre a origem de tais artigos de exportação não é um simples detalhe técnico, pois esses produtos estão moldados na compreensão da realidade dos envolvidos. Se o conceito de inimigo concebido pelos criadores do sistema está carregado de preconceitos contra aqueles que se levantam contra um regime, ele pode ser perigosamente replicado pelos seus clientes. Esse é o resultado do que vemos com todas as investigações feitas em torno do sistema Pegasus; o que deveria ser usado para proteger a todos de certos indivíduos começa a afetar aqueles que são considerados problemas para o próprio governo.

O que podemos observar é que por mais comprometidas com os direitos humanos que empresas como NSO Group dizem querer ser, seus mecanismos ou até interesse em assegurar que seu produto não seja usado de maneira arbitrária demonstra a fragilidade dessa aposta como solução em termos de segurança. Sistemas como o Pegasus outorgam aos seus possuidores a escolha do que é certo e o que é errado em termos de segurança e espionagem, sem nenhum mecanismo capaz de moderar as ações solicitadas. Considerando que uma empresa israelense necessita do aval do Ministério da Defesa para vender *spywares*, quem realmente, e de acordo com quais critérios, escolhe quais são os governos em condições de fazer um uso correto do produto?

Embora inúmeras reportagens profundas venham sendo feitas com o intuito de revelar toda a saga de Pegasus pelo México, ainda há muito para ser descoberto. Parte considerável das evidências não devem mais existir ou serem possíveis de rastrear. Casos históricos como o de Ayotzinapa necessitam dessas evidências para encontrar respostas. O próprio exemplo de Ayotzinapa requer nesse momento que Israel extradite um ex-funcionário público que sonhava em aplicar sua tecnologia espiã por todo o país. Ou seja, são demasiados interesses entrelaçados e nenhum comprometimento real com a verdade e a justiça do ponto de origem do problema. Por fim, como um país como o México pode se assegurar que o sistema já não esteja sendo operado – principalmente contra advogados, ativistas e jornalistas?

Notas

1. Formada em Letras, pela Universidade de São Paulo e estudante de jornalismo na Universidade Metodista de São Paulo.

2. Startup criada por três ex-soldados israelenses, sendo um deles ex-Mossad, sua sigla faz referência às iniciais de Shalev Hulio, Omri Lavie e Nivi Carmi. Hoje, uma das maiores empresas do setor.

3. O trabalho colaborativo foi resultado da união de dezessete organizações jornalísticas em dez países. Para o suporte técnico foi requerida a ajuda do Laboratório Técnico da Anistia Internacional. O consórcio revelou que 180 jornalistas e 85 defensores dos direitos humanos em todo o mundo foram escolhidos para figurar em uma lista de possíveis alvos do spyware.

4. CAMACHO, Zósimo. Calderón autorizó a Sedena la compra de Pegasus. Contralínea. 2021. Disponível em: https://contralinea.com.mx/calderon-autorizo-a-sedena-la-compra-de-pegasus/ Acesso em: 25 de julho de 2021.

5. Durante o mandato de EPN, o grupo Tech Bull vendeu a AIC um pacote de 500 infecções de celulares com Pegasus por 32 milhões de dólares.

6. TOURLIERE, Mathieu. Los tentáculos del abuso de EPN y la opacidade em la 4T. Disponível em: https://www.proceso.com.mx/reportajes/2021/7/26/los-tentaculos-del-abuso-de-epn-la-opacidad-en-la-4t-268565.html Acesso em: 26 de julho de 2021.

7. Empresa que cobrou 489 milhões de pesos a PGR, SEDENA e CISEN (licenças Pegasus) entre 2015 e 2016

8. As dependências públicas contratantes foram: Secretaria de Segurança Pública, Marinha, Defesa Nacional, Secretaria de Governo (SEGOB), Instituto de Formação Policial, Comissão Nacional de Água (CONAGUA), Secretariado Executivo do Sistema Nacional de Segurança Pública, Banco Nacional de Obras e Serviços Públicos, Tesouraria da Federação, entre outras. Os governos que comparam o malware foram: Veracruz, Estado do México e Colima.

9. Foi um órgão administrativo desconcentrado da antiga Procuradoria Geral da República (PGR)

10. Nos e-mails vazados pelo Wikileaks em 2015, a empresa Hacking Team apontava Zerón como “peça-chave” e “cliente definitivo” pela transnacional. Porém, insiste em comprar com a concorrente israelense ainda que o Pegasus fosse mais caro.

11. O montante foi revelado em 2017 por Carmen Aristegui, uma das principais jornalistas investigativas do México. Ela, seu filho menor de idade e alguns colegas haviam sido vigiados pelo software israelense.

12. EL GIEI fue espiado con Pegasus, confirma Citizen Lab. Animal Político. 2017. Disponível em: https://www.animalpolitico.com/2017/07/giei-espionaje-pegasus-nyt/. Acesso em: 10 de julho de 2017.

13. LAKHANI, Nina. Mexico world’s deadliest country for journalists, new report finds. The Guardian. 2020. Disponível em: https://www.theguardian.com/world/2020/dec/22/mexico-journalists-deadly-cpr-press-freedom. Acesso em: 22 de dezembro de 2020.

14. A empresa apenas regressa inteiramente às mãos dos dois sócios originais em 2019 - depois da nova aposta no gerenciamento de imagem coordenado pela Novalpina.

15. O jornalista saudita Jamal Khashoggi foi morto dentro do consulado em Istambul em 2018. Ele e pessoas próximas haviam sido vigiadas pelo sistema Pegasus.

16. FOLLOWING the publication of the recent article by forbidden stories, we wanted to directly address the false accusations and misleading allegations presented there. NSO Group. Disponível em: https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/.

17. Ibdem

18. SOLOMON, Shoshanna. Israel finds tech prowess a useful tool to burnish international image. The Times of Israel. 2018. Disponível em: https://www.timesofisrael.com/israel-finds-tech-prowess-a-useful-tool-to-burnish-international-image/. Acesso em: 5 de dezembro de 2018.

19. FRIEDMAN, Thomas L. How Israel’s economy got hooked on selling arms abroad. The New York Times. 1986. Disponível em: https://www.nytimes.com/1986/12/07/business/how-israel-s-economy-got-hooked-on-selling-arms-abroad.html. Acesso em: 7 de dezembro de 1986.

20. Por exemplo, os Emirados Árabes Unidos (EAU) normalizaram suas relações com Israel (nos chamados Abraham Accords) após tornarem-se clientes de empresas de segurança como a NSO. O país também foi apontado em escândalos relacionados ao uso do Pegasus para espiar ativistas, como o caso de Ahmed Mansoor.

21. PEGASUS Project turns spotilight on spyware firm NSO’s ties to Israeli state.The Guardian. 2021.Disponível em: https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state. Acesso em: 20 de julho de 2021.

22. LOPEZ, Oscar e BERGMAN, Ronen. Former Official Wanted by Mexico Takes Refuge in Israel. The New York Times. 2021. Disponível em: https://www.nytimes.com/2021/07/15/world/middleeast/israel-mexico-zeron-extradition.html. Acesso em 15 de julho de 2021.

23. Outro foragido mexicano que escapou para Israel foi o escritor e comunicador Andrés Roemer. Acusado de estupro e denunciado por cerca de 60 mulheres, possui uma ordem de busca e apreensão pela Interpol.

24. MONROY, Jorge.15,000 números telefónicos de México fueron detectados en lista de malware de espionaje Pegasus: The Guardian. El Economista. 2021. Disponível em: https://www.eleconomista.com.mx/politica/15000-numeros-telefonicos-de-Mexico-fueron-detectados-en-lista-de-malware-de-espionaje-Pegasus-The-Guardian-20210718-0025.html. Acesso em: 18 de julho de 2021.

25. TOURLIERE, Mathieu. Continúa el espionaje en tiempos de la 4T, denuncia Citizen Lab. Proceso.2020 Disponível em: https://www.proceso.com.mx/nacional/2020/12/1/continua-el-espionaje-en-tiempos-de-la-4t-denuncia-citizen-lab-253706.html. Acesso em: 1 de dezembro 2020.

MEMO

MONITOR DO ORIENTE MÉDIO

monitordooriente.com

/monitordooriente

/monitordoorient