A repressão importada no Médio Oriente

Um documento do ministério do interior em que se laçava um pedido de propostas de cibervigilância para o combate à blasfémia, ao sarcasmo e à 'falta de moralidade' no Egito, foi revelado ao público em Junho de 2014 – a tecnologia viria provavelmente do ocidente. Max Gallien reporta.

Quando os protestantes egípcios entraram pelos edifícios do governo adentro no pico da revolução de 2011, deram com eles a lidar com pilhas de papel rasgado e ficheiros despedaçados. O que não tinha sido já destruído eles começaram a fotografar e a pôr *online*, criando uma olhadela fascinante para o que se passava dentro do estado de segurança egípcio. Um dos documentos tornados públicos em 2011 incluía uma oferta feita por um grupo com base no Reino Unido chamado "Gamma Group" para um programa de *spyware* entitulado "FinFisher" pelo preço de cerca de um quarto de milhão de libras. "FinFisher" permite ao utilizador infetar computadores remotamente e monitorizar comunicações bem como informação encriptada, ler emails, ouvir conversas no *Skype* e até instalar *software* remotamente. Documentos tornados públicos sugeriam que os serviços de segurança egípcios até tinham recebido uma versão de demonstração gratuita do *software*, e que tinham ficado muito impressionados com os resultados, contudo a *Gamma International* rapidamente negou que tivesse alguma vez vendido o *software* total ao governo egípcio.

Em junho de 2014, uma revelação deveras estranha reacendeu o debate acerca dos programas

egípcios de cibersegurança. O jornal egípcio "Al-Watan" publicou um pedido de propostas emitido pelo Ministério do Interior em maio, pedindo a companhias de inteligência para submeterem propostas para um sistema novo de cibermonitorização. Os esboços da visão do Ministério do "Social Networks Hazard Monitoring System": o programa deverá ser capaz de fazer buscas muito abrangentes por plataformas de *social media*, incluindo *Facebook*, *Youtube* e *Twitter*, e irá colecionar informação daqueles envolvidos tanto em violações da lei como – e esta é a frase chave – em 'ideias destrutivas'. É interessante que o documento chega a oferecer uma lista do que considera ser ideias destrutivas, incluindo entre outros: a blasfémia e o ceticismo na religião, o espalhar de rumores e a distorção intencional dos fatos, o sarcasmo, o uso de palavras inapropriadas, a chamada à partida de pilares da sociedade (um eufemismo claro para os militares), o convite a demonstrações, a pornografia, a falta de moralidade, a chamada à normalização das relações com os inimigos e o contorno da estratégia do estado a este respeito.

Dado o nível de perícia que o judiciário egípcio tem demonstrado no passado, usando acusações vagas tais como 'espalhar notícias falsas' e 'dividir o país' para assediar e processar jornalistas e ativistas, não há dúvida alguma que a existência de tal programa de vigilância no Egito, se o seu pedido de propostas viesse a ter resposta, seria um vale tudo gigante para o aparato de segurança do estado, e um golpe fatal na liberdade de expressão.

Os grupos de direitos humanos no Egito e pelo mundo afora protestaram contra o plano do Ministério do Interior e apontaram para as garantias da liberdade de expressão e de privacidade (art. 57º, 73º) na Constituição egípcia nova.

Há, no entanto, mais perguntas por responder no que concerne à fuga de informação acerca da chamada para propostas, mais concretamente a questão de como isto pode ter acontecido em primeiro lugar. O *El-Watan* não é mesmo conhecido por nenhum tipo de ativismo de oposição, e a possibilidade de publicar documentos classificados do Ministério do Interior de modo independente parece no mínimo surpreendente.

Muito provavelmente, a fuga foi outro de muitos exemplos em meses recentes de que o aparato de segurança do Egito não se importa de manter o público informado acerca dos seus métodos, esperando que sirva para intimidar e desencorajar ativistas, ou mais alguém que tenha planejado "distorcer os fatos intencionlmente" na *internet*.

Repressão Importada

Um dos aspetos mais importantes do debate acerca da chamada de propostas revelados ao público é que, se tivesse sido respondida, todas as ofertas iriam provavelmente ter vindo de companhias europeias ou norte-americanas. Aliás, a Europa e os EUA têm-se tornado nos principais fornecedores de *software* de vigilância não só do Egito mas também da Arábia Saudita, Burma, e outros regimes repressivos pelo mundo afora. A apropriadamente chamada "Hacking Team" (Equipa de Pirataria) está sediada em Milão e tem aberto subsidiárias nos EUA e em

Singapura, a Trovicor opera a partir de Munique, a *BlueCoat* tem a sua sede em Sunnyvale na Califórnia enquanto a *Gamma Internacional* é parte da *Gamma Group*, sediada no Reino Unido.

À primeira vista, poder-se-ia sugerir que não há nada de errado com isto, e que o *software* de vigilância é um bem legitimamente exportável. Decerto que, numa era em que os criminosos e os grupos subversivos armados têm começado a usar a *internet* cada vez mais tanto para se organizar como para recrutar novos membros, os governos deveriam ser capazes de ocasionalmente invadir a privacidade digital de um indivíduo de modo a garantir a sua própria segurança. É o mesmo argumento que pede que os governos possam ser capazes de invadir a esfera privada de um cidadão, e a mesma justificação legal que se aplica a companhias que providenciem *spyware* para os serviços de segurança governamentais.

De qualquer modo, após uma análise mais cuidada, esta analogia falha redondamente. Antes de mais, para que um programa de invasão da privacidade em nome da segurança enquanto ferramenta de defesa, é preciso que este venha com salvaguardas legais vigorosas e o devido processo legal, muitas das quais não estão presentes ou são descaradamente ignoradas em muitos dos países que estão aqui em causa. Sem salvaguardas legais, programas como o FinFisher tornam-se numa arma ofensiva, usada pelo estado para assediar e prejudicar os seus cidadãos através da vigilância sem justa causa e de procedimentos legais politicamente motivados. Ativistas tais como o *blogger* egípcio Maikel Nabil que foi sentenciado a três anos na prisão por postar “O exército e o povo nunca foram uma mão única” no *Facebook*, podem ser disto testemunhas.

E em segundo lugar, enquanto a chamada para guardiões o torna óbvio, este *software* não só é empregue como ferramenta para salvaguardar a segurança nacional, mas também para impor um código alegadamente ‘moral’. E este código não é uma interpretação evidente de valores tidos como universalmente observados: ele criminaliza o sarcasmo, a pornografia, e o ceticismo religioso. Em 2012, um outro *blogger* egípcio, Alber Saber, foi preso e sentenciado a três anos na prisão por “difamar o Islão e o Cristianismo” e por “espalhar o ateísmo” porque ele alegadamente partilhou o filme “A Inocência dos Islâmicos” no *YouTube*.

Armamento Digital

Há uma analogia física mais apropriada para o software de ciber vigilância: armas. Um conjunto largo de restrições ao comércio nacional e internacional foi criado para limitar a venda de armas a regimes repressivos, exatamente porque as armas podem ser usadas só como uma ferramenta de defesa para assegurar a defesa nacional, mas como uma ferramenta ofensiva para assediar e prejudicar os cidadãos, e para impor um código moral que poderá não ser congruente com a Declaração Universal dos Direitos Humanos. Se os mesmos perigos se aplicam a programas de cibervigilância, então também devem aplicar-se às mesmas restrições de comércio. Não há razão porque um regime em que não se possa confiar com armas possa ser confiado com ferramentas que permitam espiar os seus próprios cidadãos.

Tem havido uma atenção do público e um ativismo crescentes quanto a este ponto, e alguns governantes têm tomado primeiros passos cautelosos nesta direção, incluindo o Reino Unido que em 2012 limitou a exportação do *FinFisher* do *Gamma Group*. Contudo, acordos internacionais mais latos acerca disto deveriam seguir-se, sujeitando a exportação de tecnologia de ciber vigilância às mesmas restrições de exportação que se aplicam a tanques e a espingardas. Enquanto isto poderia certamente ser um obstáculo a uma indústria que se estima render 5 biliões de dólares americanos, é preciso pôr isto na balança com o sofrimento real das populações sob regimes repressivos pelo mundo afora por causa da utilização ilegal e imoral da tecnologia de vigilância. Idealmente, um olhar mais próximo a como estes programas são usados poderia também levar a algumas novas conclusões acerca da exportação de *hardware* militar pelo mundo afora, enquanto o uso destas tecnologias poderia ser tratado como uma prova dos nove da sua credibilidade no que toca a caças.

Pelo sim pelo não, os regimes autoritários pelo mundo afora irão sempre encontrar acesso a tecnologia de vigilância. Mas se um dia as restrições de exportação proibissem os fornecedores mais avançados e sofisticados de cibervigilância de atender a pedidos de propostas tal como a emitida pelo governo egípcio em 2014, isso certamente seria um grande passo na direção certa.

Max Gallien pertence ao programa Dahrendorf no *St. Antony's College*, fazendo o seu *MPhil* em Estudos do Médio Oriente.

Publicado em:Agosto 1, 2014