ATAQUE CIBERNÉTICO, ANO ELEITORAL E OS MEIOS DE COMUNICAÇÃO

Daniel Laufer e Maria Francisca Accioly

No Brasil, o ano de 2022 será marcado por disputas eleitorais novamente acirradas diante da flagrante polarização no cenário político. O recente regramento jurídico eleitoral e as eleições ocorridas em 2018 e em 2020 dão conta de que as ferramentas mais utilizadas pelos candidatos serão as redes sociais ancoradas na rede mundial de computadores bem como a imprensa por meio do rádio e da televisão.

Em sendo a imprensa responsável pela propagação da informação, deve ela estar segura no que tange a incidentes cibernéticos, tendo em vista que não é de hoje que os invasores interrompem programações, propagam falsas notícias e mensagens, sequestram dados sensíveis e vazam informações sigilosas, trazendo prejuízos às diversas redes televisivas. Há exemplos como o (i) do canal francês TV5Monde que sofreu ataque hacker do Estado Islâmico em abril de 2015, deixando seus canais fora do ar e mensagens ameaçando soldados franceses foram publicadas nas redes sociais do TV5, (ii) do site espanhol EL PAÍS, a partir de doze intervenções massivas, oriundas de países como China e Turquia, impediram o acesso às notícias do jornal durante duas horas e meia, em outubro de 2017, com notório intuito político, (iii) em outubro do ano de 2021, da segunda maior rede de TV dos EUA, a Sinclair Broadcast Group, proprietária de estações afiliadas à Fox, ABC e The CW, foi tirada do ar após sofrer um ataque ransomware, cujo sequestro de dados sensíveis teve como objetivo atingir grandes empresas e também o governo americano e, mais recentemente, (iv) em janeiro do corrente ano, do conglomerado da mídia portuguesa, Grupo Impresa, que foi alvo de um ataque hacker no qual os inscritos nas newsletters do jornal Expresso receberam uma nota com o título "BREAKING Presidente afastado e acusado de homicídio", que continha

afirmações falsas e links potencialmente perigosos. O ataque ao grupo Impresa partiu da mesma organização que, em dezembro de 2021, assumiu a autoria do ataque ao site do Ministério da Saúde do Brasil e ao aplicativo ConecteSUS.

Ao que se tem notícia, um dos primeiros ataques por hacker noticiado no mundo com viés político se deu em 1987 quando dois canais de televisão, WGN e WTTW, da cidade de Chicago, tiveram os sinais sequestrados seguido da invasão da transmissão por uma pessoa trajando uma máscara e definindo determinado comentarista esportivo como um “maldito liberal”.

Em mais de três décadas, a internet evoluiu na mesma proporção da perversidade humana e neste contexto os ataques cibernéticos aumentaram 220% no primeiro semestre de 2021. O FBI, por exemplo, cuida da investigação de cerca de 100 tipos de ataque hacker ransomware atualmente conhecidos. Aliado a este contexto a pandemia de COVID-19 acarretou um número maior de pessoas trabalhando remotamente e, assim, tornando os sistemas de algumas empresas mais “abertos”, sensíveis e vulneráveis.

Do ponto de vista normativo, o governo brasileiro foi leniente ao levar mais de 20 anos para aderir à Convenção de Budapeste, responsável por traçar medidas de cooperação internacional direcionadas à segurança cibernética e ao enfrentamento dos crimes cometidos por meio da rede mundial de computadores. Apenas agora, em dezembro de 2021, o Senado Federal aprovou o Projeto de Decreto Legislativo n. 255/2021 e atualmente se aguarda a promulgação pelo Presidente do Congresso Nacional.

Já o agravamento das penas dos crimes de furto e estelionato praticados com o uso de dispositivos eletrônicos e aumentado a pena do crime de invasão de dispositivo informático, operado pela edição da Lei nº 14.155/2021, tende a não se tornar uma ferramenta apta a inibir os invasores e criminosos. Não é de hoje, nem tampouco uma particularidade brasileira, a certeza de que o recrudescimento da sanção penal não traz consigo um freio à prática delitiva.

A questão é maior e resultante da ausência de uma cultura de segurança informática que, por sua vez, facilita os ataques e fortalece os chamados “protestos digitais”. Os “apagões” momentâneos dos meios online afetam a circulação da informação, a legitimidade da imprensa, trazendo impacto financeiro às empresas jornalísticas pela impossibilidade de veicular a publicidade online, além do impacto de reputação e de imagem.

Assim, é imediata a necessidade de as empresas de telecomunicação promoverem um diagnóstico sério para prevenir ciberataques, através do mapeamento e avaliação dos riscos, com a devida qualificação do sistema interno, compreender a vulnerabilidade de seus sistemas, identificar os pontos sensíveis, verificar quais técnicas de segurança estão implementadas, qual o sistema de comunicação entre as áreas de segurança e desenvolvimento (TI), sopesar se a empresa tem capacidade para assumir internamente ou se faz necessário contratar terceiros para essas avaliações.

Ao lado da prevenção, a empresa precisa estar preparada para a reação imediata em caso de invasão eletrônica, com a devida comunicação tempestiva de incidentes e interações com as autoridades, tudo a fim de coibir ou minimizar as perdas financeiras, de reputação e de imagem da empresa, assegurando as informações e protegendo os dados que o invasor queira utilizar para chantagear ou expor o meio de comunicação.

O ano eleitoral aflora a outra face dos avanços tecnológicos da maximização da circulação da informação online. Debates ideológicos podem trazer reações radicais e os chamados “protestos digitais” desaguarem em ataques cibernéticos nunca vistos no país. Como dito acima, a adoção de uma cultura de segurança informática, resumida nas ações “prevenção” e “reação”, se apresenta como o efetivo caminho a ser seguido.

Daniel Laufer, 42, Doutor em Direito (PUC-SP) e advogado criminalista
Maria Francisca Accioly, 38, Mestre em Direito (UFPR) e advogada criminalista