Como a pericia digital contribuiu com o caso Marielle?

A computação forense, destinada a análise de dispositivos informáticos para se apurar a materialidade (se um fato ocorreu) e a autoria (quem foi o responsável) tem sido muito exigida para o esclarecimento de crimes no Brasil.

Como visto a área é crescente e praticamente está relacionada com a grande maioria dos casos judiciais, de processos trabalhistas a criminais, passando por problemas cíveis. O avanço das técnicas de análise de tráfego, data carving e análise de sistemas operacionais de celulares permitem a reconstrução de cenários e identificação de artefatos que podem se tornar indícios e até evidências de um crime.

Os peritos em informática hoje podem se especializar em diversas frentes, como a perícia em rede, em banco de dados, mobile forensics e até IOT forensics, destinada análise de dispositivos e eletrodomésticos conectados e que podem ser invadidos ou registrar evidências de um fato relevante a um Tribunal.

No caso Marielle, a polícia investigou aproximadamente 700 GB de dados, iniciando pela análise do sinal dos equipamentos e registros das Estações Rádio Base, antenas

espalhadas na cidade.
Assim, cada celular nas ERBs da “rota do crime” ou “célula” foram considerados
de início. Foram rastreadas 2.428 torres no trajeto da vitima. Após, a polícia
informa que conseguiu “analisar remotamente” estes equipamentos, sem busca e apreensão dos
mesmos, mas “quebra de dados telemáticos”.

O rastreamento trouxe uma
quantidade muito grande de telefones, 33 mil linhas, onde os peritos digitais
tiveram que refinar o numero de celulares analisados. Neste contexto, diante da
luz de um celular no carro dos suspeitos, focou sua atuação na ERB ligada àquela
região. As empresas de telefonia registram os IMEIS, códigos dos celulares
identificados e autenticados em uma ERB, o que permite traçar até mesmo sua
mobilidade e geolocalização.

A partir deste ponto a polícia
pediu a quebra de sigilo de dados de um suspeito e a partir do acesso ao
dispositivo, identificou registros de histórico de navegação ligados ao fato.
Diante de um crime onde arma e carro jamais foram encontradas, é a evidência
digital a responsável por fim a sensação de impunidade e ao mistério do crime,
pelo menos a princípio. Esses são apenas alguns artefatos que podem ser
coletados e após uma minimização de dados e análises de correlação,
solucionarem fatos e crimes. A cada dia que passa, torna-se cada vez mais

difícil não deixar rastros digitais. Mais difícil ainda é apagar tais dados.

Agora imagine se as empresas de telefonia não registrassem os dispositivos que autenticam numa ERB? Imagine aquele dispositivo "pirata" que spoofa (esconde) seu imei? Ou imagine um provedor que se recusasse em fornecer dados a partir da quebra de sigilo? Imagine ainda um processo de compra de celular ou chip onde o fraudador, com apoio de colaboradores da operadora, faz o cadastro em nome de terceiros?

Infelizmente, ainda existem, questões *Zero Knowledge System*, onde criminosos mais preparados poderiam dificultar a coleta de evidências ou mesmo utilizar dispositivos de laranjas. Felizmente, de Lei Proteção de Dados se torna aplicável em 2020 exigirá "exatidão" de cadastros e maior rigor no tratamento de dados que são essenciais para investigação de crimes e repressão a fraudes.

José Antonio Milagre é Advogado, especialista em Crimes Digitais, Mestre e Doutorando pela UNESP, fundador do IDCI – Instituto de Defesa do Cidadão na Internet e Presidente da Comissão de Direito Digital da OAB/SP Regional da Lapa www.youtube.com/josemilagre