PERÍCIA EM EVIDÊNCIA

Dualidade da tecnologia forense: uma batalha entre o bem e mal

Hoje existem diversas ferramentas para monitoramento de pessoas. O emprego que faremos delas e a regulamentação jurídica assumem um papel relevante e despertam a atenção de defensores de direitos humanos em vários países

Cássio Thyone Almeida de Rosa
4 de agosto de 2020

DIVULGAÇÃO

> UFEDs apresentam-se na forma de maletas portáteis e são capazes de extrair dados de praticamente todo tipo de telefone celular para fins de investigação forense

Peço licença aos leitores para inverter a ordem dos assuntos tratados nesta coluna. Em meu último artigo, adiantei que teríamos a segunda parte do tema "*O Perito é a última voz da vítima, mas não apenas dela*". Na sequência, traremos a parte final prometida.

Desde a última semana, um assunto repercutiu bastante na mídia: o envolvimento da Secretaria de Operações Integradas (SEOPI) no monitoramento de 579 servidores da área de segurança pública, declaradamente opositores do governo. Trabalho de inteligência? Trabalho investigativo?

Motivado por questões forenses, optei por entrar nessa discussão abordando a ferramenta que supostamente estaria sendo empregada no dito "monitoramento".

Alguns já devem ter ouvido falar das UFEDs. A UFED é a sigla em inglês para "*Universal Forensic Extraction Device*", ou, em nossa língua, Dispositivo Universal de Extração Forense. Muitos destes dispositivos apresentam-se na forma de maletas portáteis, maiores que uma maleta 007, e são capazes de extrair dados de praticamente todo tipo de telefone celular para fins de investigação forense.

Segundo a empresa fabricante, não apenas telefones podem ser acessados, mas também vários outros tipos de dispositivos móveis, incluindo aparelhos autônomos de GPS, abrangendo mais de oito mil modelos de diferentes marcas. Um UFED pode ler os dados tanto diretamente do dispositivo quanto de cartões SIM avulsos (chamados usualmente de *chips*). Basta conectar o aparelho ao UFED e, sendo detectado, muitas vezes de forma automática, as opções para "*quebra*" de senha e extração de dados são disponibilizadas. Salienta-se que mesmo os dados apagados, mas recuperáveis, são extraídos por padrão. A tecnologia para a remoção de senhas, sejam elas do tipo PIN, desenho de padrão ou por impressão digital ou facial, é mesmo impressionante, embora existam marcas e modelos específicos em que essa quebra é realmente quase impossível.

Do ponto de vista pericial, isso é perfeito. Muitos crimes já foram resolvidos graças a essa tecnologia. A capacidade de recuperar dados apagados intencionalmente pelos usuários, em especial, torna essa ferramenta uma importante aliada no combate ao crime.

Mas e quando pensamos na possibilidade de uma verdadeira interceptação de dados? Antes de tudo, é importante entender que o chamado "*grampo*" apenas pode ser realizado mediante autorização judicial e, em tese, qualquer prova obtida sem essa autorização estaria enquadrada no rol de provas ilícitas.

No caso específico, não acredito no emprego de UFEDs para a finalidade de monitoramento, uma vez que seria preciso estar com o dispositivo físico (aparelho celular ou seu cartão SIM) para extrair os dados. A interceptação de conversas ou trocas de dados digitais entre emissor e receptor é algo complexo. Nos dias atuais, a maior parte dessa comunicação é realizada de forma cifrada (criptografada), o que dificulta e até inviabiliza a obtenção desses dados.

Em casos onde existe autorização judicial, entra em cena outro tipo de recurso, conhecido nos meios policiais e de inteligência como "*Sistema Guardião*". Com a devida autorização judicial, o que se faz, na prática, é replicar o sinal de uma operadora telefônica que detém o número de um determinado usuário e, assim, as conversas e demais informações podem ser gravadas em um servidor das instituições ligadas a investigações, sejam policiais, governamentais ou militares.

A questão tratada aqui não é exclusiva para a segurança dos dados pessoais e da nossa própria privacidade. Outras questões muito relevantes envolvem o emprego de bancos de dados de DNA, assim como dados biométricos de identificação (impressões digitais entre eles). Todas são tecnologias fundamentais, mas que podem servir ao "*bem e ao mal*". O emprego que faremos delas e a regulamentação jurídica assumem um papel relevante. Muitos grupos defensores de direitos humanos em vários países têm chamado a atenção para tentativas de abusos e de um controle fora dos padrões aceitáveis por parte de governos totalitários, que passam a vigiar minorias, nos aproximando de distopias como "*1984*", de George Orwell.

Importa, assim, estarmos atentos contra o abuso de qualquer forma de invasão de nossa privacidade. Quanto ao emprego das tecnologias forenses, a escolha será sempre nossa! Façamos a opção pelo bem.

Cássio Thyone Almeida de Rosa
Graduado em Geologia pela UNB, com especialização em Geologia Econômica. Perito Criminal Aposentado (PCDF). Professor da Academia de Polícia Civil do Distrito Federal, da Academia Nacional de Polícia da Polícia Federal e do Centro de Formação de Praças da Polícia Militar do Distrito Federal. Ex-Presidente e atual membro do Conselho de Administração do Fórum Brasileiro de Segurança Pública

https://backup.forumseguranca.org.br/pericia-em-evidencia/template-multiplas-vozes-t2mgr-o6zzn-zjjuh-hi3nj-iycsx-vc35o-jes2f-p45gr-boopr-2ez42-eazzd-foepd-787sv-xqycn-hvmeu-qo7os-kan5a-kebep-iaxu4-k56jo-9meym