Luiz Sartori: Busca e apreensão em computador com programa espião é ilegal

Em um debate acadêmico, fui confrontado com a seguinte questão: O juiz pode decretar a busca e apreensão de documentos alocados em um dispositivo eletrônico, consignando que o seu cumprimento deva ocorrer por meio da utilização de um *malware*? É preciso esclarecer que, segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (Cert), os *malwares* "são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador". O exemplo mais popular de malware é o vírus, que infecta o computador e corrompe os conteúdos armazenados na memória. E há, também, os programas espiões. Pois bem, na ocasião, ainda sem muito refletir, respondi negativamente.

A época não vigorava a Lei 12.707/2012 (Lei Carolina Dieckmann), que, ao acrescentar ao Código Penal o artigo 154-A, tentou criar — mesmo que pecando na técnica — um tipo penal que criminaliza o acesso a sistemas computacionais mediante violação indevida de mecanismo de segurança (tal como ao utilizar um *malware*), bem como a disseminação destes a qualquer título. Passados alguns meses deste debate, conclui que realmente a busca e apreensão em um dispositivo eletrônico por meio da utilização de *malwares* seria absolutamente ilegal. Motivo: se vale deste meio absolutamente ilegal, ferindo de morte as garantias constitucionais como a não autoincriminação.

Segundo dispõe o artigo 240 do CPP, existem duas modalidades de busca: a domiciliar e a pessoal. Ambas as modalidades, não se nega, impõem a expedição de mandado judicial para viabilizar o seu cumprimento, posto ser inegável que estas, levadas a efeito, restringem garantias fundamentais, a saber, aquelas previstas no artigo 5.º, III, X e XII, da Constituição Federal.

É bem verdade que o próprio Código autoriza a busca e apreensão sem a expedição do competente mandado judicial (artigos 244 e 245). Contudo, trata-se de verdadeira exceção. E, ainda assim, mediante obediência a certas condições, sob pena de se macular a busca e, consequentemente, a apreensão com a pecha da nulidade. Cite-se, a esse respeito, a possibilidade de se proceder à busca e apreensão domiciliar sem o mandado judicial, notadamente quando o seu morador permite a entrada do executor da medida no local.

Contudo, para que uma busca e apreensão seja válida é preciso se atentar para diversos requisitos, não apenas relacionados à fundamentação da decisão judicial que expede o mandado como também àqueles de ordem prática, que dizem respeito ao seu cumprimento como, por exemplo, a ciência prévia do morador — ainda que seja no momento do cumprimento da ordem de busca e apreensão — acerca de quem pretende entrar em sua casa e o que visa buscar.

E daí o porquê da ilegalidade da busca e apreensão tendo como meio a utilização de um *malware*.

Nesta hipótese, haveria a insólita situação de o acusado sofrer uma busca e apreensão em seus dispositivos eletrônicos sem nunca ter ciência de sua ocorrência. Em consequência, teria o acusado e seu defensor que conviver com a dúvida acerca do quanto de informação de seu dispositivo eletrônico

tornou-se de conhecimento das autoridades. Sim, porque a depender do grau de sofisticação do código malicioso, a sua detecção torna-se quase impossível aos antivírus e demais programas dedicados a combater a ação desses programas.

A admissão deste modelo violenta infração a direitos fundamentais, na medida em que é negada a garantia da ampla defesa e do contraditório. Seria o mesmo que retroagir aos regimes ditatoriais, em que os algozes dos acusados escondiam provas sorrateiramente, justamente para neutralizar suas defesas. Hoje, a doutrina e a jurisprudência não admitem prova secreta.

Isto para não dizer que, ao se conceber uma busca e apreensão sem o conhecimento do acusado, abre-se margem para que provas sejam coletadas, sem que sejam consignadas em termo próprio. Fica, assim, o seu uso a cargo do acusador, ferindo de morte o princípio da paridade de armas.

Some-se a tudo isso que o eventual aceite desse meio de busca e apreensão, sem qualquer dúvida, mitigaria do princípio da não autoincriminação, notadamente em razão de inexistir meio de um *malware* infectar um sistema eletrônico sem que o seu legítimo usuário, de algum modo, ainda que inconsciente, permita.

É que os códigos maliciosos são sempre escamoteados, e.g. em e-mails, links, entre outros, sem alardear a sua existência, até porque, do contrário, infere-se que, se o acusado conseguisse ter a certeza de que o acesso ao e-mail ou link fosse propiciar o meio para que se procedesse uma busca e apreensão em seu dispositivo móvel, este possivelmente agiria de modo diverso.

Desta forma, inexiste espaço no ordenamento jurídico para sequer cogitar uma busca e apreensão em dispositivos eletrônicos por meio de *malwares*. Caso contrário, fica em xeque toda a lógica constitucional das garantias do acusado no processo penal, resumindo-as a letra morta, algo inconcebível em um Estado Democrático de Direito como o Brasil, que inclusive as eleva a cláusulas pétreas.

Date Created
22/11/2013