“VÃrus espiÃ£o” como meio de investigaÃ§Ã£o: a infiltraÃ§Ã£o por

Recentemente, o WhatsApp lançou nota[1] orientando seus usuários para que atualizassem a versão do aplicativo tendo em vista a descoberta de uma falha de segurança capaz de tornar vulnerável o aparelho utilizado. A falha possibilitaria a instalação remota de um *spyware* próprio para ter acesso a dados do aparelho. Diante de tais fatos, cabe a reflexão quanto às novas tecnologias digitais e como estas têm modificado procedimentos de investigação criminal. Seria possível o Estado investigador utilizar *softwares* para alcançar (fontes de) provas e assim incriminar pessoas? Quais seriam os limites dessa metodologia?

A utilização de *malware* na investigação criminal decorre do impacto significativo protagonizado pela informática no âmbito jurídico. O *malware* como método de obtenção de prova[2] é um *software* malicioso instalado clandestinamente pelo Estado em um sistema informático, uma ameaça destinada a quebra da confidencialidade e integralidade dos dados nele contidos[3]. Trata-se de um *software* previamente programado cuja função é infectar dispositivos para tornar possível o acesso remoto às informações, comunicações ou arquivos neles armazenados, ou, ainda, acessar suas funcionalidades, independentemente de estarem ativas ou não[4].

Após instalado, cria-se um portal de acesso (*backdoor*)[5] que possibilita uma comunicação entre o dispositivo monitorado e o centro de comando. Portanto, a utilização de *malware* nas investigações permite ao centro de comando um controle remoto capaz de realizar de maneira oculta o monitoramento, em tempo real, de áudio, vídeo, funções de microfone e câmeras, fluxo de dados e comunicações, memória e armazenamento e geolocalização do dispositivo móvel alvo, dentre outras funcionalidades por vezes disponíveis[6], como o acesso a senhas de usuários do sistema informático alvo, documentos, correio eletrônico e histórico de páginas da *web*[7].

2024 - www.conjur.com.br - Todos os direitos reservados.

Em alguns países como Espanha, Itália e Estados Unidos, já existem casos de uso da metodologia investigativa, contudo, diversas são as polêmicas geradas, principalmente no que tange à restrição demasiada de direitos fundamentais. Mesmo que a intervenção estatal por meio da tecnologia se mostre sutil, por vezes fronteiras de proteção (intransponíveis) são rompidas durante a persecução penal e, portanto, se faz necessário o (re)estabelecimento de (novos) limites para preservar garantias individuais.

Mas e em relação ao ordenamento jurídico brasileiro? Seria lícita a investigação criminal informática a partir da infiltração por *software*?

De imediato, como afirmado acima, trata-se de método de obtenção de prova, de tal sorte que necessita de uma lei processual que o regulamente, tendo em vista que o Estado não poderá incidir em um direito fundamental sem prévia permissão legislativa (*nulla coactio sine lege*)[8]. Neste ponto, não há que se falar na utilização de métodos atípicos de obtenção de prova, justo pelo necessário respeito à legalidade processual. É pela legalidade processual que se permite balizar a aplicabilidade do método utilizado ao conteúdo do direito fundamental restringido. E sobre essa lógica, relembramos Jorge Miranda: “não são os direitos fundamentais que se movem no âmbito da lei, mas a lei que deve mover-se no âmbito dos direitos fundamentais”[9].

Não há, atualmente, lei processual que contemple o direito fundamental restringido pelo referido método de obtenção de prova. Dizer isso, por evidente, é dizer que não se trata simplesmente de interceptação da comunicação de dados, logo, incompatível com a Lei 9.296/96; ademais não se trata — tão somente — da restrição ao direito à livre comunicação. Muito menos haveria que se falar em uso análogo dos dispositivos processuais referentes à busca e apreensão (e custódia) de provas físicas[10]. O uso de procedimentos análogos de busca e apreensão para provas físicas não contempla as peculiaridades de preservação da prova (custódia), o que poderá invalidar o material probatório.

Em verdade, trata-se de um novo direito fundamental que surge em decorrência da “datificação”[11] da vida resultante da dinamicidade atrelada à sociedade de informação. A intrusão sub-reptícia de *malware* em dispositivos informáticos, para além de incidir no direito à livre comunicação, intimidade, privacidade, autodeterminação informativa etc., restringe substancialmente o direito fundamental à integridade e confiabilidade dos sistemas informáticos[12].

Proteger os sistemas informáticos e, por evidente, os dados inseridos neles é proteger os sujeitos cujos dados fazem referência. Essa proteção demarca o critério de legitimação política daquilo que Perez Luño [13] denominará de “sistemas democráticos tecnologicamente desenvolvidos”, justo pelo fato de que a proteção de dados e a liberdade informática fazem parte do *status* que constitui o cidadão.

A Constituição Federal, artigo 5º, parágrafo 2º não exclui a possibilidade de incorporação deste e de outros direitos que pelo seu conteúdo tenham *status* de fundamentais. Trata-se, pois, da denominada cláusula de abertura. Ou seja, para além dos direitos fundamentais expressamente dispostos na Carta Magna (fundamentalidade formal), haÌ• que ser observada a fundamentalidade material do direito que se refere à estrutura básica do Estado e da sociedade[14].

2024 - www.conjur.com.br - Todos os direitos reservados.

Logo, quanto à integridade e confiabilidade do sistema informático como direito fundamental, é evidente que seu conteúdo o incorpora ao conceito material de direitos fundamentais. De tal sorte, pela análise feita, o direito à integridade e confiabilidade do sistema informático, pelo seu conteúdo, compõe a estrutura básica do Estado Democrático brasileiro.

Sendo um direito fundamental, para que o Estado o restrinja na efetivação de investigações criminais mediante *malwares* dever-se-á – antes de tudo — de uma norma constitucional autorizadora. Além disso é claro, necessitar-se-á da norma reguladora (lei processual penal) do referido instituto processual penal de obtenção de provas.

Portanto, é preciso autorização constitucional e regulamentação processual para que tal meio de obtenção de prova seja utilizado, sob pena de estarmos diante de uma prova ilícita expressamente vedada pela Constituição e pelo CPP.

[1] https://g1.globo.com/economia/tecnologia/noticia/2019/05/14/whatsapp-detecta-vulnerabilidade-que-permite-o-acesso-de-hackers-a-celulares.ghtml
[2] MENDES, Carlos Hélder C. Furtado Mendes. ***Malware* do Estado e Processo Penal**. Dissertação de Mestrado, 218f. Programa de Pós Graduação em Ciências Criminais, PUCRS. 2018.
[3] VACIAGO, Giuseppe e RAMALHO, David Silva. ***Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings*.** *Digital evidence and eletronic signature Law Review*, 13 (2016). p, 88.
[4] TESTAGUZZA, Alessandra. ***Exitus acta probat trojan di Stato: la composizione di un conflitto*.** *Orientamenti*. *Archivio Penale*, 2016, n. 2. p, 2.
[5] *Backdoors* são formas ocultas de acessar o sistema do computador infectado de maneira remota, enviando os mecanismos de autenticação existente, possibilitando, assim, que o terceiro — investigador — acesse informações ou monitore as atividades do usuário do sistema alvo infectado. Neste sentido VACIAGO, Giuseppe e RAMALHO, David Silva. ***Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings*.** *Digital evidence and eletronic signature Law Review*, 13 (2016). p, 89.
[6] TORRE, Marco. ***Il captatore informático: nuove tecnologie investigative e rispetto delle regole processuali.*** Giufrré Editore, 2017. p, 17 – 18.
[7] SALT, Marcos. ***Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos***. 1ª ed. Buenos Aires: Ad-hoc, 2017. p, 57.
[8] BRUZZONE, Gustavo. ***La nulla coactio sine lege como pauta de trabajo en mateÌ•ria de medidas de coercioÌ•n en el proceso penal*** Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier. Editores del Puerto Buenos Aires, 2005. p, 248.
[9] MIRANDA, Jorge. **Manual de direito constitucional**. 3.ed. Coimbra: Coimbra Editora, 1996. p, 276.
[10] Em que pese a “busca e apreensão” de provas físicas ter uma natureza jurídica híbrida, isto é, ser tanto medida cautelar probatória como meio de obtenção de prova, o mesmo não ocorre com o instituto processual aqui analisado. A coleta de dados pelo *malware* não conserva a fonte de prova digital, logo, não evita uma frustração processual probatória. De tal forma, não é possível considerá-lo medida

2024 - www.conjur.com.br - Todos os direitos reservados.

cautelar probatória.
[11] Referimo-nos ao incessante registro, em dados (*bits*), de atividades cotidianas, costumes, preferências e hábitos dos indivíduos de um modo geral.
[12] O Tribunal Constitucional alemão definiu como um novo direito constitucional a confiabilidade e integridade dos sistemas de tecnologia da informacÌ§aÌ?o, de modo a protegeÌ?-lo diante de ingerências estatais investigativas que buscassem alcancÌ§ar o fluxo de informacÌ§oÌ?es de maneira oculta utilizando a internet. Sobre isso ABEL, Wiebke; SCHAFER, Burkhard. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems** – a case report on BVerfG, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009. p, 120.
[13] PEREZ LUNÌ?O, Antonio Enrique. **Los derechos humanos en la sociedad tecnoloÌ•gica.** In: LOSANO, Mario G; PEREZ LUNÌ?O, Antonio Enrique; GUERRERO MATEUS, Ma Fernanda. Liberdad informaÌ•tica y leyes de proteccion de datos personales. Cuadernos y Debates. Centro de estuÌ•dios constitucionales. Madrid, 1989. p, 139.
[14] SARLET, Ingo. **A eficaÌ•cia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 12 ed. rev. atual e ampl. Porto Alegre: Livraria do Advogado Editora, 2015, p. 76.

2024 - www.conjur.com.br - Todos os direitos reservados.