Jones Alves: Invasões digitais lembram ataques bárbaros

Na melhor das ficções tecnológicas, haveria quem pudesse imaginar a quebra da privacidade por invasões digitais, ante uma perda de controle pessoal dos domínios do espaço privado mais íntimo?

Futuristas clássicos, como Jules Verne, criador do gênero (1865); Aldous Huxley (*Admirável Mundo Novo*, 1932) e George Orwell (*Mil, Novecentos e Oitenta e Quatro*, 1949), ou ensaístas mais atentos, como Ernest Renan (*L'Avenir de la Science*, 1848), não ousaram pensar tanto assim. Eles não conheceram o *Pokémon Go* (Niantic Labs., EUA, 2016).

Agora, não bastam os vírus invasores de computadores, replicantes e eficientes, para a apropriação de dados pessoais — vírus equivalentes a seres vivos (Richard Dawkins); as violações de sistemas e bases em cenário de guerrilhas cibernéticas ou mesmo a criação de redes de neurônios artificiais para superar a inteligência humana (Hans Moravec). Aplicativos sofisticados também servem a permitir o acesso a informações e imagens, ameaçando, de consequência, a privacidade e a intimidade das pessoas.

O filósofo Cícero Barros (2014) bem explica: “Hoje residimos em um mundo mergulhado na modernidade fundamentada na tecnologia avançada que está em plena ebulição esplendida”. Essa tecnologia avançada apresenta os *drones* de observação, o rastreamento de veículos por *smartphones*, os *hardwares* de controle e sensibilidade para reconhecimento de voz e de objetos; enfim a internet das coisas, interagindo nos ambientes e no cotidiano.

Acontece que, nesta semana, o Comando da Marinha do Brasil, por circular interna, impediu o uso do aplicativo *Pokémon Go* no interior de suas instalações militares.

Explica-se bem: o usuário do jogo de realidade aumentada (*augmented reality – AR*), para a captura das criaturas virtuais (*pokemóns*) explora locais e situações e, a tanto, precisa (i) do uso da câmera fotográfica do celular, (ii) autorizar a sua localização por meio de GPS e, mais, (iii) admitir que os dados sejam “compartilhados com terceiros para pesquisas e análises demográficas da base de usuários”. Além disso, o programa poderá utilizar o conjunto de dados para definir o perfil do usuário, ou seja, a identificação dos seus interesses e preferências.

A todo rigor, o celular, de há muito virou confessionário, com o uso de muitos aplicativos “gratuitos”. Assim, um aviso torna-se inevitável: não procure *pokémons* a domicílio, ou melhor, em sua casa. Eles poderão ser os anfitriões perante terceiros, de sua intimidade, das instalações privadas do seu lar ou dos bens materiais que guarnecem a moradia, em sério atrativo de prejuízo das privacidades convenientes.

A circular da Marinha, por isso mesmo, explica: é preciso evitar o risco de divulgação de informações sigilosas.

Realmente. São demasiadas as invasões da tecnologia. Exemplo mais simples é o da pessoa posta em sossego, no recinto de casa, sofrer invasão à sua privacidade, de forma insistente, por telefonemas para o consumo de oferta de serviços e produtos. O chamado “consumo exaltado” tem sido proibido, nos Estados Unidos, por leis denominadas *do not call* (“não chame”), salvo permissão prévia autorizando as

ligações aleatórias.

Eis, então, o pior: os modernos aparelhos de *smart TV*, equipados com microfones de comando eletrônico (funcionalidade de ativação por voz) e de webcâmera, podem capturar, e capturam, dados de áudio e de imagem do usuário, que podem se constituir em informações sensíveis, transmitidas e capturadas por ou para terceiros. Aliás, esses aparelhos registram o uso do equipamento, por canais assistidos (e mudanças de canais), horários e tempos de duração, serviço denominado *smart ad* que monitora hábitos e preferências do usuário e cujas informações são transmitidas ao fabricante, sem ciência daquele e, ainda, sem criptografia alguma.

Sucede, então, que um casal inglês teve a intimidade violada, em sua sala de estar, por invasão do sistema do seu televisor, quando *hackers*, com uso de *spyware* sofisticado, ligaram e controlaram a web câmera da "TV inteligente", filmando-o em cenas de sexo frente ao aparelho e postando o vídeo na internet (*Daily Mail*, tabloide londrino, 18/5/2016).

Atualmente, o Reino Unido pune as veiculações na internet sexualmente ofensivas, agressões virtuais e atos difamatórios, mediante a Lei das Comunicações Maliciosas (*Malicious Communications Act*), com sanções criminais de até dois anos de prisão para os *trolls* da internet.

Recentemente, foi anunciado um novo marco jurídico de acordo, tratando da transferência de dados pessoais entre a União Europeia e os Estados Unidos, o *Privacy Shield* ("Escudo de Privacidade", de 12/7/16). Designadamente, aqueles usados por aplicativos e empresas de internet, com fins de manipulação comercial dos dados de internautas (*profilers*, perfis estruturados), valiosos na crescente economia digital.

Em nosso país, para além do Marco Civil da Internet (Lei 12.695/2014), somente agora regulamentado pelo Decreto 8.771, de 11/5/2016, tramita na Câmara o PL 5276/2016, oriundo do Executivo (13/5/16), dispondo sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

Induvidosamente, essas invasões digitais não estão afastadas, na escala civilizatória, convenhamos, das antigas invasões bárbaras da Idade Média. A denominada "maldade gratuita" continua desumanizando a nossa condição humana, com novas armas e espaços.

No caso, as novas invasões, de ordem digital, em monitorando dados e manipulando o comportamento de usuários, estão começando uma era de busca de controle total de informações, como imaginou George Orwell.

Em ser assim, quem, afinal, está sendo caçado?

Date Created
28/08/2016