Inteligência artificial e crimes informáticos: tema de 2024

O ano de 2023 ficou marcado pelo aumento vertiginoso dos crimes informáticos, agora impulsionados pelas novas tecnologias, especialmente, por meio do uso de inteligência artificial.

A evolução dos crimes informáticos passa por quatro momentos distintos.

Em um primeiro momento, a criminalidade altamente especializada que exigia profundos conhecimentos de tecnologia da informação e de informática, geralmente cometida por meio da Arpanet ou por meio de golpes sofisticados, como por exemplo o crime praticado pelo matemático Vladimir Levin, que conseguiu transferir mais de 10 milhões de dólares do Citibank para sua conta, sem usar a internet, e Morris Worm, que invadiu mais de 10 mil computadores na Arpanet em 1988.

No segundo momento, com a criação da linguagem HTML e o advento da rede mundial de computadores, há um aumento significativo da criminalidade, já que a potencialização de vítimas, um mercado amplo e mundialmente disseminado, a ausência de legislação específica facilita a prática destes crimes. Nesta fase, já não se exige tanto conhecimento técnico para sua prática, uma vez que impera aqui a teoria da aprendizagem de Sutherland pelo compartilhamento das técnicas para seu cometimento e o acesso facilitado de informações.

O terceiro estágio se dá com o surgimento das redes sociais que multiplicam as conexões, facilitam a inteligência aberta e a engenharia social, o que gera um sem-número de crimes contra o patrimônio e a honra, “normalizando” esse tipo de criminalidade, isto é, já sem qualquer exigência de conhecimento técnico ou de informática do sujeito ativo.

A quarta onda começa com a era da inteligência artificial com ataques em IoT, golpes on-line, disseminação de imagens falsas (deep fake), RaaS (Ransoware As A Service) e a insegurança da informação causada pela opacidade entre o real e o virtual, visto que o falso se aproxima cada vez mais do real pelo uso da tecnologia, além da enorme dificuldade de identificação da autoria e materialidade destes crimes.

Desta feita, o maior desafio do ano de 2024 será lidar com a sofisticação de todos esses ataques, já queas vulnerabilidades aumentam significativamente, além das diversas portas de entrada da criminalidade como Smart TVs, totens, microfones, câmeras, sensores, aparelhos domésticos, além dos tradicionais computadores pessoais, celulares, dentre outros.

Apenas para uma ilustração estatística, segundo o site CISO Advisor: "*os ataques de ransomware registraram aumento de 12,92% globalmente no número de ocorrências em relação ao ano anterior. Somente até a data de fechamento do relatório da ISH Tecnologia, no início de dezembro, foram totalizadas 4.881 vítimas*". [1]

Nem mesmo o maior dos otimistas acreditados na teoria da anomia de Durkheim defenderiam a funcionalidade dos crimes informáticos, pois ainda que eles movimentem bilhões de dólares no mundo e possam inverter valores, na visão de Émile, a sua disfuncionalidade é clara e ululante, não só pela quantidade estatística, como pela sensação de anomia ocasionada, sem contar as cifras ocultas da criminalidade que nestes tipos de crimes é gigantesca.

Portanto, o tema de 2024 é como combater de maneira efetiva os crimes informáticos praticados com o uso de inteligência artificial e, para isso, precisamos pensar em uma política criminal que promova o conhecimento da cadeia de valores utilizadas por esses criminosos, uma conscientização das vítimas para que tenham, acima de tudo, educação digital em atuação preventiva de ataques, estreitamento de relações internacionais de auxílio mútuo (em virtude da transnacionalidade destes crimes), investimento em cibersegurança como diminuição das oportunidades, treinamento dos atores da persecução penal para identificação destes criminosos, aumento das possibilidades de investigação por meio de infiltração virtual, dentre outros aspectos.

Quem sabe esse não seja o primeiro tema a ser debatido pelo recém-criado Comitê Nacional de Cibersegurança (CNCiber), instituído pelo Decreto nº 11.856, de 26 de dezembro de 2023, já que é impossível debater cibersegurança sem ter em mente o desafio hercúleo de combate aos crimes informáticos impulsionados pelas novas ferramentas trazidas pela inteligência artificial.

E a solução não perpassa somente pelo aspecto legislativo, como sói acontecer no Brasil, pois como dizia o Marquês de Maricá: "a força sem inteligência é como o movimento sem direção".

---

[1] Disponível em https://www.cisoadvisor.com.br/ataques-de-ransomware-tem-alta-de-13-em-2023-mostra-estudo/. Acesso em 02.01.2024.

Meta Fields