Cibersegurança na robótica para uma sociedade mais segura

Jorge Pinto
Presidente
Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI - https://ap2si.org)

A robótica é uma das áreas tecnológicas que mais tem evoluído nos últimos anos, tornando-se cada vez mais presente na sociedade moderna, com uma diversidade que tem impactado positivamente diversos setores. No entanto, com a rápida Transformação Digital presente em vários níveis da sociedade, a forte adesão ao paradigma da Indústria 4.0, assim como a integração de temáticas como inteligência artificial, conetividade 5G e 6G e o aumento dos sistemas ciberfísicos, a cibersegurança torna-se, cada vez mais, crítica.

Este artigo aborda a importância da cibersegurança ao longo de todo o ciclo de vida dos *robots*, por forma a garantir a segurança dos utilizadores e a fiabilidade destas tecnologias nas nossas vidas.

Nas sagas Fundação e *Robots*, Isaac Asimov resolve o problema da segurança dos seus *robots* de uma forma que está presente no imaginário de quem trabalha nesta área: introduzindo as suas três (mais tarde, quatro) leis da Robótica como fator intrínseco ao funcionamento do cérebro positrónico que regia o comportamento dos seus *robots*, garantindo assim que estes teriam sempre como prioridade a vida dos seres humanos.

0. Um *robot* não pode causar dano à humanidade ou, por omissão, permitir que a humanidade sofra algum mal.
1. Um *robot* não pode ferir um ser humano ou, por inação, permitir que um ser humano sofra algum mal, exceto nos casos que entrem em conflito com a Lei Zero.
2. Um *robot* deve obedecer às ordens dadas por seres humanos, exceto nos casos em que tais ordens entrem em conflito com a Lei Zero ou a Primeira Lei.
3. Um *robot* deve proteger a sua própria existência, desde que tal não entre em conflito com a Lei Zero, a Primeira Lei ou a Segunda Lei.

Tradução livre para Português das Três Leis da Robótica de Asimov, com a adição da Lei Zero.

A adição da Lei Zero trouxe uma dimensão mais profunda ao conceito das Leis da Robótica de Asimov, destacando a importância da ética, da responsabilidade e do controlo no desenvolvimento de *robots* avançados. A ideia de equilibrar ações individuais com o benefício geral da humanidade continua a ser um tema relevante nas discussões éticas sobre robótica e inteligência artificial nos dias de hoje, e é também neste contexto que a cibersegurança ocupa um lugar essencial. Na ausência da capacidade de implementar as Leis de Asimov, é na segurança que temos de procurar os controlos necessários ao funcionamento seguro e controlado destes equipamentos.

Atualmente, os *robots* caraterizam-se pela sua variedade de formas e funções. Desde os *robots* industriais presentes nas linhas de produção fabris, até aos *robots* médicos que apoiam em cirurgias complexas, encontramos uma panóplia de formas e funções ligadas a atividades profissionais. Mais perto de nós, na esfera pessoal, encontramos *robots* cuidadores de idosos que fornecem apoio e companhia; os veículos autónomos que trazem a promessa de revolucionar a indústria automóvel, tornando a condução mais segura e eficiente; e, claro, os *robots* pessoais cada vez mais comuns, encarregues de tarefas domésticas, companhia e entretenimento.

Com o aumento da complexidade dos sistemas e a crescente capacidade de conetividade, a segurança da informação e a cibersegurança devem ser encaradas como preocupações críticas e incluídas em qualquer estratégia de Transformação Digital, industrial ou outra. A par do crescente interesse da sociedade em *robots* e da sua proliferação em diversos setores, os cibercriminosos têm reconhecido a robótica como um novo alvo para os seus ataques. Os *robots* podem ser explorados para aceder a redes, espiar, realizar ataques físicos, ou até mesmo para operações de extorsão. Casos de *robots* industriais comprometidos, resultando em danos físicos ou interrupção de operações, já foram relatados, demonstrando a necessidade de proteger esses equipamentos. A hiperconetividade, as comunicações *wireless*, as redes de sensores, a utilização de sistemas operativos e de controlo inseguros, associados a uma descentralização suportada em paradigmas como *cloud*, *edge computing* e *IoT*, aumentam a exposição ao risco de ciberataques, remotos ou presenciais, tornando estes equipamentos potenciais alvos para criminosos com todos os impactos negativos que daí podem advir.

É fácil compreender os riscos de um ciberataque para uma operação fabril ou uma operação logística dada a visibilidade das consequências: falhas ou paragem de operações, ferimentos em operadores, entre outros. No entanto há outros riscos cujos impactos são menos visíveis, mas igualmente perturbadores como sendo a interceção de áudio e vídeo em *robots* domésticos, ou a utilização de técnicas adversas para enganar sensores pervertendo o funcionamento dos equipamentos. Pedimos ao leitor que imagine como se sentiria se um *robot* cuidador num lar agredisse um familiar, um *robot* de companhia em sua casa lhe exigisse vocalmente um pagamento devido a um ataque de *ransomware*, ou o seu veículo autónomo tomasse decisões erradas por manipulação dos sensores, apenas para citar alguns exemplos. À medida que a robótica se torna cada vez mais comum é necessário ter