

# Sistemas de vigilância com IA: da segurança pública ao abuso de poder

 [digitalinside.sapo.pt/sistemas-de-vigilancia-com-ia-da-seguranca-publica-ao-abuso-de-poder](https://digitalinside.sapo.pt/sistemas-de-vigilancia-com-ia-da-seguranca-publica-ao-abuso-de-poder)

Bruno Castro

Nas últimas décadas, os avanços tecnológicos permitiram o desenvolvimento de sistemas de vigilância com inteligência artificial (IA) capazes de monitorizar grandes populações em tempo real. Estes sistemas, alimentados por algoritmos de reconhecimento facial, análise comportamental e processamento de grandes volumes de dados, são frequentemente apresentados como ferramentas indispensáveis para a prevenção de crimes, a manutenção da ordem pública e a resposta rápida a ameaças. No entanto, à medida que se tornam mais sofisticados e intrusivos, levantam também preocupações sérias sobre privacidade, liberdade individual e abuso de poder, sobretudo em regimes autoritários.

A China é atualmente um dos exemplos mais notórios da aplicação massiva de sistemas de vigilância baseados em IA. Cidades inteiras estão equipadas com milhões de câmaras de videovigilância interligadas a plataformas de reconhecimento facial e análise de movimento. Estes sistemas permitem, por exemplo, identificar automaticamente suspeitos procurados, detetar comportamentos considerados “anómalos” ou localizar indivíduos em grandes multidões em segundos. A justificação oficial para este investimento avultado em tecnologias de vigilância assenta na prevenção do crime, na luta contra o terrorismo e na promoção da “estabilidade social”.

Contudo, esta infraestrutura tecnológica tem vindo a ser usada para fins que vão muito além da segurança pública. Em regiões como Xinjiang, os sistemas de vigilância são utilizados para monitorizar em detalhe a população uigur, uma minoria étnica muçulmana, com recolha de dados biométricos em massa, controlo de movimentos e análise de interações sociais. Os algoritmos identificam perfis de risco baseados em fatores como religião, origem étnica ou até comportamentos considerados “desviantes”, sem necessidade de provas concretas de qualquer crime. A vigilância torna-se assim uma ferramenta de repressão, funcionando como uma forma de controlo político e não propriamente como uma forma de manter a segurança pública.

Mais preocupante ainda é o modo como estas tecnologias operam num contexto de opacidade e ausência de escrutínio público. O cidadão comum não tem forma de saber como é classificado por um sistema algorítmico, nem de contestar decisões automáticas que podem afetar o seu acesso a transportes, emprego ou serviços públicos. O risco é o de criar uma sociedade onde o controlo permanente substitui a confiança, e onde o medo de ser observado limita a liberdade de expressão, manifestação e até o próprio pensamento.

É importante sublinhar que o perigo não reside na tecnologia em si, mas antes, na forma como é utilizada. Em países democráticos, com mecanismos de fiscalização, normas éticas e regulamentação robusta, a IA pode, de facto, apoiar a segurança pública sem comprometer os direitos fundamentais. Já quando estas salvaguardas não existem, a linha entre a vigilância legítima e a opressão digital torna-se perigosamente ténue.

O caso chinês serve como alerta global – a promessa de segurança e ordem não pode justificar a construção de sistemas que tratam cada cidadão como potencial suspeito. A tecnologia deve sim estar ao serviço da dignidade humana e dos valores democráticos, e não ser usada para os minar. Cabe às sociedades modernas definir os limites éticos e legais da vigilância com IA, antes que os limites nos sejam impostos por máquinas que não compreendem valores tão fundamentais como a liberdade.