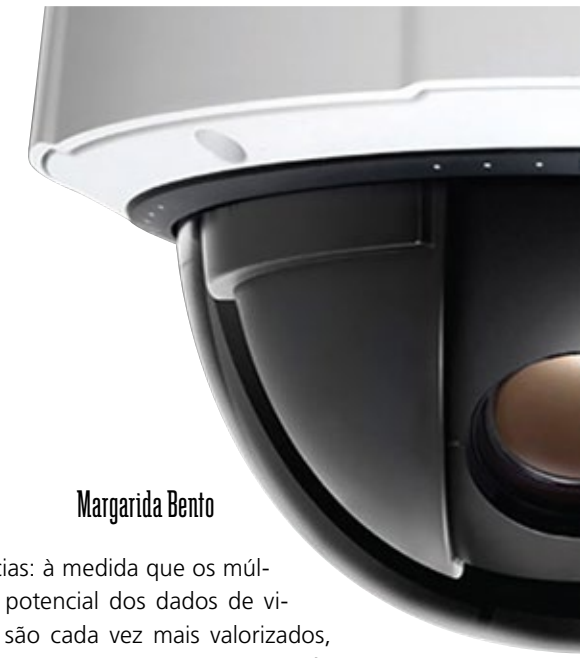


Videovigilância é agora IT

Se não tem acompanhado as evoluções no campo da videovigilância, pode ficar surpreendido como as principais tendências do setor lhe vão soar a tecnologias da informação

Margarida Bento

As vendas de câmaras profissionais de videovigilância têm crescido a um ritmo cada vez mais acelerado, e a previsão é que continuem a crescer de 2018 em diante.
É estimado que 130 milhões de câmaras de vigilância sejam vendidas até ao final do ano, algo como 13 vezes mais do a metade da década passada.

Ao mesmo tempo, desenvolvimentos tecnológicos na indústria trazem consigo mudanças de paradigma que influenciarão a forma como as organizações lidam com a videovigilância.

Conheça as 5 principais tendências do CCTV

1 DEEP LEARNING

Estamos a viver um ponto de viragem na aplicação de inteligência artificial na videovigilância. Até há pouco tempo, o principal obstáculo à adoção generalizada de *deep learning* era a dificuldade de provar benefícios significativos de segurança ou *business intelligence* na utilização da tecnologia em muitos cenários diferentes. O último ano trouxe ao mercado um grande progresso nesse sentido, com a evolução de algoritmos de *deep learning proof-of-concept* para produtos de videovigilância prontos a instalar, com interfaces *user-friendly* e soluções focadas em cenários específicos.

No seguimento da última grande evolução no mercado da videovigilância – a transição para câmaras digitais de rede – a próxima fase será provavelmente a adoção generalizada de câmaras equipadas com *deep learning*. Do mesmo modo, dever-se-á verificar, dentro de uns anos, uma redução acentuada dos preços à medida que esta adoção se for desenrolando, impulsionando um aumento rápido do número de unidades vendidas.

Em termos de abordagens, as estratégias focar-se-ão nos mercados principais, com a tendência inicial de aplicação em segurança pública e mobilidade eventualmente a evoluir para o *retail* e edifícios comerciais.

Fabricantes que adotem aplicações de *deep learning* com foco vertical alinhado com os seus portfólios deverão, portanto, ter uma boa oportunidade de crescimento na área.

2 TOLERÂNCIA A FALHAS

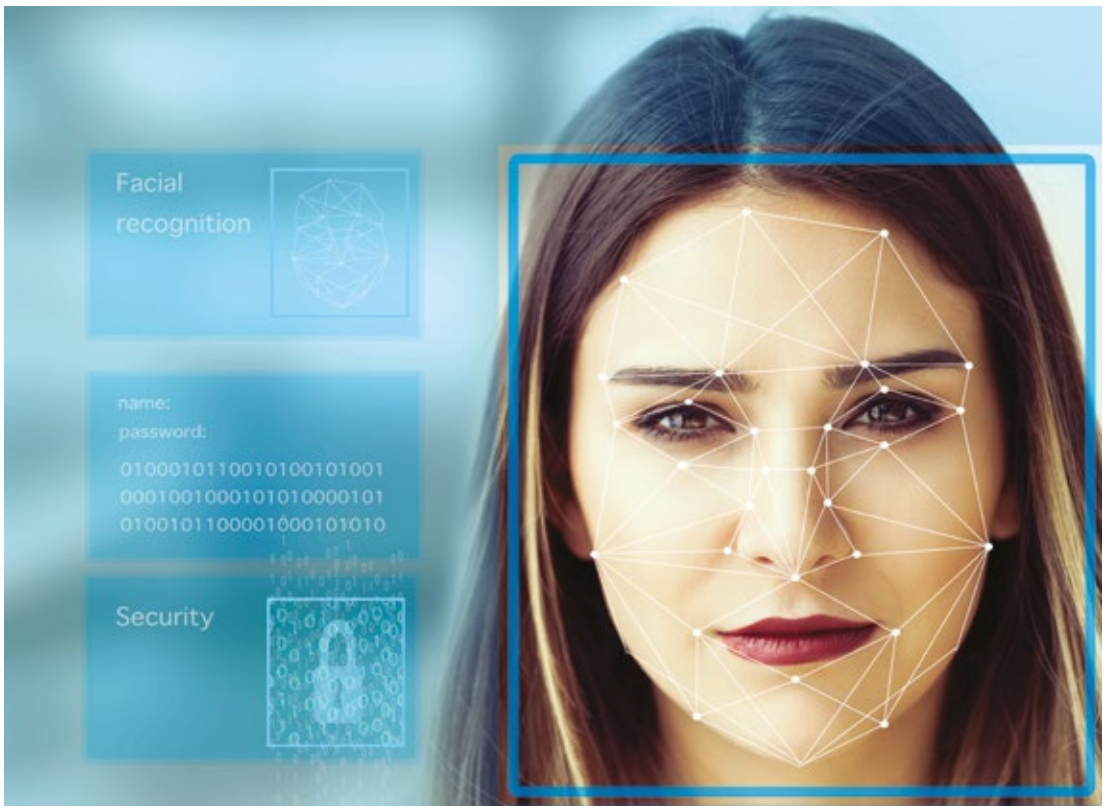
Comparada com a indústria do IT, a indústria da videovigilância tem regra geral uma atitude visivelmente relaxada face a muitos aspetos de *failover* e redundância: a capacidade de um sistema de videovigilância tolerar falhas ao mesmo tempo que mantém um nível operacional aceitável é raramente discutida.

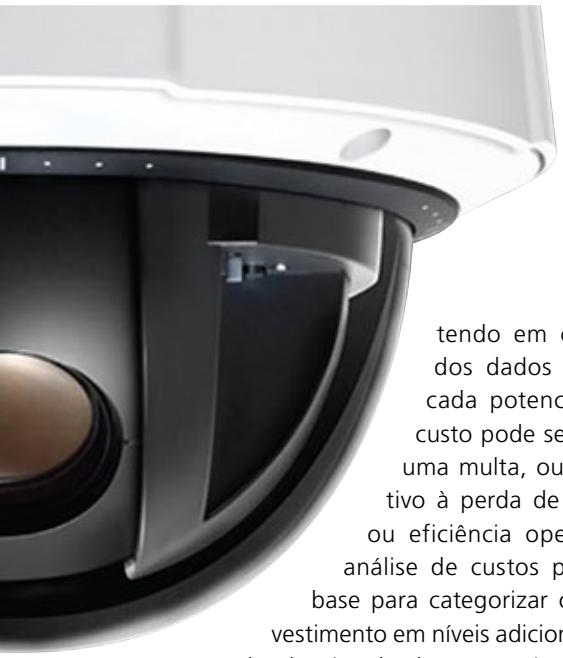
Contudo, apesar da tendência crescente da indústria para a utilização de tecnologias de IT de alto nível, a maioria dos sistemas de videovigilância ainda têm tolerância a falhas e capacidade de *failover* bastante limitadas, um problema que não deixará de existir por ser ignorado.

As boas notícias: à medida que os múltiplos usos e potencial dos dados de videovigilância são cada vez mais valorizados, veremos uma exigência muito maior de *failover,* redundância e *backups* por parte dos utilizadores finais.

Sistemas de videovigilância com um nível de tolerância de falhas mais elevado tendem a focar-se na mitigação de falhas após a captura de vídeo. Isto deve-se ao impacto mais elevado das falhas provenientes do *back-end*, em vez de câmaras individuais: a falha de uma câmara individual tem um impacto muito menor do que uma falha no servidor de gravação ou sistema de armazenamento, os quais podem levar à perda de todas as imagens de vídeo.

Isto deixa de ser tão linear quando a videovigilância é utilizada para mais do que simples segurança: este impacto pode passar a ser medido





tendo em conta o custo dos dados perdidos com cada potencial falha. Este custo pode ser direto, como uma multa, ou indireto, relativo à perda de produtividade ou eficiência operacional. Esta análise de custos pode formar a base para categorizar o potencial investimento em níveis adicionais de *failover,* redundância e *backups* para sistemas de videovigilância.

3 ANALÍTICA FORENSE AS-A-SERVICE

Com recurso a ferramentas tradicionais (papel e caneta) um investigador ou analista especialmente treinado leva em média perto de duas horas a rever uma hora de vídeo. Isto torna-se um enorme gasto de recursos, especialmente em áreas do domínio do setor público, como a polícia, que lidam com grandes e constantes limitações de tempo e orçamento.

Há muito tempo que existe a necessidade de agilizar este processo, mas à medida que o volume de dados cresce, esta torna-se especialmente sentida. Só recentemente, graças a avanços na área de *deep learning*, é que as ferramentas de analítica de vídeo alcançaram um nível de precisão suficientemente confiável para prestar assistência a analistas humanos. Constituem portanto um investimento considerável em termos de hardware, software, implementação e formação. Adicionalmente, muitos dos potenciais clientes não procuram analítica de vídeo em tempo real para sistemas integrados, mas sim ferramentas que lhes permitam analisar um repositório de potenciais provas recolhido de várias fontes em formatos diversos.

Alguns fabricantes têm oferecido os seus pacotes de analítica e software num modelo as-a-service, no qual agências ou forças policiais podem usar a infraestrutura on-site e analistas internos do fabricante para *outsourcing* da sua análise forense de vídeo.

O próximo passo lógico seria mover este modelo para a cloud, de forma a que com a formação adequada os clientes possam usar analítica forense de vídeo *on-demand* remotamente com os seus próprios analistas, sem necessidade de um grande investimento em hardware.

4 RGPD

A forma concreta como o RGPD será transcrito para a lei portuguesa fica ainda por ver, mas sabemos que se contam entre os artigos aplicáveis à videovigilância três grandes diretivas:

- Todas as entidades e organizações que lidem com videovigilância de espaços públicos devem nomear um Encarregado de Proteção de Dados;
- Todo o armazenamento de imagens de videovigilância de espaços públicos e certos tipos de espaços comerciais está sujeito a auditorias de impacto de privacidade;
- O titular dos dados tem direito a requisitar uma cópia de todos os seus dados resultantes de videovigilância se esta disser respeito a um espaço público.

Esta última cláusula, em particular, tem implicações significativas a nível administrativo e técnico. Se o sistema não estiver otimizado para este efeito, isto levará a uma sobrecarga administrativa na validação e processamento destes pedidos. Adicionalmente, material que mostre pessoas para lá do titular dos dados terá de ser editado para proteger a privacidade dos restantes indivíduos, uma tarefa que consome grandes quantidades de recursos.

Será portanto essencial que organizações sujeitas a muitos pedidos desta natureza disponham não só de ferramentas de reconhecimento facial como também de tecnologia para automatizar e/ou reduzir este *workload* de edição, como ferramentas de analítica de vídeo para ocultação automatizada de identidade.

5 CIBERSEGURANÇA

À medida que os sistemas de videovigilância se tornam cada vez mais sofisticados, integrando (ou constituindo por si só) ecossistemas de IoT, a questão da cibersegurança torna-se cada vez mais premente. Uma vez que muitos destes dispositivos não têm os mesmos níveis de proteção de outros *endpoints*, mas estão igualmente ligados à rede, tornam-se portas de entrada para cibercriminosos.

Como tal, já não basta falar da segurança na IoT, mas sim de *resiliência by design*. Ou seja, ao construir um ecossistema de raiz, as organizações devem integrar logo de início soluções de segurança que garantam a salvaguarda da rede e dos processos, corram horizontalmente no ecossistema e protejam cada *endpoint* independentemente do seu protocolo ou fabricante.

Por último, há que ter em conta que cada sistema é um sistema e, como tal, deve ser feita uma avaliação de riscos, para isolamento e eliminação, definindo potenciais cenários de ataque e diferenciando os riscos críticos e mitigáveis – um tópico que, como já mencionado, se tornará particularmente vital com a implementação do RGPD.