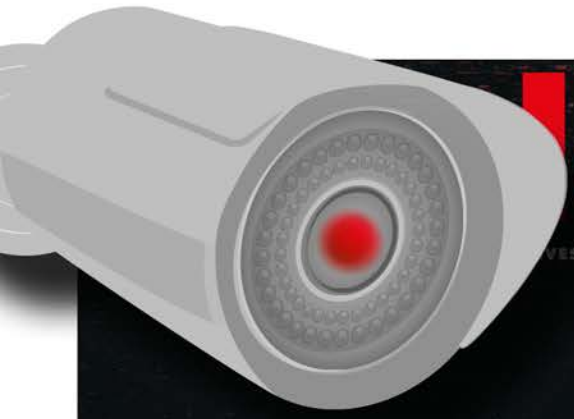


I&D

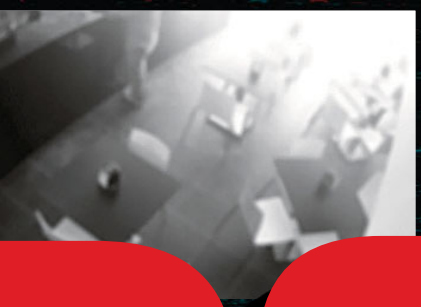
INVESTIGAÇÃO E DESENVOLVIMENTO

# VIGIA

As câmaras de videovigilância estão por todo o lado e pouco se sabe sobre elas. Uma tecnologia de segurança cada vez mais popular e que pode ter fortes implicações na privacidade dos portugueses – sobretudo com a chegada de sistemas avançados de reconhecimento facial, de monitorização e de análise comportamental. Esta é a primeira parte de uma investigação ao vasto, complexo e desconhecido mundo da videovigilância em Portugal

**Texto:** Rui da Rocha Ferreira
**Fotos:** Luís Barra, José Carlos Carvalho, Marcos Borga e Ricardo Nascimento

BOLSA DE INVESTIGAÇÃO JORNALÍSTICA GULBENKIAN



ESTAS SÃO IMAGENS DE CÂMARAS DE VIDEOVIGILÂNCIA LOCALIZADAS EM PORTUGAL E ACESSÍVEIS, POR ARQUIVO, NA WEB. ESTÃO EDITADAS POR FORMA A IMPEDIR A POSSIBILIDADE DE IDENTIFICAÇÃO, QUER DAS PESSOAS RETRATADAS, QUER DOS LOCAIS CAPTADOS

# DOS

É um cenário dantesco. Quartos de crianças e de adultos, salas de estar e de jantar, garagens e piscinas privadas, pátios e jardins. Restaurantes e cafés, escritórios, oficinas e cabeleireiros, entre muitos outros. Completamente expostos e visíveis para todos na internet. São milhares, senão mesmo dezenas de milhares, as câmaras de videovigilância em Portugal que permitem uma invasão sem precedentes da vida privada de muitas pessoas e são uma ameaça de segurança, para utilizadores e empresas. Um cenário que tem tanto de assustador como de mordaz: o sistema que muitos compraram para se sentirem mais seguros é uma porta escancarada para as suas vidas familiares, para as suas casas e para os seus negócios.

Registos de imagens destas câmaras visualizados pela *Exame Informática* mostram situações alarmantes: numa das câmaras era possível ver uma criança deitada na cama; numa outra, uma pessoa sentada no sofá; noutra câmara, um grupo de pessoas a treinar num ginásio; e numa outra, o interior de um estabelecimento de restauração, mesmo por cima da caixa registadora e do terminal de pagamentos Multibanco. Cada uma, de forma diferente, representa uma forma brutal de invasão da privacidade.

Algumas destas câmaras de videovigilância estão à distância de uma simples pesquisa num motor de busca especializado e por isso podem ser acedidas por qualquer pessoa com conhecimentos básicos de tecnologias da informação. Noutras situações, as câmaras ainda têm as mesmas credenciais de acesso – nome de utilizador e palavra-passe – que vieram de origem com o equipamento e que podem ser facilmente encontrados com uma pesquisa online. E há ainda casos de câmaras que apesar de já terem alguma proteção adicional (como uma palavra-passe definida pelo utilizador), têm software antigo e para o qual são conhecidas graves vulnerabilidades de segurança, o que significa que na prática também estão totalmente desprotegidas.

Um cenário preocupante e que segundo os especialistas tem implicações muito além da privacidade.

## O BIG BROTHER DA VIDA REAL

O problema começa logo com o grande número de câmaras de videovigilância que têm portos de comunicação abertos para a internet – ou como se costuma dizer na comunidade de segurança informática, são câmaras que estão 'viradas' para a internet. Para perceber melhor o que está em causa, imagine uma rua (a web) que dá acesso a muitos armazéns (portos de comunicação), cada um especializado numa tarefa – neste caso, interessa-nos o que está responsável pela transmissão de vídeo em tempo real. Dentro deste armazém existem salas (equipamentos conectados) que podem estar mais ou menos protegidos: uns têm as portas escancaradas e permitem ver tudo; outros têm as portas encostadas e basta empurrar para ver tudo; outros têm portas fechadas à chave, mas fáceis de arrombar; e outros têm portas com fechaduras robustas e difíceis de arrombar.

Existem depois motores de busca especializados, casos do Shodan e do Binary Edge, em descobrir equipamentos ligados à internet e que têm portos de comunicação abertos. "O Shodan é um motor de busca gigante que está a monitorizar a internet. Está constantemente a indexar equipamentos e a reunir informações sobre esses equipamentos que depois são guardados em bases de dados que podemos consultar", explica Fábio Mestre, investigador de segurança informática e membro da equipa de testes de intrusão da empresa Hardsecure.

> "ISTO PARA MIM JÁ É UM GRANDE PROBLEMA, PORQUE JÁ TENHO QUASE 20 MIL EQUIPAMENTOS EXPOSTOS E VULNERÁVEIS. SÃO 20 MIL EXPOSIÇÕES DE ALTO RISCO"
>
> **FÁBIO MESTRE**
> INVESTIGADOR DE SEGURANÇA INFORMÁTICA E MEMBRO DA EQUIPA DE TESTES DE INTRUSÃO DA HARDSECURE

O Shodan é uma das ferramentas que faz parte do seu arsenal diário de trabalho. "Tenho tendência a usar o Shodan apenas como uma ferramenta de recolha de informação", explica. Daí conhecer tão bem o quão longe se pode chegar – literalmente, entrar na casa e até nos quartos de outras pessoas – com uma simples pesquisa.

No caso das câmaras de videovigilância, a atenção recai sobre o porto de comunicação 554, usado para fazer a transmissão de vídeo em tempo real (RTSP, de Real Time Streaming Protocol) através da internet, e sobre o porto 80, um protocolo usado para ligações HTTP, que no caso das câmaras de videovigilância indica que existe um portal online para aceder às câmaras.

## O QUE ESTÁ A FALHAR?

"O que está a falhar é o que falha sempre na cibersegurança – a consciencialização. Quem compra estas câmaras quer ver as imagens muito rapidamente, mas depois esquece-se que todos estes equipamentos têm configurações, têm passwords por defeito e têm que ter uma camada de segurança – que quem compra e quem vende desconhece", lamenta Sérgio Silva, da CyberS3C.

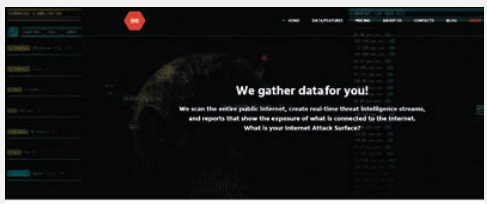
Existem termos técnicos específicos que se introduzidos em motores de busca como o Shodan permitem encontrar, em poucos segundos, milhares de câmaras cuja informação está acessível para toda a internet. Só em Portugal são mais de 41 mil. E logo aqui há um problema. O simples facto de serem encontradas pelo Shodan não significa que estão vulneráveis ou que podem ser acedidas por qualquer pessoa, significa sim que têm dados importantes expostos para a internet – tais como o endereço de IP, a versão do software, o fabricante do equipamento, entre outros dados cruciais. "Posso dizer que é um problema termos 41 mil câmaras acessíveis via motor de busca, no Shodan ou no Binary Edge – é uma grande superfície de ataque. Para quem vai tentar entrar nas câmaras, isto representa 41 mil possíveis hipóteses [de ataque]", sublinha o investigador de 37 anos, natural de Almada.

Sentado na cadeira do escritório de casa enquanto gozava uns dias de férias, Fábio Martins ia digitando novos termos de pesquisa no famigerado Shodan enquanto a entrevista decorria. E à medida que a pesquisa é refinada, tudo fica mais sério. Quando pesquisou por uma marca específica de câmaras de videovigilância e por uma versão de software em particular – que já é do conhecimento público que tem uma falha grave de segurança que permite ao atacante ganhar acesso remoto e total às câmaras –, encontrou de uma assentada mais de 20 mil equipamentos expostos só em Portugal. "Isto para mim já é um grande problema, porque já tenho quase 20 mil equipamentos expostos e vulneráveis. Se conseguir encontrar um exploit [software que tira partido de uma vulnerabilidade], funciona em quase 20 mil equipamentos. Quer dizer que consigo comprometer quase 20 mil infraestruturas, sejam elas grandes ou pequenas, tenham elas só estas câmaras ou outros equipamentos lá dentro. E isto sim já é um grande problema – são 20 mil exposições de alto risco", alerta.

Mas uma outra pesquisa de Fábio com palavras-chave mais específicas – que a *Exame Informática* não divulga para não colocar ainda mais em risco os muitos utilizadores afetados – revela resultados assustadores. Existem mais de cinco mil câmaras de videovigilância em Portugal que podem ser acedidas e visualizadas... sem qualquer tipo de autenticação. E estes sistemas de videovigilância estão espalhados por todo o País: Lisboa, Porto, Braga, Coimbra, Faro, Funchal, Ponta Delgada, Viseu, Évora, Leiria, Sintra, Castelo Branco, entre muitas outras regiões.

Uma realidade chocante que será nova para muitos, mas que Sérgio Silva, fundador da empresa de formação em segurança informática CyberS3C,

**Motores de busca como o Binary Edge e o Shodan permitem encontrar dispositivos 'virados' para a internet, entre os quais dezenas de milhares de câmaras de videovigilância**




## JACKPOT!

Em março de 2021, um grupo de hackers ganhou, de uma só vez, acesso a 150 mil câmaras de videovigilância desenvolvidas pela empresa Verkada e a todo o arquivo de vídeo da tecnológica, depois de ter encontrado falhas de segurança no sistema da empresa norte-americana. Segundo avançou a agência *Bloomberg*, os atacantes ficaram com acesso a transmissões de vídeo em tempo real de hospitais, clínicas, esquadras de polícia, prisões, fábricas, entre muitos outros locais. Algumas das câmaras tinham inclusive sistemas de reconhecimento facial.

Foto: L.B.

já conhece há bastante tempo. "É um bocado intrusivo, não é?", questiona enquanto nos mostra imagens registadas pelo Shodan de uma câmara instalada num ginásio. "E nenhuma destas pessoas certamente sabe que as imagens delas a treinar estão a ser transmitidas para todo o mundo". Com um computador Mac à sua frente e sentado numa cadeira e mesa improvisados para nos receber num novo escritório ainda em obras, foi-nos mostrando registos de imagens de câmaras de videovigilância que estão a transmitir vídeo em tempo real para toda a internet. "Cada uma destas câmaras pode ser a antena de um Big Brother", diz na voz grave que o caracteriza.

### CONSEQUÊNCIAS IMPREVISÍVEIS

Se a ideia de ter um perfeito desconhecido na internet a vigiar-nos de forma constante é suficiente para provocar um arrepio na espinha, há outras consequências com efeitos imprevisíveis que também estão à espreita. "Estarmos a ser filmados quando estamos a treinar já é mau, outra coisa é [pensar em] quem é que vai ter acesso a estas imagens e o que é que vai fazer com elas", atira Sérgio Silva. No exemplo do estabelecimento de restauração já referido, um ladrão pode usar as imagens da câmara para controlar quanto dinheiro está na caixa, os horários dos funcionários, as suas rotinas e escolher o melhor momento para fazer o assalto, exemplifica o especialista. É que uma câmara de vigilância insegura não é apenas uma porta de entrada para a vida das pessoas – é um risco real para a sua segurança. "Há pessoas que podem ter a vida destruída por causa destas câmaras", atira Sérgio Silva.



Além de permitirem controlar a vida de uma pessoa ou as rotinas de um negócio, estas câmaras vulneráveis são uma porta de entrada nas redes domésticas e empresariais, permitindo a partir daí iniciar ataques a outros equipamentos que estejam ligados – desde um computador pessoal a um servidor empresarial. "Havendo tantos equipamentos assim disponíveis, estamos a criar imensos vetores de ataque para diferentes pessoas, diferentes negócios e diferentes organizações", lembra Fábio Mestre. E segundo confirmou o especialista em segurança informática, muitas destas câmaras estão efetivamente instaladas em redes empresariais: " Isto são empresas que têm câmaras viradas para a internet e que estão vulneráveis", lamenta.

"NENHUMA DESTAS PESSOAS SABE QUE AS IMAGENS DELAS ESTÃO A SER TRANSMITIDAS PARA TODO O MUNDO. (...) HÁ PESSOAS QUE PODEM TER A VIDA DESTRUÍDA POR CAUSA DESTAS CÂMARAS"

**SÉRGIO SILVA**
FUNDADOR DA CYBERS3C

### A CALMA ANTES DA TEMPESTADE

As cinco mil câmaras às quais é possível aceder sem credenciais ou grandes conhecimentos técnicos são as que geram maior preocupação. Mas será que é assim tão fácil atacar e ganhar acesso às restantes câmaras de videovigilância que têm software vulnerável? Perguntamos a quem ganha a vida a descobrir vulnerabilidades, sobretudo em dispositivos da chamada Internet das Coisas (IoT), categoria na qual se incluem estas câmaras: Pedro Ribeiro, que já venceu a Pwn2Own, uma das mais importantes competições de hackers do mundo. "Da minha experiência, as câmaras de videovigilância são dos sistemas de IoT mais inseguros", começa por detalhar.

Nas câmaras de um único fabricante, o hacker português já chegou a encontrar mais de 20 vulnerabilidades críticas. "Nas câmaras e sistemas que eu analisei, consegui execução de código remoto de maneira relativamente fácil (...), são vulnerabilidades extremamente simples", conta. Desde ter encontrado uma página de diagnóstico da câmara que permitia aceder à mesma sem qualquer autenticação, a enviar um conjunto gigante de caracteres (uma técnica conhecida como buffer overflow) que faz com que a câmara entre em 'crash', momento no qual o atacante consegue ganhar acesso total ao sistema. "Qualquer função que a câmara faça, nós podemos controlar e até podemos adicionar novas funções. Imaginemos que o vídeo está desligado, posso ligar o vídeo. A gravação está desligada, posso ligar a gravação de X horas a X horas". Por exemplo, é possível iniciar um assalto a uma residência ou a um espaço comercial provocando primeiramente um apagão nas câmaras de videovigilância, para que não registem imagens do crime. "O problema é

# ...AMIGO É

Numa entrevista à *Exame Informática* em novembro de 2021, Ondřej Vlček, diretor executivo da Avast, uma das maiores empresas de cibersegurança do mundo, já alertava que os dispositivos IoT, sempre ligados à internet, são uma "bomba-relógio" prestes a rebentar, com destaque para as câmaras de videovigilância. "As câmaras têm sido muito populares junto dos maus da fita. Milhares, quem sabe milhões de câmaras que podes pesquisar e estão a transmitir os conteúdos 24 horas por dia de forma aberta e que estão vulneráveis. Podes carregar código malicioso para aquela câmara e tomar conta de todo o sistema operativo que está a operar a câmara, isso é um grande problema". Quem nos avisa...

que estas câmaras são ubíquas, estão por todo o lado. Se algum grupo de ladrões sofisticados quiser atacar um banco ou militares de um estado quiserem atacar outro, tomar controlo das câmaras, desligar as câmaras, como vemos nos filmes de espiões, em que eles trocam a imagem, é fácil trocar as imagens de segurança tendo controlo da câmara", alerta o investigador natural de Coimbra e atualmente a viver na Tailândia.

Pedro Ribeiro já chegou a ser abordado com propostas para atacar modelos específicos de câmaras de videovigilância. Não aceitou esses trabalhos, por ser um white hacker – um investigador que descobre vulnerabilidades não para tirar partido delas, mas para que seja possível corrigi-las, tornando os equipamentos mais seguros. Mas revela-nos como seria o *modus operandi* de um agente mal intencionado. "Comprava os dispositivos [identificados como vulneráveis] numa loja, abria-os, olhava para o hardware, olhava para o software, extraia o firmware, fazia testes dinâmicos ao dispositivo, para tentar perceber como é que ele funciona e fazia uma análise de vulnerabilidades, como as que faço profissionalmente. (...) E fabricava uma ciberarma que funciona para esses dispositivos. Depois é só usar essa ciberarma no sistema alvo".

"INFELIZMENTE A ÚNICA MANEIRA PARA [AS CÂMARAS] SE TORNAREM MAIS ROBUSTAS É SOFRENDO MAIS ATAQUES E HAVENDO MAIS MEDIATISMO, AS DUAS COISAS ANDAM LADO A LADO"

**PEDRO RIBEIRO**
INVESTIGADOR DE SEGURANÇA INFORMÁTICA

Mas se há tantas câmaras vulneráveis, se os riscos são tão grandes, por que razão não ouvimos falar em Portugal de ataques a estes sistemas? "Um ataque à videovigilância nunca será muito público", analisa Pedro Ribeiro. " Das duas uma: ou são hackers que querem fazer uma coisa muito espalhafatosa, o que é cada vez mais raro, ou é alguém que tem um interesse específico. (...) Acho que vão ser mais coisas silenciosas, o que no fundo acaba por ser pior – são ataques que não são reportados ou que muitas vezes não são detetados".

A falta de políticas de segurança das empresas que fabricam as câmaras de videovigilância, o desconhecimento dos problemas por parte dos utilizadores e das empresas acabarão por resultar, mais cedo ou mais tarde, numa situação de consequências imprevisíveis. "Infelizmente a única maneira para [as câmaras] se tornarem mais robustas é sofrendo mais ataques e havendo mais mediatismo, as duas coisas andam lado a lado. Vamos ter mais problemas porque há mais câmaras, mais problemas geram mais olhos [de investigadores] nisto, mais olhos nisto resultam em menos problemas a longo prazo", explica.

E da mesma maneira que lhe fizeram uma proposta para criar uma arma que permitisse entrar em câmaras de videovigilância, outros recebem e receberão propostas semelhantes. "Há mercado para isto, sem dúvida, há muito mercado para isto", garante. "A procura existe. Tudo o que é comum, generalizado, tem procura, desde os iPhone até essas câmaras de videovigilância que estão por todo o lado". E as câmaras de videovigilância estão, literalmente e cada vez mais, por todo o lado. ■

## DICA

## CÂMARAS MAIS SEGURAS

COMPRE CÂMARAS DE FABRICANTES CONHECIDOS E COM POLÍTICAS DE ATUALIZAÇÃO DE SOFTWARE COMPROVADAS

MUDE A PALAVRA-PASSE DE ACESSO À CÂMARA REGULARMENTE

MANTENHA O SOFTWARE DA CÂMARA SEMPRE ATUALIZADO

MANTENHA A CÂMARA NUMA REDE WI-FI SEPARADA DA REDE PRINCIPAL


Fotos: M.B.

# VIDEOVIGILÂNCIA: UMA TEIA CADA VEZ MAIOR

Nunca foi tão barato comprar uma câmara de videovigilância. Por apenas 25 euros, adquirimos numa loja um equipamento que já nos dá uma resolução elevada, movimento panorâmico, capacidade de deteção de movimento, visualização de infravermelhos para ambiente noturno, aplicação para aceder à transmissão de vídeo à distância e microfone integrado para comunicação bidirecional. É quase como se estivesse a investir num vigilante privado, que pode trabalhar 24 horas por dia, sete dias por semana, por um preço tão baixo que desafia a lógica dos negócios.

Os preços super acessíveis e a evolução tecnológica explicam o aumento significativo de câmaras de videovigilância em ambiente doméstico, mas a tendência também é notória em lojas e até nas ruas.

## UMA CÂMARA A CADA 10 MINUTOS

Dados cedidos à *Exame Informática* pela IDC, consultora especializada na monitorização de vendas de equipamentos eletrónicos, mostram que a venda de

**Só a Prosegur, cuja Central Recetora de Alarmes (CRA) visitámos, tem mais de 31 mil câmaras de videovigilância instaladas, entre câmaras IP e sistemas CCTV**

câmaras de videovigilância no segmento doméstico 'explodiu' e continua a aumentar: entre 2019 e 2020 o crescimento nas vendas foi de 250%; já em 2021 o aumento foi de 45%. "Em 2020 venderam-se um total de 42 mil câmaras e em 2021 foram vendidas 60 mil câmaras", revela Francisco Jerónimo, vice-presidente europeu da IDC para a área de dispositivos eletrónicos. Valores que dão uma média de uma câmara de videovigilância vendida a cada 10 minutos em Portugal. Já em volume de negócios, a venda destes equipamentos rendeu 3,6 milhões e 4,5 milhões de euros, respetivamente, nos períodos indicados.

A IDC estima ainda que o segmento das câmaras de videovigilância domésticas vá continuar a crescer, em média, 12% por ano, até 2027. "Tem tido e vai continuar a crescer fortemente porque o preço é atrativo. Não é um grande investimento, as pessoas não têm de pensar dez vezes [antes de comprar]. É por isso que temos visto esta explosão de produtos", explica Francisco Jerónimo. Já as marcas que dominam o mercado doméstico de videovigilância são a Xiaomi (60% de quota de mercado), a Arlo (13%) [em novembro de 2021, a Arlo foi adquirida pela Securitas Direct], a Ring, detida da Amazon, garante 7% de quota, a TP-Link chega aos 6% e a Netatmo fica-se pelos 4,2%, segundo a análise da IDC. Uma outra marca que não aparece listada nos números da IDC, a Hama, diz à *Exame Informática* ter vendido um total de 16 mil câmaras de videovigilância em Portugal no ano de 2021 e cerca de 3700 só no primeiro mês deste ano.

E o que pode parecer uma compra relativamente pacífica – a aquisição de câmaras para uso em ambiente doméstico – é também na realidade um ponto de conflito bastante comum. Segundo o mais recente relatório de atividades da


Foto: M.B.

Comissão Nacional de Proteção de Dados (CNPD), só no ano passado, a CNPD recebeu 1041 denúncias relacionadas com sistemas de videovigilância e de dados biométricos, sendo que "as matérias que mais foram reportadas prendem-se com a videovigilância no local de trabalho e no contexto das relações de vizinhança".

## OS NÚMEROS DO FENÓMENO

Começa a ser difícil, sobretudo nas grandes cidades, entrar num espaço comercial – seja um supermercado, uma loja de roupa ou um restaurante – sem ser apanhado por uma ou mais câmaras de videovigilância. Nem sempre reparamos, mas estão lá. E no dia em que começar a ficar mais atento, talvez acabe surpreendido pelo elevado número de câmaras que existem. Isto se não ficar entretanto com os números que lhe revelamos.

Um estudo, de 2015, da consultora IHS (que agora se chama Omdia) apontava para a existência de 250 mil câmaras de videovigilância em Portugal. Mas desde então esse número tem vindo a aumentar significativamente. Segundo dados da CNPD, no ano de 2015 foram emitidas 10.883 autorizações de videovigilância, em 2016 foram 11.637 as autorizações, em 2017 foram 12.580 e em 2018 foram 6.090 as autorizações concedidas. O número mais baixo em 2018 deve-se à entrada definitiva em vigor, durante o mês de maio, do Regulamento Geral da Proteção de Dados (RGPD), segundo o qual deixou de ser necessário fazer um pedido prévio de autorização à autoridade nacional em matéria de dados pessoais para a instalação de um sistema de videovigilância. Contas feitas, entre 2015 e 2018, a CNPD concedeu um total de 41.190 autorizações para sistemas de videovigilância e, segundo inúmeros pareceres desse período consultados pela *Exame Informática*, implicam na esmagadora maioria a instalação de mais do que uma câmara por autorização.

Uma tendência confirmada por Carlos Vaqueirinho, diretor-geral da Prosegur em Portugal, cujos clientes instalam, em média, "duas a três câmaras" de videovigilância por estabelecimento comercial. Só esta empresa de segurança tem instaladas 31.366 câmaras por todo o País e o número de sistemas de videovigilância instalados em pequenas e médias empresas não para de aumentar. "Desde a fase pré-covid até à data, [o crescimento] foi de 30%", revela o executivo, que confirma que sete em cada dez clientes da Prosegur são empresas, enquanto os restantes são utilizadores domésticos. Dos 91 mil clientes que a Prosegur tem no mercado português, 16% utilizam câmaras de videovigilância IP (as que são conectadas e permitem a transmissão de imagens pela internet) ou CCTV (sigla inglesa para Closed-Circuit Television, ou circuito fechado de televisão em tradução livre, que significa que a gravação de vídeo é feita num circuito interno, associado a um gravador de imagens).

> "TEMOS VINDO A FAZER UM INVESTIMENTO CADA VEZ MAIOR NA PARTE DE VÍDEO, NA PARTE DAS CÂMARAS. OS CLIENTES PEDEM CADA VEZ MAIS SOLUÇÕES DE VIDEOVIGILÂNCIA"
>
> **MARTA ALVES**
> DIRETORA DE TECNOLOGIAS DA INFORMAÇÃO DA SECURITAS DIRECT

Já a Securitas Direct, outra das grandes empresas de segurança privada em Portugal, não revela o número exato de câmaras de videovigilância que tem instaladas, mas Marta Alves, responsável pela área de Tecnologias de Informação (T.I.) da empresa, adianta que "são dezenas de milhares". Há, no entanto, um valor que a empresa partilha, por ser uma nova aposta da Securitas Direct – as câmaras de videovigilância Arlo. A Arlo é uma empresa americana de videovigilância comprada pela Verisecure (empresa que detém a Securitas Direct) em novembro do ano passado e cujas câmaras destacam-se pela integração de funcionalidades baseadas em mecanismos de Inteligência Artificial, como a capacidade de distinguir pessoas, animais ou até encomendas deixadas à porta. Desde este negócio que as câmaras instaladas pela Securitas Direct são exclusivamente da Arlo e, em Portugal, só desde o início do ano, já foram instaladas 2500. Um número que continua a crescer a grande ritmo: todos os meses são instaladas cerca de 200 novas câmaras pela empresa. "Temos feito um investimento cada vez maior na parte de vídeo, na parte das câmaras", justifica Marta Alves.

Por estes valores já se percebe que existem largas dezenas de milhares de câmaras de videovigilância em Portugal. Mas a dimensão desta tecnologia é muito maior – e mais difícil de medir.

## UM MAR DE CÂMARAS

Supermercado. Um local visitado com frequência por um grande número de portugueses. E garantidamente um dos locais mais vigiados da sua região. É que num único supermercado chegam a ser instaladas centenas de câmaras de videovigilância. "Se falarmos numa loja Continente, das maiores, algumas podem chegar às 300 câmaras", revela Bruno Bento, diretor de vendas para Portugal da Hikvision, um dos maiores vendedores do mundo de sistemas de videovigilância e também um dos maiores no mercado nacional. "Só para lhe dar uma ordem de grandeza, a loja maior do Continente é a do Colombo e só o sistema de contagem de pessoas levou 60 câmaras", detalha. Já outras tipologias de loja têm um número

mais reduzido de câmaras instaladas. "Se falarmos de uma Modalfa, falamos em 20 câmaras, 30 câmaras [por loja]", acrescenta. Mas até um dos maiores fornecedores de equipamentos do mercado nacional tem dificuldade em saber ao certo quantas câmaras de videovigilância existem. "Para a Hikvision, como líder de mercado e a faturar o que tem faturado, é quase impossível termos noção do número de dispositivos instalados", confidencia Bruno Bento. Já Norberto Barroca, diretor de vendas da Bosch, outro grande fabricante de câmaras de videovigilância, diz que a tecnológica coloca três mil novas câmaras todos os anos no mercado português.

Outros exemplos de quão prevalecente é a videovigilância no nosso dia-a-dia. Durante uma apresentação no Proteger 2022, o maior evento de segurança que se realiza em Portugal a cada dois anos, Paulo Gonçalves, do gabinete de prevenção e segurança da Caixa Geral de Depósitos, revelou que o banco tem instaladas 7.935 câmaras de videovigilância nos seus diferentes espaços. Já numa infraestrutura como o aeroporto de Faro existem 300 câmaras de videovigilância, confirma o intendente Mário Oliveira, do comando distrital da PSP de Faro. E Filipe Araújo, vice-presidente da Câmara Municipal do Porto, responsável pela área de Inovação e Transição Digital, adianta que "todos os equipamentos municipais – escolas, piscinas, bibliotecas, museus [da cidade] – têm sistemas de videovigilância. Estamos a falar de muitas [câmaras] mesmo". Quantas, ao certo, isso não sabe. Uma notícia do jornal *Público*, de setembro de 2021, dava conta que só nas escolas portuguesas há mais de dez mil câmaras de videovigilância instaladas.

Quem também tem uma infraestrutura gigante de videovigilância é o Auchan: são mais de sete mil câmaras que vigiam um total de 95 instalações, entre supermercados, gasolineiras e plataformas logísticas da empresa. Num único espaço, como o supermercado em Paço de Arcos, tem mais de 100 câmaras instaladas, adianta Silvestre Machado, diretor de segurança do grupo. "O cliente não tem a perceção, nem se preocupa em ter essa perceção do número de câmaras, o cliente quer é sentir que está num espaço seguro", comenta sobre o elevado número de equipamentos de videovigilância num único espaço comercial.

## VIDEOVIGILÂNCIA NAS RUAS CONTINUA A AUMENTAR

Mas também a videovigilância no espaço público – que está expressamente proibida a todas as pessoas e empresas (segundo a lei n.º 58/2019, "as câmaras não podem incidir sobre vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel) – está a aumentar. Somente as forças e serviços de segurança – como a Polícia de Segurança Pública (PSP) e a Guarda Nacional Republicana (GNR) – e a Autoridade Nacional de Emergência e Proteção Civil é que o podem fazer, com a autorização expressa do Ministério da Administração Interna (MAI). Uma análise da *Exame Informática* a pareceres da CNPD e a despachos do MAI mostra que já foi autorizada a instalação e a utilização de 900 câmaras de videovigilância em ruas de cidades (em setembro do ano passado, o jornal *Público* noticiava que à época eram 850) – e sabe a *Exame Informática* que este número vai ultrapassar as mil câmaras em breve. Filipe Araújo, da Câmara Municipal do Porto, revela-nos que apesar de o município já ter recebido autorização para a instalação de 79 câmaras de videovigilância, na realidade quer instalar um total de 196, sendo que o pedido para a instalação das restantes 117 já está do lado do MAI. E também o intendente Mário Oliveira revelou que está a ser ultimado o pedido de alargamento do sistema de videovigilância pública de Olhão – vão ser requisitadas mais 38 câmaras para juntar às 26 já existentes, o que fará com que Olhão fique com 64 câmaras. Mas sobre os sistemas públicos de videovigilância, a sua eficácia e impacto na privacidade dos cidadãos, poderá ler mais na segunda parte desta investigação, a ser publicada na próxima edição.

O número de câmaras nas ruas pode até não ser considerado elevado, se pensar em quantas câmaras há só no supermercado que costuma frequentar. E é justamente nos supermercados que já está a ser usada a próxima geração de sistemas de videovigilância. Um cenário que de futurista tem muito pouco – a videovigilância com reconhecimento facial, análise de dados e até de comportamentos já está a acontecer em Portugal. ■


**O Auchan tem mais de 7000 câmaras instaladas nos seus espaços e controla-as num único sistema, que centraliza toda a segurança da empresa**

# MUITO MAIS DO QUE CÂMARAS

São 1270 metros quadrados de área e que incluem de tudo um pouco – um quarto de repouso, um pequeno ginásio com máquinas, salas de reuniões, um gabinete de crise (foi pensado para situações como sequestros de loja, mas até agora só foi usado em simulacros), um laboratório para testes de equipamentos e até uma loja fantasma. Esta "ghost store", como lhe chama Silvestre Machado, é uma loja fictícia, mas recriada como uma loja real – tem pórticos anti-roubo, prateleiras e muito aparato tecnológico. É aqui que são colocadas à prova muitas das tecnologias que o grupo Auchan pretende instalar nas suas lojas. O diretor de segurança, cargo que ocupa desde 2014, conhece como ninguém os cantos à casa e é quem nos leva, sala após sala, a perceber o que faz do Auchan Portugal um caso tão distinto em matérias de segurança.

Mas é só quando entramos na sala de operações que sentimos que estamos, de facto, num dos maiores centros de segurança e videovigilância do país. A partir desta sala, o Auchan consegue ter controlo sobre praticamente todos os elementos que existem nas lojas – e para o demonstrar, Silvestre Machado fez questão de pedir a um dos seguranças em serviço que desligasse um eletrocutor de moscas num supermercado em Viseu. E durante vinte segundos, alguma mosca que ali estivesse voou mais descansada.

Naquela sala são geridas mais de sete mil câmaras de videovigilância, mas o que nos chamou a atenção foram as imagens de uma câmara específica numa das duas paredes de vídeo gigantes que a empresa tem – pequenos quadrados apareciam e desapareciam à volta das caras das pessoas. Por que razão aquela câmara é diferente? Porque é capaz de fazer reconhecimento facial.

Nos últimos anos as câmaras de videovigilância passaram a fazer muito mais do que vigiar, graças à Inteligência Artificial e às suas subcategorias, como a aprendizagem automática (machine learning) e a aprendizagem aprofundada (deep learning). Na prática, estes mecanismos usam técnicas diferentes de computação para extrair informação – dados – do vídeo captado pelas câmaras. É a chamada analítica de vídeo, que pode variar muito na sua finalidade. "Há câmaras que têm duas, três, quatro, cinco analíticas, para detetar uma intrusão, uma entrada numa zona [delimitada], uma contagem de pessoas. Por exemplo, as câmaras de sistemas inteligentes de transportes já conseguem dar informação da matrícula, da cor, do modelo e da marca do carro, se a pessoa vai ao telefone ou se traz o cinto", exemplifica Bruno Bento, do fabricante Hikvision.

## O QUE DIZ A SUA CARA?

A câmara do Auchan é um caso único por ter reconhecimento facial a ser usado num espaço comercial em Portugal. A câmara esteve meses em testes internos na loja fantasma da empresa e está agora há cerca de três meses a ser testada em ambiente real numa loja na área da grande Lisboa – a empresa pediu, por motivos de segurança e confidencialidade, que a localização exata da mesma não fosse revelada. O reconhecimento facial desta câmara é feito de forma vectorial. Isto significa que "o sistema vai buscar um certo número de pontos [da cara do cliente]", explica Silvestre Machado. Estes pontos são usados para criar uma máscara (também conhecida como

Foto: J.C.C.

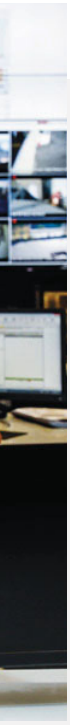


Foto: J.C.C.

"SE TIVER ALGUÉM QUE SÓ VEM À MINHA LOJA OFENDER OU FURTAR, O SISTEMA DIZ-ME 'A PESSOA QUE VOCÊS QUEREM COMUNICAR ÀS AUTORIDADES, PROVAVELMENTE ESTÁ AGORA NA LOJA'"

**SILVESTRE MACHADO**

DIRETOR DE SEGURANÇA DO AUCHAN RETAIL PORTUGAL

template) que é única para cada pessoa – uma espécie de impressão digital criada a partir das feições do rosto de cada pessoa. A informação extraída (distância entre os olhos, posicionamento do nariz face aos olhos, etc) é denominada de metadados, informação essa que é usada para criar o template, que posteriormente é guardado, encriptado, numa base de dados. Se entrar na loja do Auchan hoje e amanhã, o sistema será capaz de perceber que a mesma pessoa esteve duas vezes naquele local, mas o Auchan não sabe efetivamente quem é aquela pessoa, nem qual o seu nome. "Temos autorização da CNPD. Não associamos dados pessoais a nenhuma pessoa [identificada pela câmara]" (...) Trabalha por metadados, não sabemos quem é aquela pessoa", garante Silvestre Machado.

Por agora, a empresa só está a testar a eficácia do sistema. E Silvestre Machado assegura-nos que é altamente eficaz. Na prática o que a câmara faz é gerar uma


**O software de análise de comportamentos por videovigilância da Veesion já está a ser usado em mais de 50 lojas em Portugal**

probabilidade de um determinado rosto de um cliente corresponder a um rosto que está guardado na base de dados. Segundo os testes da empresa, sempre que a correspondência é igual ou superior a 67%, "não há erros", ou seja, a partir desse valor de correspondência a pessoa é sempre corretamente identificada pela câmara. Mas as capacidades desta supercâmara do Auchan vão ainda mais longe: é igualmente capaz de identificar se a pessoa que entra na loja é do género masculino ou feminino, também faz uma estimativa da idade média da pessoa e avalia ainda se está – ou não – bem disposta. "Isto são tecnologias novas que ainda estão em teste, não estão ainda a ser exploradas", garante. No futuro, poderá ajudar a identificar uma pessoa específica em loja em poucos segundos. "Com esta mesma solução de metadados, se tiver alguém que só vem à minha loja ofender os clientes, ter comportamentos abusivos ou só para furtar, não sei quem é esse cliente, não quero saber o nome, mas com a mesma solução, posso meter o fotograma do cliente e o sistema diz-me 'a pessoa que normalmente vem cá, vai embora, provoca danos e vocês querem comunicar às autoridades, provavelmente está agora na loja'", exemplifica Silvestre Machado.

A Hikvision também confirma à *Exame Informática* que já vende equipamentos com reconhecimento facial no mercado português. "Temos câmaras que têm essa possibilidade de reconhecimento facial. Nós no reconhecimento facial temos a possibilidade de a fazer na câmara ou ter uma base de dados por trás", explica. Igualmente Marcos Paulo Lima, diretor-geral da Visiotech Portugal, empresa de sistemas de segurança, confirmou-nos durante o evento Proteger 2022 que a empresa também vende câmaras de reconhecimento facial no mercado português. Enquanto nos explicava como o sistema funciona – também por sistema vectorial – uma câmara da marca Safire captou o nosso rosto dezenas de vezes em poucos minutos. "Antes [o cliente] tinha de comprar a licença de reconhecimento facial à parte. [Agora] Podemos colocar a base de dados [com deteção de rosto] no gravador", explicou. E ter a funcionalidade de reconhecimento facial numa câmara já é possível num equipamento que custa cerca de 100 euros.

**Cerca de 10% das câmaras de videovigilância do Auchan já são capazes de fazer análise inteligente das imagens captadas**

Se o reconhecimento facial é um dos mais avançados sistemas de IA aplicado às câmaras de videovigilância, garantidamente não é o único.

## CUIDADO COM OS MOVIMENTOS

A *Exame Informática* revelou, no início de junho, que já há 50 espaços comerciais em Portugal, como super e mini mercados – das insígnias Intermarché, Mini Preço, Coviran e Aqui é Fresco –, joalharias e farmácias, que estão a usar um algoritmo de Inteligência Artificial para analisar o comportamento dos clientes, através de gravações feitas por câmaras de videovigilância, com o objetivo de detetar e evitar o roubo de produtos. A tecnologia é da empresa francesa Veesion, que está desde fevereiro a trabalhar diretamente no mercado português. E o número de lojas com este software de análise comportamental vai continuar a aumentar, segundo as expectativas de João Madeira, representante da Veesion em Portugal. "Daqui a um ano quero ter 500 lojas com o nosso serviço", adianta.

Este software, na prática, deteta potenciais roubos em tempo real, inclusive de objetos tão pequenos quanto um parafuso. O software da Veesion trabalha sobre as imagens captadas pelos sistemas de videovigilância existentes nos espaços comerciais. O algoritmo analisa o movimento da cabeça, tronco e membros para identificar padrões que se assemelhem, em termos de comportamento, aos movimentos feitos durante um roubo. "Estamos a falar de clientes tirarem produtos das prateleiras e meterem no bolso, no casaco, em malas ou mochilas da escola", explica João Madeira. Imaginando que alguém mete uma lata de feijão ao bolso e não no carro de compras, o algoritmo

Fotos: M.B.


**Lisboa, Amadora, Coimbra e Olhão estão entre as cidades que já têm sistemas de videovigilância em funcionamento**

atribui uma classificação àquela ação. Depois cabe ao segurança da loja decidir se vai agir. A taxa de erro deste sistema de análise comportamental é de 5%. "Em cem notificações, cinco são falso alarme. Vale a pena. Se 95 notificações em cada 100 forem um alarme real e que se trata de um movimento de furto, então vale a pena ter o serviço", atira João Madeira.

O responsável garante ainda que a tecnologia da Veesion identifica movimentações, não identifica pessoas. "Não identifica raças, sexos, alturas, idades. Ele vai identificar seres humanos, vai subdividir as partes do corpo e o que faz é uma leitura puramente comportamental. Não há qualquer tipo de discriminação associada ao nosso serviço", garante. Mas há outro tipo de impactos que esta tecnologia pode ter, por exemplo, no número de seguranças contratados. "Neste momento, em algumas lojas, há três, quatro seguranças, mais um a olhar para as câmaras. Se a nossa solução realmente funciona, [as lojas] não precisam de fazer um investimento tão grande em segurança. Basta ter um, dois seguranças a receber as notificações e a agir perante elas".

## SUPER-VIGILÂNCIA TENTA CHEGAR AO ESPAÇO PÚBLICO

Em janeiro de 2020, a Comissão Nacional de Proteção de Dados emitiu dois pareceres negativos para a instalação de câmaras de videovigilância com tecnologia de Inteligência Artificial, nas cidades de Portimão e de Leiria. Os casos tornaram-se amplamente mediáticos por terem sido os primeiros nos quais se tentou usar funcionalidades de IA em videovigilância em espaço público. Mas pareceres analisados pela *Exame Informática* mostram que vários outros municípios portugueses têm tentado obter aprovação para a instalação de sistemas de videovigilância com Inteligência Artificial no espaço público, incluindo com reconhecimento facial.

Quando a Câmara Municipal da Amadora pediu o alargamento do sistema de videovigilância que existe na cidade, de 103 para 141 câmaras, pretendia que o sistema fosse capaz de fazer a "monitorização da circulação das pessoas, viaturas e bens". No pedido submetido, o município queria também que o sistema tivesse capacidade de deteção de faces, deteção de movimento e deteção de objetos abandonados. A análise da CNPD foi muito clara. "É por demais evidente a ausência de fundamento de licitude da realização do tratamento de dados pessoais por via de reconhecimento facial em sistema de videovigilância num espaço público como o da cidade da Amadora". Porquê? Os riscos para a privacidade dos cidadãos são demasiado elevados. "Não há apenas afetação da liberdade individual de circulação e de comportamento. Há também um risco elevado de perturbação da sociedade democrática, como em outros pontos do mundo tem vindo a ser demonstrado", concluiu a CNPD.

Já a Figueira da Foz tenciona instalar câmaras que têm funcionalidade de reconhecimento facial. No pedido que fez ao MAI, o município diz que "tais capacidades não serão utilizadas e ficarão desligadas". Mas a CNPD lembra que "ainda que desligadas, [as funcionalidades] permanecem disponíveis no referido software e, portanto, são suscetíveis de ativação. (...) Recomenda-se, assim, que (...) seja proibida expressamente a ativação das funcionalidades de IA que permitem reconhecimento facial e o rastreamento dos cidadãos". O MAI proibiu, de facto, o uso do reconhecimento facial neste sistema. Mas a capacidade está lá.

Também a cidade de Albufeira ("aptidão do sistema de videovigilância para identificar cidadãos a partir de características físicas e o rastreamento dos mesmos") e do Porto (analítica de vídeo capaz de gerar alarmística que ajude o operador) fizeram pedidos de videovigilância com capacidades inteligentes, que mereceram parecer negativo da CNPD e foram recusadas pelo MAI. Filipe Araújo, da CM Porto, confirma no entanto à *Exame Informática* que o município não vai desistir do uso da analítica de vídeo no sistema que quer instalar na cidade. "A CNPD disse que precisava de mais informação e [é] onde estamos a trabalhar", adianta o vice-presidente. "O sistema de interpretação de imagens que queremos pôr em cima da mesa tem essa função, como é que consegue ajudar a que o olho do polícia consiga estar mais atento a uma zona onde é potencialmente mais previsível que aconteça ilícitos e não estar a olhar para as câmaras todas ao mesmo tempo".

E os receios de potenciais más utilizações de sistemas de videovigilância, sobretudo os que permitem análise avançada de vídeo, têm algum fundamento. Num País com cada vez mais videovigilância, são muitos os sistemas que são usados à margem da lei, incluindo em carros da Tesla. ■


# ALERTAS NA VIDEOVIGILÂNCIA

"Se houver uma [equipa de] fiscalização, não vai cansar-se muito. Ao saírem das instalações, podem começar logo a parar. Quase que podem ir a pé e é muito fácil de encontrar". É assim que Sílvio Gomes, especialista em proteção de dados e de segurança da informação na empresa Compliance Way, coloca o estado das irregularidades em sistemas de videovigilância. "Pode a minha amostra não ser representativa, desconfio que é, porque já faço auditorias há bastante tempo e ando pelas organizações também em consultoria, em especial no âmbito da proteção de dados, e não tenho ideia de ter encontrado um sistema de videovigilância que respeitasse a lei", analisa.

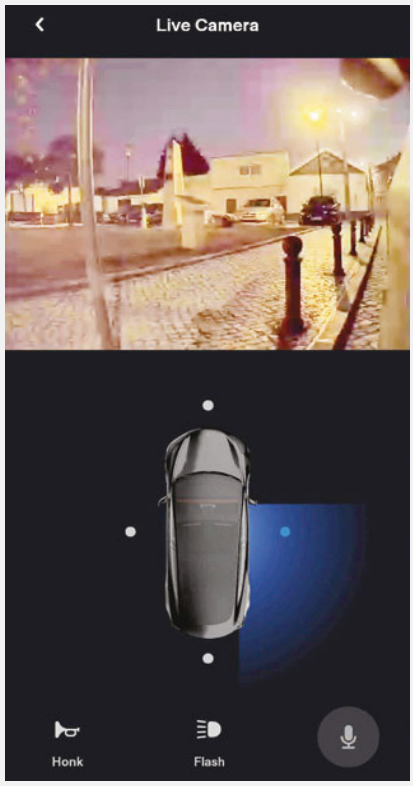
Os números da Polícia da Segurança Pública são ilucidativos – todos os anos são identificadas centenas de irregularidades em sistemas de videovigilância. Entre 2018 e 2020, a PSP detetou 655 irregularidades, de acordo com dados do Relatório de Segurança Privada de 2020 (o mais recente à data do fecho de edição). E dos últimos três anos conhecidos, 2019 foi o que mais se destacou pelo número de irregularidades detetadas: 125 locais tinham falta de sinalização do sistema de videovigilância; 124 não conservaram as gravações de imagem por um prazo de 30 dias; 53 não destruíram, num período de 48 horas após os 30 dias definidos, as gravações de imagens; e 23 dos sistemas inspecionados não garantiam o funcionamento efetivo dos sistemas de segurança. Em 2020, houve uma diminuição significativa das fiscalizações a sistemas de videovigilância, consequência direta da pandemia na atividade das forças de segurança. Ainda assim, só nesse ano foram detetadas 200 irregularidades pela PSP.

Já das fiscalizações realizadas pela GNR, em 2019 foram 97 as infrações detetadas e em 2020 foram 75, igualmente com destaque para a não conservação das imagens por 30 dias, a falta de avisos e símbolos de que está a ser realizada videovigilância num espaço comercial (ou seja, há câmaras e as pessoas não são informadas disso), e foram ainda detetados "sistemas à margem dos requisitos legais".

> "A VIDEOVIGILÂNCIA É MAIS UM INSTRUMENTO [PARA O TRABALHO DA POLÍCIA] E NESTE MOMENTO JÁ É IMPORTANTE. (...) NÃO SENDO O ÚNICO, É MUITO ÚTIL"
>
> **MÁRIO OLIVEIRA**
> INTENDENTE DO COMANDO DISTRITAL DE FARO DA POLÍCIA DE SEGURANÇA PÚBLICA

O ambiente de autorregulação que existe em Portugal será tanto mais eficaz, quanto mais fiscalização houver, considera Sílvio Gomes. "A grande debilidade, que é constante também em outras áreas, então na proteção de dados nem se fala, é o problema da fiscalização. Temos aqui um problema – não existe autorregulação por parte das organizações se não houver um ambiente de fiscalização".

Também Jorge Martinez Batalha, formador, encarregado de proteção de dados e fundador da empresa Protec Dados, alerta para um cenário de muitas irregularidades que encontra enquanto consultor nesta área. "Há muitas ilegalidades. A minha dissertação de mestrado focou-se em videovigilância em contexto laboral. E com muita tristeza minha, hoje a situação é pior do que em 2017 [ano de publicação da tese]", conta. "Já tenho visitado vários clientes onde chego ao escritório, ao gabinete do diretor, e tem um monitor grande com as imagens todas. Então aqueles que têm pequenas lojas... É prática comum. Há um controlo regular e sistemático sobre o desempenho profissional dos trabalhadores. Isto é inadmissível. Mas como as pessoas estão numa condição vulnerável, sujeitam-se", denuncia. A


**O Modo Sentinela permite, através da aplicação para smartphone, usar as câmaras do Tesla para ver em tempo real o que está a acontecer nas imediações do carro. Quando alguém se aproxima muito, no ecrã, surge um aviso de que está a ser feita uma gravação**

CNPD refere, no relatório de atividades de 2021, justamente que as câmaras em local de trabalho está entre as causas que mais queixas geraram na videovigilância.

## O RELATÓRIO DEMOLIDOR DA CNPD

A Comissão Nacional de Proteção de Dados é a entidade responsável por fiscalizar os sistemas de videovigilância em espaços públicos, que estão à responsabilidade da PSP. E nas inspeções feitas, a CNPD verificou muitas, muitas falhas. Há de tudo um pouco: câmaras de videovigilância com firmware desatualizado (algumas tinham as mesmas versões de software desde o momento em que foram instaladas); num dos sistemas inspecionados, a sala usada como centro de dados "era o único caminho de passagem para o vestiários dos agentes"; num outro caso, a rede do sistema de videovigilância estava a ser partilhada com a rede do município; a CNPD detetou ainda acessos aos sistemas de videovigilância por utilizadores que não estavam autenticados no sistema; câmaras com filtros (as chamadas máscaras), para tapar as portas, janelas e varandas de casas de cidadãos, mal posicionados; e, talvez a 'cereja' deste relatório demolidor, havia um sistema de videovigilância que tinha instaladas as aplicações Facebook, Netflix, Royal Revolt2 e Twitter quando deveria estar a funcionar numa rede isolada. "A simples existência e utilização deste tipo de software apresenta vetores de risco inadmissíveis num sistema de videovigilância das forças de segurança".

Quando questionado sobre o que melhorou após este relatório da CNPD, o intendente Mário Oliveira, da PSP, considera que regulador encontrou "vulnerabilidades, mais do que irregularidades". "Eles não reportaram extração de dados, ou seja, eles não informaram que os dados tinham sido usados de forma incorreta ou tinham sido extraídos. Informavam era situações [que] apresentavam vulnerabilidades que, no limite, alguém mal intencionado poderia aproveitar para fazer essa extração. Aquilo que estamos a tentar é, nesta nossa aprendizagem, corrigir essas vulnerabilidades". Na próxima edição, poderá ler com maior detalhe sobre o uso que a PSP faz dos sistemas de videovigilância.

## PSP NÃO TEM CONTROLO SOBRE VIDEOVIGILÂNCIA

Outra das críticas apontadas pela CNPD é à forma como os sistemas de videovigilância pública estão contratualizados – como são as câmaras municipais a financiá-los, fazem contratos com empresas instaladoras. Conclusão? "A PSP não tem legitimidade para exigir qualquer apoio, correção ou atualização dos sistemas". Um cenário confirmado à *Exame Informática* pelo intendente Mário Oliveira. "Se corremos o risco de os sistemas serem desligados porque as Câmaras não querem? Claro que sim, agora, neste momento, a experiência que temos tido é positiva. Aquilo que nós protocolamos, até hoje as câmaras cumpriram o protocolo", sublinha.

Mas há outra achega da CNPD que faz soar os alarmes – segundo o regulador da área da privacidade, os perfis de administração do sistema de videovigilância, aqueles que permitem realizar todo o tipo de operações, incluindo as de maior sensibilidade, "não pertencem a agentes da PSP, que os desconhecem, mas antes a pessoas das empresas prestadoras de serviços". Ou seja, as contas com maiores privilégios de acesso aos sistemas de videovigilância de acesso público não estão sequer na posse da PSP.

## O CASO SINGULAR DOS TESLA

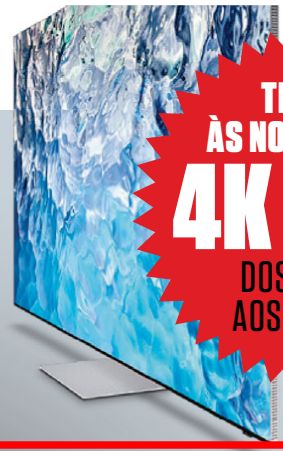
É um dos fabricantes automóveis mais conhecidos do mundo e desenvolve tecnologia de ponta que integra nos seus veículos. Mas aquela que é uma das funcionalidades mais conhecidas dos veículos Tesla, o Modo Sentinela (Sentry Mode, em inglês), é um exemplo paradigmático de sistemas de captação de imagem à margem da lei. Segundo a opinião dos especialistas ouvidos pela *Exame Informática*, a utilização do Modo Sentinela dos Tesla é ilegal. Este modo ativa as várias câmaras integradas no veículo e sempre que, quando estacionado, alguém se aproxima demasiado, faz captação de imagens. Esta até poderia ser uma funcionalidade de segurança para proteger o veículo, só que vai mais longe: os donos dos Tesla podem, através de uma aplicação para smartphone, aceder em tempo real e de forma remota às câmaras do veículo, que estão a captar a via pública. "Eu tenho um Tesla estacionado à frente de uma escola, é legal o carro estar a filmar as crianças?", coloca como cenário Sérgio Silva, da CyberS3c. "[O uso do Modo Sentinela] É ilegal. Conforme está na lei portuguesa, quem pode recolher imagens, sejam gravadas ou em tempo real da via pública são só as forças e serviços de segurança. Mais ninguém pode recolher imagens da via pública", considera Jorge Martinez Batalha, que vai mais longe na forma como aborda a questão: "Nem a polícia cá em Portugal pode andar com câmaras dentro do carro!". A *Exame Informática* questionou a Tesla, que não respondeu a tempo do fecho desta edição. Mas no site oficial, a marca diz que a responsabilidade do uso do Modo Sentinela é do utilizador final.

E se pensa que a discussão sobre o tema da videovigilância acaba aqui, engana-se. Só agora está a começar. ■

EXAME INFORMÁTICA
PARA QUEM GOSTA DE TECNOLOGIA
SETEMBRO 2022 • N.º 327 • MENSAL • ANO 27 • €4,10 • PORTUGAL CONTINENTAL
EXAMEINFORMATICA.PT • FACEBOOK.COM/EXAMEINFORMATICA •
VIGIADOS!
327 SETEMBRO 2022

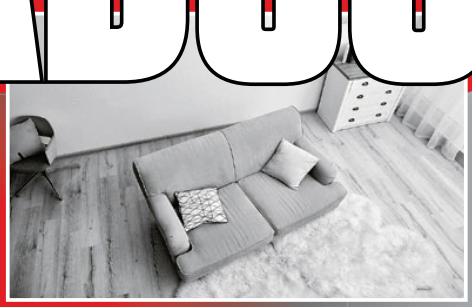
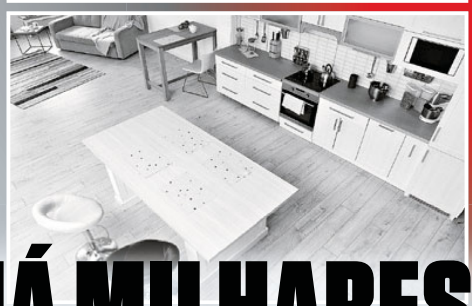
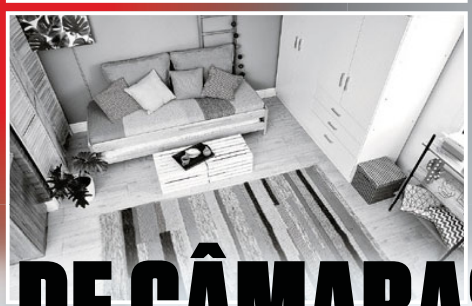
# ESPECIAL SMART CITIES

# EXAME INFORMÁTICA



**TESTE ÀS NOVAS TVs 4K E 8K**
DOS €800 AOS €6000

# VIGIADOS!

## HÁ MILHARES DE CÂMARAS VULNERÁVEIS EM PORTUGAL

### VIDEOVIGILÂNCIA AUMENTA E JÁ INCLUI RECONHECIMENTO FACIAL

ESPECIALISTAS ALERTAM PARA SISTEMAS ILEGAIS E DIZEM COMO ATÉ OS TESLA ESTÃO À MARGEM DA LEI

**FREEBUDS PRO 2 VS ENCO X2**
HUAWEI E OPPO: QUEM GANHA NA QUALIDADE DE SOM

**INZONE M9 E H9**
SERÁ A SONY CAPAZ DE INOVAR COM UM MONITOR E HEADSET PARA GAMERS?

**FOLD 4 E FLIP 4**
OS NOVOS DOBRÁVEIS DA SAMSUNG

**DVD**
ASTRONOMIA EM CASA
PEÇA O SEU NA BANCA!
€1,90
(CONT.)

**ENTREVISTA**
**HEIDEMARIE STEFANYSHYN-PIPER**
ASTRONAUTA DA NASA

**GÉMEOS DIGITAIS**
O QUE SÃO E COMO ESTÃO A SER USADOS NA MEDICINA E INDÚSTRIA

**SPACE UNIVERSITY**
O QUE SE APRENDE NUMA ESCOLA FOCADA NO ESPAÇO

5 600384 017284 00327