Gonçalo Cerejeira Namora Seguir

Advogado, Associado Cerejeira Namora, Marinho Falcão

O olho que tudo vê

Temos casos no Oriente onde a implementação destas tecnologias levou à instalação de mais de um milhão de câmaras na China, num sistema de "crédito social" que enforma um autêntico big brother social.

28 jan 2020, 07:42 5

Muito se tem falado sobre os polémicos (ou nem tanto) Pareceres da CNPD sobre o pedido de autorização de instalação de sistemas de videovigilância solicitados pela PSP ao MAI. O prisma de análise tem sido mais político do que técnico, o que forçosamente tolda ou limita a opinião pública.

Urge, todavia, centrar as atenções naquele que acreditamos ser o prisma preponderante: a protecção dos direitos fundamentais dos cidadãos, nomeadamente do direito à privacidade, à liberdade, identidade pessoal e à não discriminação.

De certo modo, é inevitável concluir que todos nós, em maior ou menor grau, temos vindo a desvalorizar a nossa privacidade e até mesmo a comprometê-la, muitas vezes por falta de conhecimento do alcance e impacto dos recursos tecnológicos ao nosso dispor, outras por mera comodidade.

O desbloqueio de smartphones por representação da impressão digital ou reconhecimento facial e o upload de fotografias para plataformas ou apps lúdicas (como por exemplo a Faceapp) são alguns dos exemplos de como amiúde vamos fragilizando o controlo sobre os nossos dados pessoais.

É certo que também compete a cada um de nós a adopção de uma atitude consciente e informada sobre o modo como utilizamos a tecnologia e expomos a nossa informação pessoal. Porém, questão significativamente diferente é a instrumentalização e utilização da tecnologia pelo Estado, quando daí possam advir perigos sérios e injustificados para os direitos e liberdades dos cidadãos.

É precisamente neste âmbito que os polémicos pareceres da CNPD se inserem. Com o mote da segurança e prevenção criminal, a CNPD averiguou a conformidade dos sistemas de videovigilância contínua de espaços públicos com recurso a Inteligência Artificial e tecnologia de *soft recognition*.

Os referidos sistemas de videovigilância permitem, entre outras funcionalidades, a gravação de vídeo com equipamentos que permitem a **rotação e ampliação de imagem**, a **captação de som**, a detecção automática de eventos anormais, a procura avançada por determinadas características físicas (sejam elas sexo, cor de cabelo, cores da roupa, tom de pele, etc.) e a leitura automatizada das placas de matrículas.

Por um lado e como bem asseverou a CNPD, a utilização destas tecnologias é idónea em alguns contextos, como será o caso da leitura de matrículas para auxiliar e facilitar a finalidade de deteção de infrações rodoviárias e a aplicação das correspondentes normas sancionatórias e a realização de ações de controlo

Gonçalo Cerejeira Namora Seguir

Advogado, Associado Cerejeira Namora, Marinho Falcão

de tráfego e o acionamento de mecanismos de prevenção e de socorro – o que, aliás, está expressamente previsto na Lei n.º 1/2005. Por outro lado, é fundamental garantir que o hardware e software que se pretende utilizar foram desenvolvidos de modo a garantir padrões éticos e morais e a diminuir o nível de intrusão nos direitos e liberdades dos titulares em função de cada uma das finalidades visadas.

A averiguação da conformidade do hardware e software terá de ser feita numa avaliação de impacto (DPIA) que assentará necessariamente em dois juízos de necessidade e proporcionalidade distintos: nos impactos da utilização dos sistemas de videovigilância e nos impactos recurso à IA e tecnologia de *soft recognition*.

Efectivamente, como refere a CNPD num dos seus pareceres, o cumprimento do regime jurídico de protecção de dados pessoais atinge-se pela forma como os recursos para tratamento de dados são concebidos e implementados. Contrariamente ao que tem sido veiculado pela opinião pública, a CNPD não coloca em causa as vantagens das tecnologias emergentes, escudando-se numa sobrevalorização da privacidade em detrimento de uma sociedade mais segura e de um sistema criminal mais eficaz.

As recomendações e cautelas reforçadas pela CNPD visam garantir que as implementações deste tipo de tecnologias não possam afectar de forma desproporcionada os direitos à privacidade e proteção de dados pessoais dos titulares, bem como que da sua utilização não poderão resultar decisões (por vezes automatizadas) capazes de consubstanciar acções discriminatórias. O tema não pode ser apreciado de forma leviana, pois temos exemplos no Oriente onde a implementação deste tipo de tecnologias levou já à instalação de mais de um milhão de câmaras na China, que monitoriza o comportamento dos cidadãos num sistema de "crédito social" que enforma um autêntico *big brother* social.

Afortunadamente, no mundo ocidental a opção estruturante foi a de afirmação e reforço dos direitos dos cidadãos à privacidade, da qual o RGPD e os diplomas conexos são um bom retrato. Todavia, impõe-se uma actualização legislativa que preveja os novos avanços tecnológicos concretamente nesta área. A Lei n.º 1/2005 (actualizada em 2012) não dá resposta a esta realidade e, conforme se comprova, há prementes necessidades de regulação da utilização da Inteligência Artificial. O primeiro passo pode passar por tornar as orientações do Comissão Europeia sobre ética e inteligência artificial divulgadas no final de 2018 como leitura obrigatória para o legislador nacional.

Na verdade, não acreditamos que seja avisado passar um "cheque em branco" para a utilização dos referidos sistemas de videovigilância com recurso a tecnologia de Inteligência Artificial e *soft recognition* sem serem detalhadamente conhecidos e escrutinados os algoritmos e as limitações da sua utilização em função das finalidades previamente consideradas como necessárias.