Big brother, big data & China. E se fosse em Portugal?

Joana Cunha de Miranda
Associada da Data Protection Team da CCA ONTIER



Martim Bouza Serrano
Associado Coordenador da Data Protection Team da CCA ONTIER



Os cidadãos chineses estarão a ser perfilados na sua condição de cidadão, como se a relação com o Estado de uma relação de prestação de serviços de Uber se tratasse.

Centremo-nos nas aplicações que fazem parte, hoje em dia, do nosso dia-a-dia: a *Uber*, em que se dá pontuação ao prestador de serviço e se é pontuado; o *Airbnb*, em que se regista a descrição do serviço que foi prestado, com as inerentes consequências ou a mais recente aplicação *Skorr* que mede a influência dos utilizadores nas redes sociais. Agora transponhamos essa realidade para a nossa relação com o Estado.

Comportamento criminal, irregularidades financeiras, o que se compra, o que se diz e o que se faz, difundir falsas informações sobre terrorismo, causar distúrbios em voos, utilização de bilhetes expirados ou fumar em comboios são comportamentos pelos quais todos os cidadãos podem ser banidos através do sistema de *scoring* ou "créditos sociais" que a China implementará a partir de 2020.

À partida, teríamos uma boa intenção e, no limite – no delírio semelhante ao que se vive na China –, até enquadraríamos este tratamento no fundamento de legitimidade de "interesse público importante": o interesse em controlar as massas, o interesse em que os cidadãos fossem cumpridores das suas obrigações fiscais e financeiras, o interesse em prevenir a criminalidade, entre muitos outros… Sucede que o sistema, tal como está feito, é opaco e desproporcional, uma vez que tanto os comportamentos mais graves como o simples facto de deixar bicicletas no caminho ou pedir desculpas que não sejam consideradas sinceras podem ter a mesma influência no *score*.

Este quadro, que mais parece um episódio retirado de um filme de ficção científica em que, de alguma forma, um *robot* adivinha o futuro com base em algoritmos assentes em dados recolhidos em massa (*big data*), já é uma realidade na China. Não é menos verdade, porém, que é um perigo iminente em todo o mundo, inclusive no nosso país. Assistimos, em Portugal, a uma proposta de lei de proteção de dados que isenta as autoridades públicas do pagamento de coimas por violação de regras de proteção de dados, que permite, na alegada prossecução de interesse público, que se tratem dados pessoais por entidades públicas para finalidades diferentes das que determinaram a recolha e que viabiliza a transmissão de dados pessoais entre entidades públicas, mediante um simples protocolo.

> **"Comportamento criminal, irregularidades financeiras, o que se compra, o que se diz e o que se faz, difundir falsas informações sobre terrorismo, causar distúrbios em voos, utilização de bilhetes expirados ou fumar em comboios são comportamentos pelos quais todos os cidadãos podem ser banidos através do sistema de *scoring* ou "créditos sociais" que a China implementará a partir de 2020"**

Isto equivale a dizer, por absurdo que pareça, que os dados de saúde recolhidos num certo hospital público, nomeadamente de doentes oncológicos, poderiam ser transmitidos a uma Câmara Municipal, mediante um protocolo para, por hipótese, predizer o número futuro de eleitores nessa cidade.

Esta intenção aparenta ser legítima se não consubstanciasse, flagrantemente, a rutura com todos os princípios de proteção de dados pessoais.

Desde logo, pois, de acordo com o princípio da finalidade, os dados pessoais não podem ser tratados (nem comunicados) para finalidade incompatível com a que determinou a recolha e, muito menos, para fins discriminatórios, que fazem do objeto do tratamento ilegal em si mesmo, independentemente dos fundamentos de legitimidade que possamos imaginar.

Supondo que o exemplo da China contaminava as nossas civilizações, importa referir que, mais do que a violação das regras de proteção de dados, deparamo-nos com a negação de serviços públicos essenciais, designadamente da negação da venda de bilhetes de comboio aos cidadãos, fundamentada na recolha de dados em massa dos cidadãos através da qual se presume o alegado "mau comportamento" dos mesmos, o que, por si só, assenta em critérios

que, por serem altamente vagos, imprecisos e falíveis, têm um potencial discriminatório colossal, sendo precisamente esse o risco que se pretende evitar com o *profilling*.

Valha-nos por cá a consagração dos direitos fundamentais à privacidade e à proteção de dados, com a inerente proibição de ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação e a remanescente proibição de atribuição de um número nacional único aos cidadãos, entre outras garantias…

A nível europeu, podemos socorrer-nos do Regulamento Geral de Proteção de Dados que, não obstante a faculdade que deu aos Estados-Membros para legislarem certas matérias que resultam em absurdos como o explicado anteriormente, consagrou, quanto ao chamado *profiling*, regras algo restritas.

Este tratamento de dados consiste em qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

As decisões individuais automatizadas, incluindo a definição de perfis, são admissíveis, no que toca a dados pessoais que não se insiram nas categorias especiais de dados, mediante o preenchimento de um dos fundamentos de legitimidade previstos no artigo 6.º do Regulamento Geral de Proteção de Dados.

Contam-se entre os fundamentos de legitimidade referidos o consentimento explícito do titular dos dados (suscetível de ser revogado a todo o tempo), a necessidade para execução de um contrato, a necessidade para cumprimento de uma obrigação legal, a necessidade para proteger interesses vitais do titular dos dados ou de terceiros, a necessidade para o exercício de funções de interesse público e a necessidade para a prossecução de interesses legítimos do responsável pelo tratamento, desde que não devam prevalecer os interesses ou direitos e liberdades fundamentais do titular dos dados.

Perante estas circunstâncias, o titular tem, no entanto, o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, exceto se o mesmo for necessário para a execução de um contrato entre o responsável pelo tratamento e o titular dos dados ou se for autorizado por lei da União Europeia ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito.

Por outro lado, as decisões automatizadas tomadas com base no tratamento de categorias especiais de dados[1] são, em regra, proibidas.

Excecionam-se os casos em que o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas (e não estivermos perante direitos indisponíveis) ou se o tratamento for necessário por motivos de interesse público importante.

Este tratamento está sujeito a especificidades exigentes, que, segundo o Grupo de Trabalho para a Proteção de Dados do Artigo 29.º[2], justificam-se pelo seu potencial discriminatório e de perpetuação da existência de estereótipos, uma vez que consiste na catalogação de titulares dos dados, restringindo-os a uma certa oferta de bens ou serviços e, consequentemente, enfraquecendo a sua liberdade no que toca à escolha de certos produtos ou serviços, como livros, música, notícias… Noutros casos, poderá levar a prognósticos imprecisos e interferir, de facto, nos seus direitos, produzindo efeitos na sua esfera jurídica ou afetando-o significativamente de forma similar. São os casos em que, através de um algoritmo, é tomada uma decisão automatizada (sem nenhuma intervenção humana) de recusa de um crédito ou de recusa de uma oferta de um emprego.

Concluindo, se fosse em Portugal, (ainda) haveria alguns obstáculos à implementação de uma *app* de "créditos sociais", obstáculos esses cuja preservação cabe ao olhar atento dos cidadãos na defesa dos seus direitos fundamentais, uma vez que o legislador, por vezes, entusiasma-se na atribuição de poderes ao Estado, com a consequente compressão dos direitos dos cidadãos.

"Concluindo, se fosse em Portugal, (ainda) haveria alguns obstáculos à implementação de uma *app* de "créditos sociais", obstáculos esses cuja preservação cabe ao olhar atento dos cidadãos na defesa dos seus direitos fundamentais, uma vez que o legislador, por vezes, entusiasma-se na atribuição de poderes ao Estado, com a consequente compressão dos direitos dos cidadãos"

1. Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
2. Orientação do Grupo de Trabalho para a Proteção de Dados do Artigo 29º sobre Decisões Individuais Automatizadas, incluindo Definições de Perfis, adotada a 3 de outubro de 2017 e revista a 6 de fevereiro de 2018.