



Inês de Castro Ruivo | Associada da Área de TMT da PLMJ

Anonimização de dados pessoais: o que deve saber

Escrito com Soraia Lopes, Estagiária da PLMJ

"If you think you've anonymized a data set, you're probably wrong"



A frase é do jornalista e autor Cory Doctorow e cai como uma pedrada no charco. Poderão os meus dados pessoais que foram anonimizados deixar ser... anónimos?

A dúvida é fundada, depois de este jornalista ter afirmado ser possível identificar as pessoas que viajaram de táxi, em Nova Iorque, bem como os respetivos trajetos, valores pagos e hábitos semanais a partir de um conjunto de dados, anonimizado, que foi disponibilizado pela entidade pública que licencia os conhecidos táxis amarelos da Big Apple.

A anonimização de dados tem um vasto campo de aplicação, podendo ser adotada como medida de segurança (por exemplo no âmbito das fases de desenvolvimento e teste de um novo software), ou como base para uma aplicação que permite, sem sair de casa, saber qual o tempo de espera na Loja do Cidadão mais próxima e, ainda, no âmbito da investigação clínica.

Em que consiste a "anonimização" de dados pessoais?

A expressão "anonimização" é ela própria vaga, uma vez que abrange uma diversidade de técnicas que podem ser usadas para converter dados pessoais em dados anonimizados.

Segundo a definição do Grupo de Trabalho Sobre a Proteção de Dados do Artigo 29.º (um órgão consultivo europeu independente, em matéria de proteção de dados e privacidade), "dados anonimizados" são dados relativos a uma pessoa identificada ou identificável que não pode, razoavelmente, voltar a ser identificada ou identificável. O critério da razoabilidade significa que o processo de anonimização deve ser suficientemente robusto, de tal modo que a reversão deste processo seja "razoavelmente impossível". A anonimização também é definida como "o processo pelo qual a informação pessoal identificável é irreversivelmente alterada, de tal forma que a informação pessoal identificável principal não pode mais ser identificada direta ou indiretamente, quer pelo responsável pelo tratamento, quer em colaboração com terceiros".



O que diz a Lei sobre a anonimização de dados?

A Diretiva em matéria de Dados Pessoais em vigor refere que as regras do tratamento de dados pessoais não são aplicáveis a dados tornados anónimos de forma irreversível. Significa isto que, de uma forma geral, será mais simples tratar e divulgar dados anonimizados do que dados pessoais.

Importa no entanto, ter em conta quatro pontos: qualquer entidade que recolha dados pessoais, ainda que com o objetivo de os anonimizar, está já a efetuar um tratamento de dados pessoais, estando por isso sujeita à lei em vigor e, ainda, qualquer operação de anonimização não eficaz cairá no escopo desta lei. Em acréscimo, é óbvio que qualquer entidade que recolha dados anonimizados e os submeta, sem consentimento dos titulares, a um processo de "re-identificação", estará a efetuar um tratamento de dados ilegal. Ainda, é um erro considerar que a aplicação de um processo de anonimização robusto anula quaisquer garantias dos titulares dos dados. Na verdade, existem regras que continuam a ser aplicáveis, como por exemplo a Diretiva relativa à Privacidade e às Comunicações Eletrónicas, a qual impõe limitações ao armazenamento ou acesso a qualquer tipo de informação, independentemente de estar anonimizada ou não.

Recomendações sobre boas práticas de anonimização

A Lei da Proteção de Dados Pessoais portuguesa não clarifica a forma como o processo de anonimização deve ser desenvolvido. Segundo o referido Grupo de Trabalho, um processo de anonimização suficientemente robusto significa que: (1) os custos e o conhecimento exigidos para implementar a reversão da anonimização devam ser consideravelmente elevados; (2) o próprio responsável pelo tratamento de dados não consegue identificar os titulares (se após o processo de anonimização, o responsável pelo tratamento não eliminar o ficheiro original, continuamos a estar perante dados pessoais); (3) Não é mais possível estabelecer relações entre os dados de tal forma que ainda seja possível identificar o seu titular.

Recomenda-se que os responsáveis pelo tratamento de dados considerem os riscos residuais de identificação, devendo proceder ao seu controlo, monitorização e reavaliação regular.

Assim, a solução ideal sobre o processo de anonimização que apresenta maior robustez deverá ser avaliada caso a caso, ponderando-se as consequências da "re-identificação dos titulares dos dados".

Terminando como começámos, com as palavras de Cory Doctorow, "anonymising data is a very, very difficult business".