United Kingdom

Investigatory Powers Tribunal: Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Ors Part II

*Teresa Quintel*

I. Introduction

Data retention and timely access to stored data may be useful for the fight against terrorism and to prevent threats to national security, as it provides a possibility to discover criminal networks, to locate perpetrators and to determine probabilities as to where criminal activity is likely to occur. At the same time, the analysis of large amounts of data poses risks to privacy and data protection rights, as datasets typically include information about individuals who are not related to criminal offences or perpetrators. While automated processing of personal data provides advantages, such as a decreased risk of biased results and is less privacy intrusive in the sense that it allows for reduced access to data by personnel, it poses at risk privacy and data protection rights, not only for the individuals directly involved in a crime, but certainly for those whose data coincidentally happen to be included in those datasets that are being analysed.

Intelligence agencies use Big Data surveillance technologies and bulk data acquisition from private bodies to identify links between terrorist networks and utilize data analysis to discover unknown threats to public security. At the same time, concerns regarding the legitimacy of shifting public powers to private parties for the performance of public functions are being voiced. The Court of Justice of the European Union (CJEU) progressively strengthened data subjects’ rights through its case law during the past years. Particularly Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter) have been an important factor for the Court’s interpretation of privacy and data protection rights.

In its Tele2/Watson judgment from 21 December 2016, the CJEU limited the possibility of national legislators to oblige telecoms providers to store the metadata of all their subscribers. By this judgment, the CJEU required data retention to be targeted and based on the objective evidence of serious crime. The Court set clear limits for the derogations under Article 15(1) of Directive 2002/58/EC (e-Privacy Directive), which had, after the invalidation of Directive 2006/24/EC (Data Retention Directive) in Digital Rights Ireland, been used to...