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.[1] At the same time, concerns regarding the legitimacy of shifting public powers to private parties for the performance of public functions are being voiced.[2]

The Court of Justice of the European Union (CJEU) progressively strengthened data subjects' rights through its case law during the past years.[3] 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*[4] 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[5] (e-Privacy Directive), which had, after the invalidation of Directive 2006/24/EC[6] (Data Retention Directive) in *Digital Rights Ireland*[7], been used to

DOI: 10.21552/edpl/2017/3/15

* Teresa Quintel is a FNR-funded PhD Candidate at the University of Luxembourg and Uppsala University under the supervision of Prof Mark D Cole and Assistant Prof Maria Bergström. For correspondence: <teresa.quintel@uni.lu>.

1 Dennis Broeders et al, 'Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data' (June 2017) 33(3) Computer Law & Security Review 309–23, doi:10.1016/j.clsr.2017.03.002.

2 Ian Loader and Neil Walker, 'Necessary Virtues: The Legitimate Place of the State in the Production of Security' in Benoit Dupont and Jennifer Wood (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press 2005) 165–95; Lucia Zedner, 'Policing Before and After the Police: The Historical Antecedents of Contemporary Crime Control' (2006) 46(1) British Journal of Criminology 78-96.

3 Cases concerned with data retention and mass surveillance, see Case C-301/06 *Ireland v European Parliament and Council* [2009] ECLI:EU:C:2009:68; Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* (C-293/12) and *Seitlinger* (C-594/12) [2014] ECLI:EU:C:2014:238; Case C-362/14 *Schrems* [2015] ECLI:EU:C:2015:650; Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB* (C-203/15) and *Watson* (C-698/15) [2016] ECLI:EU:C:2016:970.

4 *Tele2 Sverige AB and Watson* (ibid).

5 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201/37, as amended by Directive 2009/136, OJ L 337/11.

6 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58, OJ L 105/54.

7 For an in-depth analysis, see Mark D Cole and Franziska Boehm, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014) <https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf> accessed 9 October 2017.