Chapter 2.6
Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy

Anna Tsiftsoglou[1]
University of Athens, Greece

ABSTRACT

The Greek Data Protection Authority (DPA) was asked in July 2009 to review a proposed legislation that was exempting personal data processing via camera installations in public spaces from the scope of the Greek Data Protection Law 2472/1997. Such an exemption was justified, among other reasons, for the protection of public safety and crime prevention. This paper examines the legitimacy of this security measure from two angles: European and Greek Law. Furthermore, our analysis focuses on questions of privacy, the concept of public safety and its application, as well as the DPA's role in safeguarding citizens' privacy even in city streets.

INTRODUCTION: QUESTIONS OF LEGITIMACY AND POLICY

In July 2009, the Greek Data Protection Authority ('DPA') was asked to draft an opinion regarding a proposed legislation concerning the electronic surveillance of public spaces. According to the proposed legislative provision (art.12(1) of Law 3783/2009), all competent public authorities processing personal data via a closed-circuit television ('CCTV') system installed in public spaces in Greece for the purposes of state security, defense and public safety were exempted from the scope of the national Data Protection Law 2472/1997, thus also from DPA supervision. To examine the legitimacy of this new security policy, the DPA pursued a three-level analysis: Greek national law (constitutional and legislative), European

DOI: 10.4018/978-1-61350-323-2.ch2.6

law (European Convention on Human Rights, EU Charter of Fundamental Rights, Convention 108 of the Council of Europe and Directive 95/46/EC) and comparative law (France, Germany and Austria). In the present study, we will focus on the European and Greek national law analysis of the proposed legislative provision.

SURVEILLANCE IN PUBLIC SPACES AND THE EUROPEAN PUBLIC ORDER

The Scope and Exemptions of Directive 95/46/EC

Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing and free movement of personal data ('the Directive') explicitly exempts (Art. 3(2)) from its scope all activities falling outside the range of EU Law. Such activities were traditionally classified under the former 2nd and 3rd EU Pillars (Craig & De Burca, 2003, pp. 44-52). At any case, they included data processing for the purposes of public order, defense, state security and criminal action. After Lisbon Treaty entering into force in Dec. 2009, such actions are still left virtually to their entirety to State regulation (Van Raepenbusch, 2008, pp. 461-463).

In the cases C-317/04 & C-318/04 ('the PNR cases'), the European Court of Justice ('ECJ') ruled that the transfer of airline Passenger Name Records (PNRs) by airline carriers to the US Customs and Borders Control for the purposes of state security and crime prevention cannot be considered as an internal-market affair (thus not classified under the former First Pillar) but may fall under the exemption of Art. 3(2) of the Directive (pp. 54-59). The PNR cases encompass a strong political flair (De Leon, 2006, pp. 327-328) due to the important role assigned to the European Parliament in the decision-making yet provocatively set aside, in the end. The exemption of PNR data transfer from the level of data protection provided by the Directive creates precedent in favor of protecting state security (Sotiropoulos, 2006, p. 949).

Thus, member-states retain the power to regulate if and how the level of data protection provided by the Directive will be enforced in these sensitive areas of state action. Such discretion is in accordance with the notion and the economically-oriented purposes of the European legislator. Nevertheless, it leaves space for possible arbitrariness by the national legislator as well as it leads to the creation of heterogeneous data protection levels in the European area of security (Sicilianos, 2001, pp. 123-141). This may be pointed as one of the Directive's main weaknesses (Robinson et al., 2009, pp. 36-38) since it leaves the member-states the freedom to regulate this field *ad hoc* boundlessly, while it extends its protective shield exclusively to internal market affairs. Greece did not adopt the above solution, but rather subjected the complete spectrum of personal data processing to the protective level provided by the Directive (Alivizatos, 2007), even in areas not originally covered by it.

The Right to Data Protection within the EU Public Order

On a European public order level, the right to data protection is *autonomously* established also in other legally binding statutes (Sicilianos, 2001, pp. 123-141; Papadimitriou, 2007). Firstly, it is established in the Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') (Art. 1). Convention 108, applicable also to the public sector thus to police activity too (Art. 3(1)) offers the member-states the discretion to derogate from the principles of legitimate data processing provided by the Convention, if a state measure is considered to be 'necessary in a democratic society' for the purposes of state security and the regulation of criminal law