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

Anna Tsiftsglou

Available at: https://works.bepress.com/anna_tsiftsoglou/
Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices

Christina Akrivopoulou
*Democritus University of Thrace, Greece*

Athanasios-Efstratios Psykgas
*Yale Law School, USA*
Chapter 6

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

Anna Tsiftsoglou
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.

I. 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 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.
II. SURVEILLANCE IN PUBLIC SPACES AND THE EUROPEAN PUBLIC ORDER

a. The Scope & 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.

b. 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 issues (Art. 9(2)). Regarding Convention 108 we should note that:

a) The term ‘necessary measure in a democratic society’ refers in its wording to the European Convention on Human Rights (‘ECHR’). In the ECHR jurisprudence the
term ‘necessary measure’ is a relative concept, and should be judged in concreto for each country and within a specific political context (Explanatory Memorandum, section 56).

b) The Council of Europe adopts a ‘traditional’ definition of state security as ‘protection of national sovereignty against internal or external threats’ (Explanatory Memorandum, section 56).

c) The ‘major interests of the State’ justifying exemptions from the protective level of the Convention are listed exhaustively and do not allow the states to regulate differently.

Additionally, Recommendation R (87)15 of the Committee of Ministers of the Council of Europe, an important soft law legal resource, also provides principles regarding data processing, applicable in the public sector.

Finally, the right to data protection is independently established in the legally binding EU Charter of Fundamental Rights (‘The Charter’), in Art. 8, which provides personal data processing principles (Art. 8(2)) as well as the subjection of data processing to the supervision of an independent authority (Art.8(3)). The incorporation of this right within the Charter, an ‘international legal text that has received the most diverse influences and has received inspiration from a wide number of sources more than any other legal document’ (Gerapetritis, 2002, p. 920), which also ‘signifies a clear turning point of the EU by placing the individual’, instead of policies, ‘at the heart of the European evolution’ (Gerapetritis, 2002, p. 912), is of particular importance. It signifies that the right to data protection, along with the rest of the rights incorporated in the Charter, provides a privacy rights-based constraint on the exercise of the EU power – ‘a matter of principle, for a political entity with the power of the EU’ (Craig, 2002, p. 217).

c. Data Protection as an Aspect of Privacy within the ECHR

The right to data protection is protected also under Art. 8(1) ECHR, as an aspect of the right to privacy. Regarding public spaces in particular, the European Court of Human Rights (‘ECtHR’) recognizes a right to privacy. In Peck v. the United Kingdom (28.01.2003), ECtHR ruled that the mere monitoring of people in public spaces via CCTV, without any further processing of data, does not constitute breach of privacy (p.60). However, any further processing of this material, such as storing or unauthorized dissemination, may raise such issues (Alivizatos, 2005, pp. 15 and 22).

Art. 8(2) ECHR has as follows:

‘There shall be no interference by a public authority with the exercise of this right, except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights & freedoms of others’.

The above provision, as interpreted recently by the ECtHR places conditions for the legitimacy of the interference to the exercise of the right to privacy by a public authority:

a) be in accordance with the law, meaning:
1. to have a legal foundation in the national law of the member-state
2. the legal provision should have specific quality elements: accessibility (Khan v. the United Kingdom, 12.05.2000, pp. 26-28; P.G. & J.H. v. the United Kingdom, pp. 37-38), foreseeability (Amann v. Switzerland, 16.02.2000, pp. 55-62; Peck v. the United Kingdom, p. 66; S & Marper v. the United Kingdom, 04.12.2008, pp. 95-99) and provide safeguards against arbitrariness (P.G. &
Surveillance in Public Spaces as a Means of Protecting Security


b) be necessary in a democratic society, meaning:
1. there is a pressing social need for the establishment of a restriction, and the measure is considered to be sufficient and relevant.
2. it complies with the principle of proportionality stricto sensu, meaning the measure should be proportional to the achievable aim (Peck v. the United Kingdom, pp. 79-85; Weber & Saravia v. Germany, decision on the admissibility, 29.06.2006, pp. 107-118).

c) be justified by one or more of the following legitimate aims: national security, public safety, the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or the protection of the rights and freedoms of others.

III. SURVEILLANCE IN PUBLIC SPACES AND THE GREEK PUBLIC ORDER

a. The Concept of Public Safety:
Legitimate Aim and Legislative Tool

The concept of ‘public safety’ is crucial for specifying the aim of the relevant legal provision [Art.12(1) of Law 3783/2009]. Its clarification is also important, since it is perceived differently by people especially in the context of the city environment. Ball (2002), for example, when discussing about the use of CCTV systems in public spaces, comments on the differing public attitudes towards the concept of safety in the city: ‘Cities, by their nature, are uncertain places [...] People want the city itself to be safe, and any attempt to manage and homogenize the space detracts from its social richness’ (Ball, 2002, pp. 575-578).

The DPA gives the following definition of public safety: ‘the obligation of the State to take the appropriate measures for the protection and the efficient exercise of civil rights’. The concept of public safety as an obligation to protect rights is founded, according to the Authority, on the generic clause of Art. 25 (1), Sec. 1 of the Greek Constitution (‘The rights of man as an individual and as a member of the society as well as the principle of the social state are guaranteed by the State. All agents of the State shall be obliged to ensure the unhindered and efficient exercise thereof’) (Papaioannou, 2007, p. 729; Anthopoulos, 2005, pp. 113-114). DPA thus comprehends public safety not as a self-existent good, but rather as the ‘concentration of fundamental legitimate goods individually protected within their own constitutional limits’. It rejects, thus, two contradictory theoretical but also practical schemes, security viewed either as an individual good (Hrysogonos, 2006; Kamtsidou, 2006; Anthopoulos, 2005, pp. 113-126; Katrougalos, 2006) or as a public good (Mantzoufas, 2006; Kourakis, 2006). It further confuses human security with the security of the state. We could argue that security hereby used as a restriction to the exercise of the fundamental right to privacy, is more closely related to the second concept.

Public safety constitutes an indispensable aspect of security of the state. If we followed a traditional definition (Manesis, 1980, p. 390) state security consists of maintaining order within the state (internal security or public safety) and protecting the independence and sovereignty of the state among other states (external or national security). Moreover, the security of the state viewed as the protection from internal or external threats sustains the very core of the State’s existence (Manesis, 1980, p.391). Furthermore, the relationship of security and freedom – in our case, privacy – resembles an issue of ‘drawing limits’
Surveillance in Public Spaces as a Means of Protecting Security
(Manesis, 1980, pp. 392 and 417) while achieving the balance in this relationship constitutes ‘one of the major issues of our era’.

The contemporary version of security also contains the element of ‘risk’. In the post-modern times, state security has been promoted to the protection of the state from ‘whichever source the threat may originate’ (Papaioannou, 2007, p. 731). The priority in the modern ‘state of prevention’ (Anthopoulos, 2005, pp.109-113) is now given to the protection of goods from possible risks threatening them (Mantzoufas, 2004). In the risk society, risk -objectively observable though not easily predictable- helps us grasp the magnitude of state security. The size of security, a function of risk, is constantly being edified and transformed within specific socio-political factors (Manoledakis, 2004, p. 26) and hazard conditions. As a consequence, the continuous transformation of the concept of state security may lead legislators to constant transformations of legitimate aims. Thus, extensive data processing today may be justified for the purposes of state security but may become outdated once risk will not be evidently present to manage.

b. The Right to Data Protection [Art. 9A Con.]

The right to data protection is established in the Greek Constitution, after the Constitutional Revision of 2001, under the new Art. 9A, which provides the following: ‘All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law’. The right to data protection is not a novel right, however (Venizelos, 2002; pp. 148-150, Mitrou, 2001). On the contrary, it standardizes values already developed by the jurisprudence or pre-existing within the Greek or the European public order. Firstly, it encompasses the jurisprudence of the German Federal Constitutional Court (Pararas, 2001, pp. 64-65; Vlahopoulos, 2007, pp. 60-61), specifically the judgment in its notable decision on the Census case (BVerfGe, 65, 1983). There, the Court introduced the concept of ‘informational self-determination’, the essence of which rests in the ability of the person to determine him/herself if, when and under what circumstances his or her personal data shall be made public. This concept could be applied in various contexts, even in the case of electronic surveillance of public assemblies (Anthopoulos, 2007, pp. 721-723).

In addition, Art. 9A of the Greek Constitution incorporates certain values already established under the Greek Constitution of 1975, like the value of human dignity, [Art. 2(1)], free development of personality [Art. 5(1)] and privacy [Art. 9] with which it is closely related in its concept and application (Akrivopoulou, 2009, pp. 430-439). Additionally, Art. 9A formalizes principles found in legally binding international texts (Sotiropoulos, 2006, pp. 109-118; Mitrou, 2001, pp. 92-94; Venizelos, 2002, pp. 148-150) like those provided by Directive 95/46/EC for data protection and Convention 108 (1981) of the Council of Europe. Such principles governing the processing of personal data are also included in Law 2472/1997, the most notable of which being the principles of fair and lawful processing, proportionality, purpose specification (Art. 4) and the supervision of personal data processing by an independent authority (Art 15). Finally, similar principles can be found in the now legally binding Charter (Papadimitriou, 2007, pp. 218-219) in Arts. 7 (right to privacy and family life) and especially 8 (right to data protection). The latter establishes, among others, the principle of fair and lawful processing (Sect. 2) and assigns the supervision of data protection rules appliance to an independent authority (Sect 3).

At any case, every restriction of a fundamental right must respect the general conditions set by Art 25(1) of the Greek Constitution and the
related jurisprudence of the Hellenic Council of State regarding permissibility of restrictions, and particularly:

a) to be founded in law; the term ‘law’ may refer either to the procedures of the parliament (Vegleris, 1982, pp. 22-25; Manitakis, 1994, pp. 348-357) or to the procedures of the executive body exercising its regulatory authority (Manitakis, 1994, pp. 348-357; Hrysogonos, 2003, pp. 74 - 82).
b) to be justified by compelling public interest aims.
c) to be linked with the proposed legitimate aim and to be sufficient and relevant with the aim.
d) to not affect the very core (essence) of the right

c. The Role of the DPA within the Modern Greek Democracy

The allocation of powers to an independent administrative authority like the DPA is a relatively novel issue in the Greek public order. Such practice is closely related to the broader role of independent authorities in our modern democracy and to the concept of agencification as a means of new public management (Flogaitis, 2006, p. 112). The establishment of independent administrative authorities received wide applause as an important step in the modernization of the Greek Public Administration by instituting decentralized bodies with extensive powers and appointing experts with personal and functional independence to handle cases of their expertise (Art. 101A(1) of the Greek Constitution). Such modernization was initiated, firstly in the common legislation (the Greek Competition Authority being the first Greek Independent Public Authority established by Law 702/1977), and then Constitutionally for an exclusive group of five Independent Agencies (including the Data Protection Authority [Art. 9A of the Greek Const.] and the Authority for Communication Security and Privacy [art.19(2)]). It is worth noting here, on a comparative note, that in the US, which is the origin of this administrative model, independent regulatory authorities are created by the Congress, thus by the common legislator, and are not established by the US Constitution (Strauss, 2003, pp.159-160). Strauss (2003) furthermore claims that ‘the American Constitution and the general national statutes concerning the responsibilities given to governmental agencies or the procedures required of them neither define nor distinguish among the various forms the Congress creates’ (p. 160). The ‘innovation’ of the Greek legislator to include independent authorities within the constitutional text, makes it harder to control their influence or to even abolish them. Certainly not a solution followed by the American legislator.

Venizelos, the parliamentary majority rapporteur during the 2001 Constitutional Revision, claims that the Parliament was led to vote for the constitutional establishment of Anglo-Saxon-type independent authorities in Greece for various reasons. The most important was to shield some fundamental rights with additional guarantees but also to transfer several political responsibilities to ‘neutral/apolitical’ bodies so as to lift the heightened political burdens on sensitive issues from the Government (Venizelos, 2008). Alivizatos insists that both the sensitive nature and the rapidly shifting parameters of certain issues called for technocratic management and could not be left over to political manipulation (Alivizatos, 2001, p. 121). However, the wide institutionalization of independent authorities in Greece received skeptical reviews, mostly due to the democratic deficit characterizing such bodies (Venizelos, 2001, pp. 479-480; Kozyris, 2003, pp. 39-40).

The DPA has a prominent supervisory role in Greece. Particularly, its mission as an independent supervisory body / watchdog but also as an ‘institutional guarantee’ (Manesis, 1961, pp.15-17; Venizelos, 2008) of the right to data protection is established under Art. 9A Sect. b’ of the Greek Constitution (‘The protection of personal data is...’).
Surveillance in Public Spaces as a Means of Protecting Security

ensured by an independent authority’). On the other hand, its competence is strictly defined by Law (‘…which is constituted and operates as specified by law’), hereby meaning Law 2472/1997. The proper specification of DPA’s mission is especially important for future judicial decisions, since erroneous constitutional interpretations of the DPA’s mission may lead to perilous expansion of its allocated powers (Stratilatis, 2004, pp. 558-559). It lays in the discretion of the common legislator to regulate (Art. 15-22) everything concerning the formation, operation and allocation of powers to the DPA. The competence of an administrative body, such as the DPA, involves powers towards specified aims, which the DPA has the right and the obligation to exercise only according to law. The DPA’s powers are confined by law, according to the principle of legality (Spiliotopoulos, 2007, pp. 151-152; Dagtoglou, 2004, pp. 529-531). Consequently, the Greek Constitution establishes the mission, though not the action framework of the DPA.

The DPA’s supervisory role could be lawfully limited, though strictly within the boundaries prescribed by the Constitution (Mitrou, 2008, pp. 123-124). Since the DPA is considered an institutional guarantee of the right to data protection, the common legislator could not limit the DPA’s powers to the point that it practically extinguishes it. The amended provision of article 3(2) of the section c’ of the Law 2472/1997, which removes from the supervision of the DPA all the personal data processing by the competent public authorities (Taylor, 2003, p.86) via CCTV for the purposes of state security, defense and public safety, may raise serious issues of unconstitutionality. Those issues are relative to the amount of public authorities competent to process personal data, the range of data processing for the specific legislative aims and the scope of such an exemption from the supervision of the DPA. At any case, the existence of a fully independent supervisory body like the DPA is provided as a guarantee both by the Greek Constitution and by international legislation against state arbitrariness. As such, the limitation of DPA’s allocated powers must take place with additional legislative caution.

D. CONCLUSION

Surveillance in public spaces as a security measure must observe all relative national and European legislative principles. Furthermore, it must respect the constitutional role of the DPA as a guarantor of the right to data protection. In this sense, the proposed legislative provision has three central issues, according to the DPA’s Opinion. Firstly, it does not cite a specific legitimate aim. According to the DPA the vague referral to the aim of ‘public safety’ and ‘especially the protection of people or goods’ is very generic and leaves space for multiple interpretations. Particularly, the absence of a specified aim renders the application of proportionality test more difficult for the courts. However, the DPA wrongfully concludes that the provision should have included risk criteria for the specification of time and space to install and operate CCTV systems, since their enactment rests on the discretion of the competent authorities. The legislator should enrich the provision with safeguards against arbitrariness, as ordained by the ECtHR. Secondly, the provision does not comply with the quality standards of law shaped by the ECtHR jurisprudence regarding the restrictions of the Art 8(2) ECHR. The proposed provision is not foreseeable; it is not precise on the terms and conditions of processing personal data, with the exception of collected data and their destruction procedure, or on security measures of processed data. The data processor is also not specified. Lastly, the provision does not cite sufficient safeguards against arbitrariness. The DPA suggests that the proposed legislation does not provide sufficient safeguards, but instead removes the existing ones, by exempting a specific field of state action from the supervision of the DPA. However, in this point rests the only counter-argument against the
evaluation of the provision as fully inadequate: it offers some safeguards. Specifically, it assigns the supervision to a body with functional independence, the District Attorney, and further provides criminal sanctions in case that this regulation is breached. And this is something that the DPA fails to underline.

E. REFERENCES


Surveillance in Public Spaces as a Means of Protecting Security


**ENDNOTE**

1 E-mail address: tsiftsoglou[at]gmail[dot]com.