Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe[1]

Anna Tsiftsoglou[2] & Spyridon Flogaitis[3]

Abstract

Directive 2006/24/EC ('the Data Retention Directive'), a product of political compromises following terrorist attacks in New York, Madrid and London, reflects growing trends of serious 'pro- security' limitations to privacy. In February 2011 the Greek Legislator finally transposed the controversial Directive. This transposition is influenced by a landmark decision of the German Federal Constitutional Court. On March 2010 the *Bundesverfassungsgericht* ruled against the constitutionality of several national provisions implementing the Data Retention Directive in Germany. This paper aims to address the crucial points of the BVerfG decision and make suggestions as to what the Greek legislator should learn from Karlsruhe.

I. Introduction

In the Academy-Award winning film *Das Leben der Anderen* (The Lives of Others), a 1984 East Berlin memoir, a Secret Police agent is assigned the task of listening to the private life of an artist couple. As his task requires, he drafts detailed reports of all their home conversations and actions, seeking evidence of suspicious behavior towards the existing Regime. Accustomed to conducting surveillance, the Stasi Agent gradually becomes absorbed by his subjects' intimate lives.

If art depicts reality or is, at least, inspired by reality, then films like the latter should trigger us to think – if such practices were conducted under oppressive regimes, could we legitimize them within a democratic state? And if so, under what circumstances?

---

[1] Paper first presented at the 4th International Conference of Information Law with the special theme "Values & Freedoms in Modern Information Law and Ethics", Thessaloniki, Greece, May 20-21st 2011

2 LL.M. (Berkeley), PhD Candidate, Public Law, University of Athens, Greece (tsiftsoglou@gmail.com)

3 Professor of Public Law, University of Athens, Greece; Director, European Public Law Organization

This research has been co-financed by the European Union (European Social Fund – ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: Heracleitus II. Investing in knowledge society through the European Social Fund.

The German Constitutional Court attempted to give answers to such hard questions. Applying strict scrutiny on a federal law implementing the contested Directive 2006/24/EC ('the Data Retention Directive'), it nullified it on proportionality grounds (Federal Constitutional Court of Germany, 2010). The case serves as an example to -among others- the Greek legislator, who only recently implemented the Data Retention Directive, as well as to the Greek courts, which may encounter possibly similar challenges. Moreover, there are lessons to be learned from the Karlsruhe Court, both from a constitutional law perspective and from its stance towards EU regulation & control of public safety measures. One thing is certain: *there are tough times ahead*.

II. Transposing the DRD: What Karlsruhe said

On March 2nd 2010, the *Bundesverfassungsgericht* (BVerfG) overturned a German federal law implementing the Data Retention Directive (BBC News, 2010; Privacy International, 2010). The 2008 federal law [*Gesetz zur Neuregelung der Telekommunikationsüberwachung*- GNTR] amended several provisions of the **German Criminal Procedure Code** [*Strafprozeßordnung*- StPO, art.100g par.1§1] and of the **German Telecommunications Act** [*Telekommunikationsgesetz*- TKG, art.113a, b].

The amended provisions called for a *6-month preventive retention of all traffic and location communications data* (not content), to be retained *mandatorily by communications service providers* [113a TKG] for the broadly defined purposes of *crime prosecution*, combating *serious threats to public safety* or performance of *intelligence tasks* [113b TKG]. Moreover, *access* to such data for crime prosecution purposes would be permitted under a vague provision covering retention of traffic data in general, thus also for commercial aims [100g (1) StPo], without further guarantees.

While the BVerfG did not question the constitutionality of the Directive *per se*, nor accepted the request for a preliminary ruling [267 TFEU] to the ECJ on this matter, it found data retention to be *permissible in principle* as a security measure. The BVerfG thereafter performed strict scrutiny on the national provisions implementing it.

IIa. Applying *the Privacy Test*

Since the above telecommunications surveillance measures constituted an interference to the confidentiality of communications, the BVerfG had to judge them under the light of **Article 10 of the German Constitution** (*Grundgesetz* –GG), protecting the 'Privacy of Correspondence, Posts and Telecommunications'. Article 10GG protects all kinds of communication, electronic or otherwise, and extends *both to the actual content and its circumstances*, thus *also to traffic and location data* [BVerfG, §§189-190]. In addition, the provisions would be judged under the light of the fundamental **right to informational self-determination** ('*informationelle selbstbestimmung*'), jurisprudentially created by the very same court in the notable 1983 'Census Case' (Skouris, 1984, pp.692-694; Goold, 2007, pp.65-67; De Simone, 2010, pp.292-295). The latter right is a 'precursor' to the newer 'right to data protection', protected under

the EU Charter of Fundamental Rights (art.8), as well as an aspect of *privacy* under the European Convention on Human Rights (art.8) (Simitis, 2010, p.1992-93, 1997-98).

To check the constitutionality of the amended national provisions, the Karlsruhe Court applied *a Privacy Test* similar to the one employed by the European Court of Human Rights ('the Strasbourg Court') (De Vries et al., 2011, pp.6-8). The Strasbourg Court has developed this test when performing checks on restrictions to privacy under article 8§2 ECHR (Tsiftsoglou, 2011, pp.95-96). The privacy test followed by the BVerfG follows the Strasbourg Court three-level formulation (Tzanou, 2011, pp.281-283), though placing more emphasis on the final level (proportionality check), as follows:

A. Legality check [quality of *the legal basis*]: the interference must be *founded* on a law that is *accessible* and *foreseeable*, a standard satisfied by the above provisions

B. Legitimacy check [legitimate *aim*]: the interference must be *justified* by a legitimate aim, here viewed as "effective criminal prosecution" and prevention of dangers"

C. Proportionality check: a broader check of the nature of the interference comprising of checks on: a. *data security standards*, b. *purpose limitation*, c. *transparency* and d. *legal protection* (judicial control)/ *sanctions*

The final (proportionality) check is thus the most crucial one for the Karlsruhe court. Whereas the former two levels (legality & legitimacy) could relatively easily be satisfied, the last level requires *additional guarantees* to counter-balance the *intensity* of the interference to the fundamental right to telecommunications privacy.

The **intensity** of the interference is boldly acknowledged by the BVerfG, which talks about the danger of a 'diffuse threat' of being under constant surveillance [§§241-242] that may ultimately have *a chilling effect* on the exercise of other rights, such as freedom of speech. Solove, an American privacy expert, stresses that *"Even surveillance of legal activities can inhibit people from engaging in them […]* ***Chilling effects*** *harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity"* (Solove, 2007, 765). This 'side' or ill effect of massive surveillance had been emphatically asserted by the BVerfG in the Census Case (DeSimone, 2010, pp.294-5):

"Whoever is unsure if their dissenting behavior may be recorded at any time and, as information, permanently saved, will try to avoid attracting attention through such behavior. This would impair not only the personal development chances of individuals, but also the public good, as self-determination is a prerequisite for a free democratic polity based on its citizens' capacities of civic action and collaboration".

Judges Schluckebier and Eichberger, in their dissent, expressed the view that retention of *traffic and location data* cannot be considered an 'intense' interference or at least comparable to other forms of surveillance. This, they argued, was due to the fact that retention does not extent to *content*, the fact that all retained data are dispersed within servers of private parties and the fact that a judicial order is required for access to data.

However, the majority of the BVerfG recognizes that this kind of massive surveillance without occasion constitutes 'an especially heavy rights burden…with a dispersion, as yet unseen in our legal system to date' [§§210-212]. Even if retention does not cover the actual *content* of communications, the retained data may be used to create 'meaningful *personality profiles* of virtually all citizens and track their movements'. Thus processing of such vast amounts of communications data may help **construct social profiles** for every possible user, a scenario that the Karlsruhe court finds truly *disturbing*.

Profiling techniques are becoming, though, an increasingly useful tool for law enforcement agencies within Europe. The police utilize them to target 'not just *criminal*, but also more generally *deviant* behavior' (Brown & Korff, 2009, 5, 9). The emphasis now shifts from defendants to *abstract suspects* (Paraskevopoulos, 2004, 50, 58).

Nevertheless, the BVerfG finds that, despite its intense character, data retention is not unconstitutional in principal, given its features [§§205]. The *disperse nature* of retention by private actors (not the State) as well as its *limited duration* (6 months – minimum set by the Directive-art.6) seem, in the Court's view, to ease the intensity of the encroachment to the right to communications privacy (10GG). Overall, the *exceptional* character of this precautionary measure to serve important public interests such as the combating of organized crime contributes to its judicial acceptance, provided that additional conditions, set by the Court, are fully satisfied.

To pass the proportionality check, specific *criteria* have to be met. These preset conditions (*purpose limitation, data security standards*, *transparency* and *effective legal protection*) relate principally to the *quality* of the law (Breyer, 2005, pp.366-373; Pinakidis, 2007, pp.422-426), which the Strasbourg Court places in the primary (legality) check (De Vries et al, 2011, p.6). The presence of **procedural safeguards** had been underlined immediately following the voting of the Data Retention Directive, in view of a uniform implementation of data protection standards throughout Europe (Article 29 Working Party, 2006). The *ratio* is that the national legislator should offer serious counter-balances for the intensity of this security measure.

C (i). Purpose Limitation

Given the nature of the intrusion, data retention may only be permitted for *limited purposes*. Thus, the common legislator ought to minimize the scope of communications data use by *enlisting specific data uses*. As such, the prescribed purposes of data retention, as listed under the provisions of **StPO &TKG**, must be substantively **limited**.

(1) **"Criminal Prosecution"** should be clarified by a list of serious crimes, possibly specified by type (i.e. felonies only) for which concrete suspicion & proof is necessary;

Article 100g (1) StPO, to which §113b TKG refers, does not satisfy these conditions. **Section 100g (1) (1) StPO** allows direct use of communications data if a person "has committed a criminal offence *of substantial significance*", a vague term left to multiple interpretations, instead of enlisting *a numerous clausus of serious crimes only* (§228). **Section 100g (1) (2) StPO** is drafted in an even more generic manner, as it allows for

direct use of communications data if a person "has committed a criminal offence *by means of telecommunications*". Given the central role of telecommunications nowadays, such a clause permits direct data use for *virtually any crime, regardless of its seriousness*. Thus the *scope* of data retention 'for criminal prosecution' is *magnified* to an extent possibly not envisioned by the drafters of the Data Retention Directive Whereas data retrieval is permitted only in limited cases and under a judicial order, the current provisions treat this measure as a norm (§278) even "*without* the knowledge of the person concerned", contrary to the general *duty of notification* (101(4) (6) StPO). Moreover, no judicial control is hereby provided in case of failure of notification (Antoniou, 2008, 25-28; Kaiafa-Gbanti, 2010, 43-45; Tzalavra, 2007, 566-567).

(2) **"Prevention of hazards to public safety"** must be limited to only serious threats to a person's high values or to the integrity of the State. The same applies to (3) **performance of intelligence tasks"** (§231-232). In addition, where certain confidentiality relationships (i.e. emergency phone calls seeking help) apply, data retention should be totally prohibited, given the nature of such communications.

Sections 113b (2) and (3) TKG are also drafted in an unacceptable generic manner and satisfy very broad objectives. TKG leaves great space to future legislative acts (on a Federal or especially State level) to specify this objective, thus opening ground for multiple and extensive uses of communications data, which is greatly disproportionate.

The above restrictions are less stringent regarding *indirect* use of communications data. That is, in cases where public authorities request only user identifying information- such as info resulting from collected IP addresses- from service providers. The Court does not take any position on whether IP addresses (static or dynamic) should be considered "personal data" (according to article 2 of Directive 95/46/EC) (Fragkouli, 2008, p.204). At any case, this ***right to information*** is viewed as a moderate interference to the right to communications privacy; however, it is also subject to conditions, given its impact on *the anonymity* of Internet communications. Anonymity on the Internet should only be lifted for *substantial and serious public interests*, which are precisely specified by law. As such, a blanket right to information for the general purpose of "criminal prosecution" (Section 113b TKG) and with no notification of the data subject attached is considered unconstitutional by the Court.

C (ii). Data Security Standards

A high degree of data security standards is required (§222). The legislator can assign an independent authority the task of drafting detailed and legally binding provisions to ensure the implementation of such standards in data processing. Moreover, additional measures should be taken to limit the service providers' discretion in applying data security standards and subject data processing to effective supervision.

The required high degree of data security standards is hereby *missing*. **Article 113a§10 TKG** is drafted in a *generic* manner that leaves discretion to the private parties (service providers) to define the appropriate standards themselves. However, such clauses do not

guarantee any quality standards neither can be enforceable, since no sanctions are provided to punish serious data security violations.

C (iii). Transparency of Processing

All data processing must be transparent. Exceptions should be allowed only in cases where the purpose of data retention would otherwise be frustrated, such as in certain criminal prosecution acts or while carrying out intelligence tasks. Even in those cases *judicial oversight* is required, as well as *a posteriori notification* of the subject (§243).

C (iv). Effective Legal Protection

Data subjects must be protected against the secrecy of data processing. Thus *judicial control* is mandatory, as a form of resistance, to prevent arbitrariness as well as to offer recourse to potential victims of unlawful processing (Paraskevopoulos, 2004, 53, 55). Additionally, *effective legal sanctions* against rights abuse and *liability* of service providers for damages caused should be essentially provided by the legislator (§252).

Overall, the **present structure** of the above provisions lacks the *mandatory standards* of purpose limitation, high data security and transparency guarantees as well effective judicial control and sanctions. As such, these clauses are considered disproportionate and, thus, unconstitutional contrary to 10GG. Therefore, the Court declares them void.

Interestingly, the contested provisions were deemed contrary only to the right to communications privacy (10GG) and not to the right to self-determination. The BVerfG however extended the protective shield of 10GG to traffic and location data (circumstances and not mere content of communication) and to any further data processing conducted following their retention and information gathering (§§ 188-190).

Judge Schluckebier, in his dissent (§§ 310-336), accused the Majority for *judicial activism* and of dictating the legislature *how to balance competing interests*. Given the *changing nature* of organized crime, the state must conform to the challenges posed by technology and develop measures such as data retention that effectively serve *the duty to protect its citizens*. By restricting access and use to retained data, the majority basically restricts the legislator's freedom and power to regulate and thus surpasses its duty of judicial self-restraint. Surprisingly, Judge Schluckebier noted that, while the Majority acknowledged the challenges posed by technology in order to assess the *intensity* of interference, it did not reach any similar conclusions regarding the State's positive obligation to protect citizens against modern risks (Brown & Korff, 2009, 9).

IIb. *The Role of Telecommunications Service Providers*

An interesting aspect of this case is the role assigned to telecommunications service providers. The BVerfG considers them as 'guarantors' of the retained data, to which state authorities have access, directly or indirectly, only in limited occasions (§214).

This approach, however, rests on a fallacy, since nowadays several private parties tend to be much more powerful and effective than the State. We actually experience a form of "distributed surveillance", an evolving public-private network where several private enterprises act as Government agents (Mitrou, 2010, 140-141). "The Government no longer sticks to the traditional direct collection of data. *It turns instead to private entities*. In doing so, the State not only acknowledges that the majority of data is stored in the private sector, but also establishes **a processing model** systematically combining information gathered in both public and private sectors" (Simitis, 2010, 2003). Indeed, prominent American web-services companies such as Google and Facebook control today vast amounts of personal data, while their relationship with the US Government may not be as transparent as it seems (De Vries et al, 2011, p.9; Info Wars, 2011).

The European legislator entrusts private parties with a duty of storage for security purposes, additional to storage for their obvious commercial purposes, which imposes **a considerable financial burden** on them. Nevertheless, it is uncertain who is paying this price. Service providers in Germany are obliged to bear this cost *on their own*. Such industry-wide costs ranged between €130 million in France in 2006 (Pateraki, 2011, 324) to €150 million in the UK alone in 2008 (DeSimone, 2010, 310). Even worse, the lack of harmonization in this respect has serious financial impacts on competition in the EU telecoms market (Igglezakis, 2009, 1285; Sotiropoulos & Talidou, 2006, 185).

Rejecting allegations about the unconstitutionality (12GG- occupational freedom together with 14GG- private property) of such a burden and demands for compensation, the BVerfG confirmed that the cost associated to the *duty of storage* (113a TKG) does not exceed the obligations of service providers, as long as it is proportional. *"Entrusting private entities with public duties is not, in itself, constitutionally problematic, nor does it require public reimbursement for private expenses"* (§301). The BVerfG does not seem to take into account protection of property under the First Protocol to the ECHR [article 1(2)] either. The latter would definitely call for adequate compensation for such state-imposed obligations to service providers (Breyer, 2005, 374-375).

In the Court's view, the burden of cost should be assumed by the market, and be shifted eventually *to consumers*. With this 'twisted' frame of logic the citizens will be obliged to *pay for their own surveillance*! (Kaiafa-Gbanti, 2010, p.43).

IIc. *Karlsruhe* v. *Luxembourg*: Tough Times Ahead!

Another interesting aspect of the case is how the Karlsruhe court tries to 'avoid dialogues' (Papadopoulou, 2009, 382-4) with the European Court of Justice (ECJ)

The core issue brought forward to Karlsruhe was *the constitutionality of the Directive itself*, rather than the various national laws implementing it. The German court however lacked jurisdiction to originally interpret EU law. Nevertheless, it declined to refer the matter to Luxembourg, by relying on a former ECJ decision to illustrate how core criminal affairs still rest on the imperium of national legislators and courts.

In February 2009, the Luxembourg Court, in C-301/06 (Ireland v. Parliament and Council) rejected Irish claims on the wrongful adoption of the Data Retention Directive. Instead, it confirmed that former article 95 EC (now 114 TFEU) constituted the *appropriate legal basis* for the Directive as a former First Pillar measure, since the Directive's prime objective was to harmonize internal affairs within the EU telecommunications market (Loideain, 2011, p.260; Igglezakis, 2009, 1281-1286). By rejecting Irish allegations about *ultra vires* adoption of the Directive, the Luxembourg Court erred in its reasoning to decline that the directive's objectives were properly classified under the former EU Third Pillar. Characteristic in this respect is article 9 of the Preamble to the Directive which states 'Because **retention of data** has proved to be such **a necessary and effective investigative tool for law enforcement** in several Member States, and in particular concerning serious matters such as organized crime and terrorism…'. Moreover, the Luxembourg Court avoided exercising scrutiny on *this Directive for compliance of to the ECHR standards* (Breyer, 2005, 366; Pinakidis, 2007, 422-437) as data retention was considered merely as a First Pillar measure.

The adoption of data retention as an 'internal market affairs' issue by co-decision of the EU Parliament and the Council was not random. A product of political compromises between central EU institutional actors (the Council, the Commission, the Parliament and data protection bodies) it strengthened the Parliament's powers on the matter, which would have been impossible if a different legislative instrument, such as a framework decision, was chosen (DeSimone, 2010, 301-303; Antoniou, 2008, 14-17; Sotiropoulos & Talidou, 2006, 185-193). Thus the debate over the legal basis of this measure 'was not about rights but about *the nature of EU democracy*' (Bignami, 2007, 244, 238-251).

While the European Union was primarily conceived as an *economic* union, the emphasis following terrorist attacks in New York, Madrid and London seems to have shifted towards the creation of a *political* union, through the promotion of enhanced law enforcement cooperation policies. As such, 'The European Union is proving to be the nation-state in reverse chronology. The functions that the nation-state developed first – *protection from physical violence* –the European Union is acquiring last. Those functions that the nation-state acquired last – *administrative regulation of complex markets* – the European Union took on first' (Bignami, 2007, 233, 253).

As confirmed by the ECJ and highlighted by the Karlsruhe court (§§80-83), **data retention and storage** by telecommunications service providers are regulated *by the Directive* (articles 1-3), while **access to and use** of the retained data are *left to Member State discretion* (articles 1, 4, 6, 12) (Gerontas, 2007, 49). The principle of Subsidiarity, a procedural rule managing shared competences (Rantos, 1995, 32, 34-6), is hereby applied flexibly: *data retention and storage* are regulated by **EU law** whereas the issues of *access to and use of data* are regulated by **national law**. This sharp distinction also corresponds to a set of different actors: access and use are treated as law enforcement policies and are thus decided by national police authorities, who act with a great margin of appreciation. The Karlsruhe court clearly uses this distinction to its own advantage: since the core issues of the constitutional complaints touch upon *access and use*, then referral to Luxembourg is deemed unnecessary (De Vries et al, 2011, 12-13).

The tension between the 'integration-oriented' approach of the Luxembourg Court and the 'protection of sovereignty' approach (Kokott, 2010, 100-101) is hereby evident. The Karlsruhe court, by avoiding dialogues with Luxembourg, is seeking to preserve its status as 'the ultimate interpreter of constitutional legitimacy' (Papadopoulou, 2009, 148-150). A statement is declaratory: "The fact that *the exercise of civil freedoms cannot be totally recorded* belongs to the German Constitutional identity, which Germany must seek to preserve in European and international contexts" (§218). The respect of the German constitutional identity is thus presented by the Karlsruhe Court as an *ultimate limit* to control human rights degradations imposed by the European legislator on security grounds (Tsatsos, 2005, 24; Papadopoulou, 2009, 380-381). In an age of rapidly evolving European integration, the BVerfG should serve as an example for other Constitutional Courts and restate its relationship with Luxembourg by regaining 'the lost balance'. As Advocate General Kokott suggests, 'The German Constitution has no monopoly on the ideal protection of democracy, the rule of law and fundamental rights. (…) The solution must lie in recalling the international and open spirit in which the Basic Law was drafted and adopted in 1949' (Kokott, 2010, 102).

III. Transposing the DRD in Greece: Law 3917/2011

The Greek legislator transposed the Data Retention Directive in February 2011 with Law 3917/2011 (Government Gazette No. 22A/ 21.02.2011). This transposition was completed with considerable delay followed by a bitter ECJ ruling imposing a fine for failure of timely transposition (C-211/09, Commission v. Greece).

Nevertheless, the Greek transposition should be judged overall positively. By treating traffic and location data as elements of intimate communication, the Greek legislator subjects them to the enhanced guarantees of Article 19 of the Greek Constitution (an analog to 10GG) that protects the privacy of communications. Thus, traffic and location data can be retained only for limited purposes, as stated under the provisions of Executive Law 2225/1994 governing the waiving of confidentiality. As such, data retention is allowed only for an exclusive list of crimes (article 1), while access to the retained data is permitted only to the competent authorities and according to the conditions and procedures described in the Executive Law (article 4).

Furthermore, the Greek legislator provides additional guarantees such as limited location (Greece) and duration (12 months) of retention, the automatic destruction of retained data by service providers upon the end of provided duration as well as various data security principles (articles 6, 7). The latter shall be specified by a complete data security plan drafted by service providers. Lastly, Law 3917/2011 provides strict criminal and administrative sanctions in case of data security breach (articles 11, 12) and civil liability for possible damages caused (article 13).

Despite the above full spectrum of *essential* procedural guarantees (Gerontas, 2007, 66-67; Antoniou, 2008, 31), the Greek legislator fails to provide the most crucial one:

effective control. By allocating shared competences (articles 7§2, 9 and 12§2) and overlapping responsibilities (articles 7§2 and 8§2, 9) to two independent administrative authorities (DPA – the Data Protection Authority- and ADAE –the Hellenic Authority for Communication Security and Privacy) the Greek legislator unsuccessfully attempts to balance competing elements: effectiveness of data protection control with 'institutional verbosity'.

It is thus puzzling why one of the two rapporteurs argued that a possible merger of the two authorities would constitute a threat to the right to data protection and the right to telecommunications privacy (Pavlopoulos, 2011, 131) Since the Greek Constitution (articles 9A and 19) does not seem to prohibit such a merger, and given the central role afforded to independent administrative authorities as 'counterbalances' within its system **(**Flogaitis, 2001), this might have been a good idea both logistics-wise and in terms of administrative effectiveness.

IV. Lessons from Karlsruhe: What Lies Ahead?

Overall, we are eager to see the evolution of the data retention matter on two levels. First, on a regulatory level. EU Home Affairs Commissioner Malmström has announced a possible amendment of the Data Retention Directive, following the publication of its long-awaited evaluation in 2011 (Hustinx, 2010, 5). Second, on a judicial level. Since 2008 several national supreme courts in at least six Member-States (Bulgaria, Romania, Germany, Ireland, Cyprus and, most recently, the Czech Republic) have declared national laws implementing the Data Retention Directive unconstitutional. Most importantly, the constitutionality of the Directive is currently pending before the ECJ, after a referral again thanks to Irish initiative (Loideain, 2011, p.266).

BVerfG President Papier called the data retention ruling as 'One of the most important" [and also the very last] of his tenure (DeSimone, 2010). Indeed, this German ruling will be a reference point to other courts and legislators around Europe in years to come.

If data collection is deemed essential for the State's very self- existence (Gerontas, 2007, 55-56) and even if it is promoted as a 'temporary measure' in the fight against terrorism (Weinreb, 2007, 483, 486) it must still be subject to **guarantees**. It should be allowed for very specific uses, to prescribed authorities, for limited times and under judicial control. A high level of data security must be ensured, and should not be left on the discretion of private parties. Effective sanctions should punish violators. Independent administrative authorities could play a crucial role in these practices, both by imposing regulatory standards and by intervening when needed as watch-dogs (Papakonstantinou, 2006, 446; Tsiliotis, 2006, 541-542; Tsiftsoglou, 2011, 98-99)

Moreover, the BVerfG highlighted the importance of proportionality as *a measure of justice*. Counter-terrorist measures have to be judged from different angles, and both good regulators and hard-working judges have to equally contribute in this respect.

Lastly, the biggest lesson from Karlsruhe should be that ***self-regulation does not suffice***. The legislator, European and national, should impose, as clearly pronounced by the German justices, mandatory privacy standards and rules to all private actors (Simitis, 2010, 2004). In the words of former BVerfG Vice-President Hassemer, '*The State is no longer the Leviathan* (…) Instead, the State has become, so to speak, *civilized*. Citizens no longer see the State as a cause of risks, but see risks as originating outside of the state, *from third parties*. And they see the state as a possible partner, a potential ally in overcoming these risks' (Hassemer, 2004, 605).

In an era of social networks and of 'diminishing privacy' the State must persistently prove to be the biggest alliance for all citizens.

References

Antoniou Th. (2008), Telecommunications Privacy on Trial: Directive 2006/24/EC under Transposition, *Applications of Public Law*, 1 [in Greek], 13-31

Article 29 Working Party (2006), [WP 119] Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending directive 2002/58/EC, online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_en.pdf - last accessed 15.03.2011

BBC News (2010, March 2), German Court Orders Stored Telecoms Data Deletion, online at http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/8545772.stm - accessed 3.3.2010

Bignami F. (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 8, 233-255

Breyer P. (2005), Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 11:3, 365-375

Brown I., and Korff D. (2009), Terrorism and the Proportionality of Internet Surveillance, *European Journal of Criminology*, 6:2, 119-134

DeSimone Ch. (2010), Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive, *German Law Journal*, 11:3, 291-317

DeVries K., Bellanova R., De Hert P. and Gutwirth S. (2011), The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't it?), in: Gutwirth S. et al (eds.), *Computers, Privacy and Data Protection: An Element of Choice*, Springer

Federal Constitutional Court of Germany (2010), Press Release No. 11/2010 concerning the Judgment of 2 March 2010 - 1 BvR 256/08, 1BvR 263/08, 1 BvR 586/08, online at http://www.bundesverfassungsgericht.de/en/press/bvg10-011en.html -accessed 3.3.2010

Flogaitis Sp. (2001), The Independent Administrative Authorities, *Ta Nea* [in Greek], January 23rd, 2001

Fragkouli Ath. (2008), Are IP Addresses Considered Personal Data and Under What Consequences?, *Mass Media & Communication Law Review*, 2 [in Greek], 198-204

Gerontas Ap. (2007), Personal Data Protection – Public Security or Protection of Basic Rights?, *Applications of Public Law*, Special 20th Anniversary Issue [in Greek], 31-68

Goold B. (2007), Privacy, Identity and Security in: Goold B. and Lazarus L. (eds.), *Security and Human Rights*, Hart Publishers

Hassemer W. (2004), "The State is No Longer the Leviathan", Interview of the German Federal Constitutional Court Vice-President, *German Law Journal*, 5:5, 603-607

Hustinx P. (2010), *The Moment of Truth for the Data Retention Directive*, Speech given at the Conference "Taking on the Data Retention Directive, Brussels, December 3rd 2010

InfoWars (2011, February 17), *Facebook and Google are CIA Fronts*, online at http://www.infowars.com/facebook-google-are-cia-fronts, last accessed 30.03.2011

Igglezakis I. (2009), The Electronic Communications Data Retention after ECJ Decision C-301/06 of 10.02.2009, *Armenopoulos*, 8 [in Greek], 1278-1286

Kaiafa-Gbanti M. (2010), *Surveillance Models in the Security State & Fair Criminal Trial* [in Greek], Nomiki Vivliothiki Publications

Kokott J. (2010), The Basic Law at 60: From 1949 to 2009: The Basic Law and Supranational Integration, *German Law Journal*, 11:1, 99-114

Loideain N. (2011), The EC Data Retention Directive: Legal Implications for Privacy and Data Protection in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Mitrou L. (2010), The Impact of Communications Data Retention on Fundamental Rights and Democracy – The Case of the EU Data Retention Directive in: Haggerty D. & Samatas M. (eds.), *Surveillance and Democracy*, Routledge

Papadopoulou L. (2009), *The National Constitution and EU Law: The Principle of 'Supremacy'* [in Greek], Ant.N.Sakkoulas Publishers

Papakonstantinou E. (2006), Comment on Law 3471/2006, *Administrative Law Review*, 4 [in Greek], 442-446

Paraskevopoulos N. (2004), Security of the State and Legal Insecurity in: Manitakis A. and Takis A. (eds.), *Terrorism and Human Rights* [in Greek], Savvalas Publishers

Pavlopoulos P. (2011), Speech during the Parliamentary Discussion of the Law Implementing the Data Retention Directive in Greece, Plenary Session Proceedings (10.02.2011) [in Greek] online at http://www.hellenicparliament.gr/ last accessed 21.02.2011

Pateraki A. (2011), The Implementation of the Data Retention Directive: A Comparative Analysis in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Pinakidis G.(2007), The Obligatory Telecommunications Data Retention According to Directive 2006/24/EC Facing the European Convention of Human Rights Guarantees, *Hellenic Review of European Law*, 2 [in Greek], 405-438

Privacy International (2010, March 9), German Federal Constitutional Court Overturns Law on Data Retention, online at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566038 – last accessed 23.12.2010

Rantos A. (1995), The Principle of Subsidiarity according to the Treaty on the EU, *Hellenic Review of European Law*, 1 [in Greek], 25-38

Skouris V. (1984), Civil Rights & the Census Case, *Armenopoulos*, 9 [in Greek], 689-694

Simitis Sp. (2010), Privacy –An Endless Debate?, *California Law Review*, 98, 1989-2005

Solove D. (2007), "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *San Diego Law Review*, 44, 745-772

Sotiropoulos V. & Talidou Z. (2006), The Preventive Retention of Telecommunications Data for Crime-Combating Purposes (Directive 2006/24/EC), *Mass Media & Communication Law Review*, 2 [in Greek], 181-195

Tsatsos D. (2005), Security vs Freedom: The European Dimension in: Anthopoulos H., Contiades X. and Papatheodorou Th. (eds.), *Security & Human Rights in the Age of Risk* [in Greek], Ant.N.Sakkoulas Publishers

Tsiliotis H. (2006), The Threat of Human Rights by Modern Risks Emerging from Private Sources and the State's Obligation to Protect Them Through the Independent Administrative Authorities, *Administrative Law Review*, 4 [in Greek], 539-542

Tsiftsoglou A. (2011), Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Tzanou M. (2011), Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Tzalavra V. (2007), Preventive Surveillance of Electronic Communications for Crime Combating Purposes [1 BvR 668/04], *Criminal Chronicles*, NZ [in Greek], 565-569

Weinreb L. (2007), Responding to Terrorism - Lecture Given at the University of Athens, Greece on May 8th 2006, *Criminal Chronicles*, NZ [Greek translation], 481-487