Focus

DESTRUCTING DEMOCRACY ON THE GROUND OF DEFENDING IT? THE DATA RETENTION DIRECTIVE, THE SURVEILLANCE STATE AND OUR CONSTITUTIONAL ECOSYSTEM

Theodore Konstantinides, University of Surrey

Abstract
Recent technological developments have brought into question the protection of personal data and individual privacy. This contribution focuses on the harmonisation of "data retention" rules in the European Union, in particular the controversy surrounding the adoption and implementation of the Data Retention Directive (2006/24). It first considers the initiation of secondary EU legislation on data retention and the human rights implications of the retention of "traffic data" for the purpose of law enforcement. It then discusses challenges against domestic implementation legislation that have been initiated by NGOs. The analysis leads to the conclusion that harmonisation of the length of time that telecom operators and internet providers must retain data, along with other measures regarding the prosecution of crimes, have not met with success. These measures have rather generated uncertainty as to the form that data retention should take vis-à-vis the permissible degree of centralisation of power to the European Union and the adoption of legislation that allows for abuses of retained data contrary to the rule of law and fundamental rights. With an ECJ preliminary ruling pending on the constitutionality of Directive 2006/24, this debate is all the more interesting.

Introduction
In less than five years, EU criminal law has become a sub-discipline of EU law and what one can comfortably describe as well-travelled ground. A central element of the development of EU criminal law comprises the increasing tendency to adopt EU mechanisms for the intensification of access to, collection and exchange of personal data. Data surveillance has indeed occupied a special place in the European Union’s response agenda for countering global security threats such as terrorism and organised crime. Co-operation between private and public actors has been crucial for the retention of data related to the use of electronic communications services for the purposes of combating crime—for instance, tracing the source of illegal content and identifying those involved in misusing the above-mentioned services. This contribution will deal with the adoption and implementation of Directive 2006/24 by Member States—the so-called Data Retention Directive—which has sought to harmonise the way in which private providers of

1 This article was first produced by Thomson Reuters (Professional) Limited in European Law Review, (2011) 30 E.L. Rev. 722 and is reproduced by arrangement.
2 The title is inspired by Klaus v Federal Republic of Germany (1979-80) 2 E.H.R.R. 214 ECHR. Thanks go to Leslie Blake and to Filibert Nic Schrijner for their constructive comments and to Natalie Gousoul for her support. The usual disclaimer applies.
4 See Mitikgas, EU Criminal Law, 2009, Ch.6.
FOCUS

electronic communications services, or public communications networks, are obliged to retain data (telephone calls and internet access) under art.16 of the Directive 2002/58 on privacy (which states that Member States may adopt measures to restrict the scope of the rights that it introduces) [2002] OJ L201/37.

Although the Data Retention Directive has only been in force since 2007, it has generated considerable controversy among national authorities, which have been called upon to implement it. In a recent speech, Cecilia Malmström, the Commissioner responsible for Home Affairs, stated that most Member States have implemented the Directive, but differences are still noticeable on “several important points”, namely the duration and purpose of data retention; the procedures regulating access to personal data; and the cost of data retention for economic operators, to list but a few. This forms only one aspect of the thorny implementation of the Directive. Retaining communication and location data of all citizens in the European Union has raised sensitive issues related to the far-reaching impact of EU harmonisation legislation on privacy and the protection of personal data. Hence the argument is that the regime of the Data Retention Directive needs to be complemented by adequate legal safeguards in order to limit the risk of abuses or any undermining of the rights guaranteed by art.16 TFEU, the European Convention on Human Rights (ECHR), several EU regulatory initiatives such as Directives 95/46 and 2002/58, Regulation 45/2001 and the EU Charter of Fundamental Rights (discussed further below). The Charter is now in force and can be invoked as a guarantee of justice and constitutional recognition of the right to data protection (art.7).

Although the discussion hereafter is focused on the Data Retention Directive, this article aims to reflect upon the broader tension between the efficiency of implementation of the Member States’ obligations within the European Union and effective compliance of secondary EU legislation with constitutionally focused standards, such as the protection of fundamental rights. It is submitted that a balance must be achieved between the two. This is true not only in the context of the Data Retention Directive but also when it comes to many other EU legislative instruments of general or targeted application that Member States are called upon to transpose into national legislation. Despite the fact that the balance between implementation efficiency and preservation of constitutional standards is essential to this contribution, the ambition is to go beyond the procedural aspects of data retention. In other words, this article invites the reader to consider two constitutional dangers impending the European polity. First, even prior to Lisbon’s “Communisation” of the former Third EU Pillar, one can notice a shift in EU criminal law from mutual recognition to harmonisation. After all, the Data Retention Directive was adopted as an internal market measure. Secondly, one may also notice a shift from a co-operative model towards a coercive one. This model is based on rapid and intrusive action against potential serious security threats. More suspicion suffices to resort to actions, such as intrusive and all-encompassing telecommunications surveillance, bringing Member States close to the pervasive Orwellian “surveillance state” model.

Inception and adoption of the Directive

In the aftermath of the London terrorist attacks (2005) and Madrid bombings (2004), where—according to the Commission—telephone data up to six months old was investigated, it became apparent that control over telecommunications (especially the use of mobile telephony and the electronic communications systems) played a significant role in the prevention, investigation, detection and prosecution of terrorism and organised crime. Yet there was a gap in national and EU legislation. Traffic data was not always stored by operators in the Member States (e.g. not even for billing or settling customer disputes).

---

8 The specified classes of data that can be retained are listed in art.5 of the Data Retention Directive (2006) OJ L305/54). Article 6 of the Directive sets the limits of the period of retention, which may be between six months and two years from the date of the communication.


10 For measures of general application, see the Council Framework Decision on the European Arrest Warrant and the Surrender Procedures between Member States [2002] OJ L190/1 and for measures of targeted applications, see Regulation 881/2002 (2002) OJ L158/1 on the imposition of specific restrictive measures (i.e. freezing of funds and economic resources) against persons and entities associated with Osama bin Laden, Al Qaeda and the Taliban.


---

xii European Current Law Issue 1 2012
and was not, therefore, available for public authorities to use against criminals whenever there was a legitimate cause to do so. Hence, shortly after the Brussels EU Summit of March 25 and 26, 2004, which emphasised the necessity of rules guaranteeing the availability of traffic data for anti-terrorism purposes across the European Union, a number of Member States presented a Draft Framework Decision to be adopted under the Third Pillar (articles former Title VI TEU). The Draft concerned the a priori mandatory storage by a state and/or exchange between Member States of telecommunications traffic and location data (excluding content) of all users for law enforcement purposes for a period between 12 to 36 months (art.4), depending on the usefulness of the data in relation to countering crime and the cost of retention.

The Draft’s main point was the need to ensure the harmonisation of national procedures regarding the way in which individual data is processed and stored by providers of a publicly available electronic communications service (or network) for the purpose of detecting and prosecuting serious crime, including terrorism. This Draft noted that “many Member States have passed legislation concerning a priori retention of data” for those same purposes but “the content of this legislation varies considerably.” These differences, according to the Draft, were prejudicial to co-operation between Member States and, therefore, counter-productive to effective police and judicial co-operation in criminal matters in the European Union. The Draft also highlighted, on the one hand, the imperative for the maintenance of a balance between the protection of personal data and the necessity for law enforcement authorities to access such data (for criminal investigation purposes), on the other. To avoid being criticised for proposing the adoption of a measure encouraging excessive state intrusion into private life, the proposing Member States recalled both the ECHR and EU privacy legislation. These references served as thresholds calculating the appropriateness (and proportionality) of state interference vis-à-vis the risks at stake.

On November 9, 2004, the Article 29 Data Protection Working Party, an independent European advisory body on data protection set up under Directive 95/46, published its Opinion on the Draft Framework Decision’s compliance with human rights and data privacy laws. In particular, the Working Party assessed the conditions that legitimise state interference with the right to private life by looking at the broad criteria laid down in art.8(2) ECHR.

“...there shall be no interference by a public authority with the exercise of this right except such as is 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...

91 The proposal was presented by France, Ireland, Sweden and the United Kingdom.
of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.\(^{16}\)

The Working Party did not consider it "opportune" to scrutinise the Draft against all the contingencies set out in art 8(2) ECHR. It rather focused on the requirement of necessity of state interference "in a democratic society", citing the case law of the European Court of Human Rights (ECtHR). This provided that any "interference" must respond to a "pressing social need" and should only occur in "exceptional cases."\(^{17}\) The Working Party concluded that the Draft not only failed to satisfy the above criteria but even sought "to nullify them".\(^{16}\)

It thus concluded that:

"The mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft Framework Decision, is not acceptable within the legal framework set in Article 8."\(^{16}\)

Following a detailed consultation process with representatives drawn from law enforcement authorities, the electronic communications industry, and data protection experts, the Commission considered that aspects of the proposed Framework Decision should be adopted (under former art 47 TEU, now deleted)\(^{16}\) using First Pillar rather than Third Pillar instruments. These aspects consisted of the regulation of, first, the harmonisation of retention periods across the European Union (including the types of data to be retained) and, secondly, access to (and exchange of) such data by national law enforcement authorities. The Commission's proposal of September 21, 2005 stressed that a directive harmonising data retention obligations forms the most appropriate legislative instrument to regulate the obligation on providers of electronic communication services because it is less stringent compared with a regulation and it allows considerable room for implementation manoeuvre (e.g. leaving the choice to Member States to decide which authorities should have access to data retained and under which conditions).\(^{21}\) Moreover, it was proposed that the cross-availability of data would be ensured for the period of not less than six months and not more than two years from the date of the communication.

According to the Commission, differences in the national legal, regulatory, and technical provisions concerning the retention of "traffic data" presented obstacles to the internal market for electronic communications. This was due to the fact that service providers had to deal with different requirements regarding the types of data to be retained and the conditions for doing so. The Commission agreed, therefore, that these provisions needed to be subject to harmonisation under former art 14 EC (current art 26 TFEU) and proposed that the specific legal basis of former art 95 EC (current art 14 TFEU) was appropriate for the adoption of the Directive. The Commission concluded that the principles of subsidiarity and proportionality had been complied with: the former because organised crime and terrorism are often cross-border and the latter because the Directive only deals with the processing (and not the content) of traffic data by service providers. It was further noted that the matter was indeed one that came under Community competence, given that data retention had already constituted the subject-matter of

\(^{16}\) In a similar manner, art. 15(1) of Directive 2002/58 on privacy and electronic communications (2002) OJ L 201/37, which has harmonised personal data protection rules in relation to electronic communications services, provides that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and 4, and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period."

\(^{17}\) \textit{Alto v Germany} (1979-80) 2 EHR 214.


\(^{21}\) Former art 47 TEU regulated the relationship between the Treaty on European Union (TEU) and the EC Treaty stipulating that no legal instruments adopted under the TEU may affect the legislative framework adopted under the EC Treaty.

previous instruments based on First Pillar legal bases, such as Directives 2002/68 and 95/46.

When it came to the protection of fundamental rights, the Commission admitted that "it is clear that the proposed Directive will have an effect on the privacy right of citizens as guaranteed under Article 7... as well as... Article 8 of the [EU] Charter [of Fundamental Rights]...". It is worth repeating that, although the text of the Charter has not been incorporated in the Treaty of Lisbon, art.6(1) TEU confirms that it "shall have the same legal value as the Treaties". This includes and applies to Directive 95/46. The Charter reproduces art.8 ECHR (right to privacy), art.8 of the Charter concerns the protection of personal data. This is an independent fundamental right, which has no equivalent in the ECHR. The legally binding nature of the EU Charter of Fundamental Rights adds emphasis to the rights aspect of Directive 95/46. The right to protection of personal data has also been reproduced in art.16 TFEU, which provides for provisions having general application in areas such as judicial co-operation in criminal matters and data protection in areas such as the Common Foreign and Security Policy. Despite the protection offered by the Charter, the Commission recalled in its 2005 proposal for a data retention Directive that art.62 of the Charter provides justification for interference with the right to privacy and protection of personal data.

Since the Commission concluded that limitations to privacy and to the protection of personal data are both proportionate and necessary to meet the objectives of countering serious crime and terrorism, it abstained from proposing any general provisions to safeguard the retention of "traffic communications data" from potential abuses. To that end, it drew from the existing EU data protection provisions enshrined in Directives 95/46 and 2002/68. It concluded that "specific additional provisions on general data protection principles and data security are not necessary."22 In this fashion, the Commission appeared to have proposed a Directive which was in line with art.6(2) TEU, and thus in compliance with fundamental rights as guaranteed by the ECHR.

Yet, according to the European Data Protection Supervisor (EDPS), which is an independent supervisory body devoted to protecting personal data and privacy, such a level of protection of personal data was deemed to be neither necessary nor proportionate. The EDPS stressed that "a simple reference to the existing legal framework on data protection (in particular the Directives of 1995 and 2002/58) was not sufficient."23 What is more, the European Economic and Social Committee (EESC) shared that sentiment, expressing its surprise and concern over the submission of such a proposal for a Directive.24 The EESC predicted that the Directive, in its proposed form, was at risk of being declared unconstitutional by national constitutional courts because the "fundamental rights" test used by the Commission was both "flimsy" and "flawed". For instance, the EESC suggested that the Commission's proposal only mentioned arts 7 and 8 ECHR as safeguards, while it ignored arts 36 (access to services of general interest); 39 (consumer protection); 47 (the right to an effective remedy) and 48 (presumption of innocence). These criticisms were also echoed in the European Parliament Minority Opinion where it was stressed that the proposed retention period was "far too long".

The Commission's proposal for a Directive based on former art.95 EC (art.114 TFEU) was adopted by the EU legislature taking the form of Directive 2006/24, on March 15, 2006 and entered into force on May 4, 2006.26 Ireland and the Slovak Republic were the only Member States that voted against it in the Council. What is more, a number of Member States took up the option (available under art.15(3) of the Directive) to postpone the Directive's application to the retention of communications data relating to internet

---

access, internet telephony and email for a period between 18 and 36 months after the date of adoption of the Directive.

In a nutshell, the Directive established that individual data is to be made available for the purpose of the investigation, detection and prosecution of serious crime (as defined by each Member State in its national law) and, also, eliminated national regulatory differences deemed to impede the functioning of the internal market for electronic communications. Thus the Committee on the Internal Market and Consumer Protection was wise when it commented that the Directive represents "a paradigm shift in the way society looks at traffic data".37

Implementation problems and judicial challenges

The European Union’s pre-emptive response to cross-border crime has altered our ‘constitutional ecosystem’ by transferring competence to supranational institutions with limited accountability. With regard to the Data Retention Directive, it is argued that this has put national judges under enormous pressure to uphold constitutional values in light of the fact that the Directive allowed Member States to transpose it using divergent rules in terms of the retention and availability of data. This is clearly demonstrated in the various national challenges against the Data Retention Directive. This section considers the Irish, Romanian and German cases on data retention, which have gained considerable academic attention.38 These adverse judgments are used here as case studies to demonstrate the difficulties and inconsistencies in the implementation of the Directive. They are also indicative of the role of national courts as the last line of defence when it comes to the protection of national constitutional values.

Ireland

The first challenge to the Directive came before the ECJ on July 1, 2008. Ireland, which voted against the Directive in the Council, sought its annulment on the ground that it was not adopted on an appropriate legal basis.39 Ireland, supported by the Slovak Republic (also outvoted in the Council), argued that the Community was not competent to adopt such a measure, at least not on the legal basis that was chosen, because its centre of gravity was not the functioning of the internal market but public safety and crime prevention.40 Apart from the Slovak Republic’s human rights concerns (which were based on art.8 ECHR), the case revolved solely around the scope of the EU legislature’s power to adopt harmonising measures pursuant to former art.95 EC (art.114 TFEU).41 If nothing else, the judgment was academically stimulating. It shed some light on the ECJ’s threshold for connecting a particular measure with the internal market and the relationship between internal market competence and other legal bases stemming from the Treaties.

In addressing those issues, the ECJ compared the case at hand with the Passenger Name Records (PNR) case, where a Council Decision was annulled.42 That Decision had enabled the transfer of air passenger name records from the Community to the US Bureau of Customs and Border Protection.43 That annulment related, however, to the dividing line between the former First and Third Pillars. The ECJ concluded that the two cases shared no similarities. One the one hand, Council Decision 2004/498 was annulled because it concerned a transfer of personal data within a framework instituted by public authorities in order to ensure public security. On the other hand, Directive 2006/24 could be defended because it covered the activities of service providers in the

---

38 It should be noted that the decisions of the constitutional courts of the Czech Republic, Bulgaria and most recently Cyprus and Hungary are of equal importance but are not considered in this article. See for a summary: European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (Brussels, April 18, 2011) COM (2011) 236 final, pp.20-21.
40 Ireland’s argument was that the Directive should have been adopted under art.95 TEU, art.31(1)(a) TEU and art.34(2)(b) TEU.
41 Ireland v European Parliament (C-301/06) [2009] ECR I-693 at [57].
internal market. It did not, therefore, contain any rules governing the activities of public authorities for law enforcement purposes.\textsuperscript{34} Had the Directive contained a detailed system of data access and safeguards, it would have shared the same dismal fate of the PWF Decision. Ironically, the lack of safeguards in the Directive (and, by implication, in national implementing legislation) has proved to be its Achilles heel.

Much comment has been published on the merits of Ireland v Parliament and Council, and the manner in which the ECJ (using the "Community preference clause" of former art.47 TFEU) held in favour of former art.95 EC.\textsuperscript{35} Thus our analysis of the judgment will draw to a close. In any event, as Dougan notes, after the coming into force of the Treaty of Lisbon, the value of this aspect of the judgment has become marginal.\textsuperscript{36} This is true, given that, post-Lisbon, the EC-EU dichotomy is no more; art.47 TFEU has been deleted; and under current Title V of the TFEU, measures in the area of police and judicial co-operation in criminal matters will inevitably take the form of regulations and directives. Judicial co-operation in the fight against serious crime has become a fully fledged EU policy. The ordinary legislative procedure applies and the ECJ’s jurisdiction has been extended in former Third Pillar areas, albeit subject to certain limits defined in Protocol 36 annexed to the Treaty.

Almost at the same time that the Irish Government sought to annul the Data Retention Directive, a civil rights advocacy group, Digital Rights Ireland (DRI), brought a case against the Irish Government in the High Court of Ireland\textsuperscript{37} seeking, inter alia:

1. Declarations to the effect that s.63(1) of the Criminal Justice (Terrorist Offences) Act 2006 (C.I.TOA 2006) was (was) null and void for breach of domestic law (both statute\textsuperscript{38} and the Constitution\textsuperscript{39}) and EU data protection law; and the ECtHR.\textsuperscript{40}

2. An Order pursuant to art.267 TFEU addressing the validity of Directive 2006/24 netwistingandart.6(1) and (2) TEU; arts 3a and 21 TFEU; arts 7, 8, 11 and 41 of the EU Charter of Fundamental Rights; and art.5 TUE.

On May 5, 2010, the High Court, having considered the relevant case law on locus standi,\textsuperscript{41} agreed that a more flexible and liberal approach was necessary where questions of EU law are raised "so that a person’s rights are not unduly hampered or frustrated."\textsuperscript{42} Accordingly, the High Court judge was satisfied that the DRI had a bona fide concern and interest in the subject-matter of the provisions seeking to be impugned, and that the rights that it sought to protect were of general importance to society at large. He therefore granted standing to the plaintiffs to bring an actio populorum to question whether the contested provisions violate citizens’ rights to privacy and communications (but not with regard to family and marital privacy or travel).\textsuperscript{43} The judge further agreed with the DRI that a reference to the ECJ under art.267 TFEU was required since there was no effective remedy under national law and because, under Foto-Frost, a national judge has no discretion to declare an EU instrument invalid.\textsuperscript{44}

Compared with Ireland v Parliament and Council, this pending case tackles the problem at its root—i.e. the Directive’s interference with the right to privacy of all citizens.

\textsuperscript{34} Ireland v European Parliament (C-301/08) (2009) E.C.R. I-693 at [86]-[92].


\textsuperscript{39} Constitution arts 40.3.3, 40.3.2, 40.6.1 (the rights to privacy, travel and communication).

\textsuperscript{40} See Digital Rights Ireland May 6, 2010 High Court at [70]. Here the High Court referred to the much celebrated concern of the ECtHR in Klass v Germany (1979-80) 2 E.H.R.R. 214 at [49]: "Powers of secret surveillance of citizens, characteristic as they are of the police state, are tolerable under the Convention only so far as strictly necessary for safeguarding the democratic institutions... [T]he Court being aware of the danger such a [telecom interception] by police of underrating or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism adopt whatever measures they desire appropriate."

\textsuperscript{41} Especially Culhane v Sutton (1980) 1 LR 269 and The Irish Penal Reform Trust Ltd (2006) IHC 305 regarding the relaxation of standing rules in cases where a category of person may not be in a position to adequately assert their Constitutional rights.

\textsuperscript{42} Digital Rights Ireland May 6, 2010 High Court at [46].

\textsuperscript{43} Data Protection Ireland May 6, 2010 High Court at [116].

living in the European Union. Because Ireland maintained a longer (i.e. more invasive) retention period under s.63(1) of the CJ(TO)A 2005 (three years) than that proposed by art.6 of the Directive (six months and two years respectively), it is clear why the Irish Government did not challenge the measure on human rights grounds. The ECJ's Digital Rights Ireland judgment, expected in 2012, will be significant because the ECJ will be called upon to determine the material aspects of the Directive. These are far more important to the citizen than the procedural aspects of implementation efficiency, for they will determine the permissible degree of EU involvement in the Area of Freedom, Security and Justice through restrictive regulation to the right to privacy.

Romania

On October 8, 2009, the Constitutional Court of Romania ruled that Romania’s national implementation law (238/2008), which transposed Directive 2006/24 into domestic law, was unconstitutional. The case was initiated by a national human rights NGO, Comisia de Protecția Drepturilor Omului, which brought an action before the Tribunalul Bucuresti (Bucharest Tribunal) against a mobile operator (Orange Romania) for storing traffic data according to the new domestic legislation. Once a motion for the unconstitutionality of Law 238/2008 was raised, the Tribunal referred the case to the Constitutional Court on February 6, 2009. The latter declared the law on data retention unconstitutional in its entirety for affecting several rights entrenched in the Romanian Constitution. It stressed that the implementation law did not offer sufficient safeguards to compensate for the risks to the exercise of constitutional rights, such as the right to free movement, private life, secrecy and freedom of expression. The Constitutional Court further condemned the lack of precision in the law, mainly with regard to its broad notions of “related data” and “threats to national security”. It held that the former term was in breach of the requirements of accessibility and foreseeability, and that the latter term allowed too much discretion to public authorities to render all citizens potential suspects by requiring the retention of data on all communications (contrary to the presumption of innocence).

In harmony with the Irish High Court’s decision in Digital Rights Ireland, the Constitutional Court of Romania made reference to the judgment of the ECtHR in Klass. It is remarkable, according to some commentators, that despite the fact that the literal wording of the ECHR does not cover modern means of communication, the ECtHR has favoured both a dynamic and broad interpretation of the ECHR to bring those means within the scope of art.8 of the Convention. Equally, national courts appear keen on applying the ECtHR’s jurisprudence on adequate safeguards in order to balance interference by public authorities with individual freedoms. This similarity aside, two main features distinguish the position of the Romanian Constitutional Court from that of the Irish High Court. First, the former did not mention Directive 2006/24 in its judgment, although it was obvious that (since Law 238/2008 was the only national implementing measure for the Directive) any criticism aimed at it would actually constitute a criticism of the Directive itself. The Irish High Court, on the other hand, spent considerable time assessing the merits of the DRI claim against the Directive. Secondly, unlike the Irish High Court, the Romanian Constitutional Court did not demonstrate a willingness to make a preliminary reference to the ECJ regarding the validity of Directive 2006/24. Because the decisions of constitutional courts cannot be

45 Decision 1258 of October 8, 2009 on the objection of unconstitutionality of the provisions of Law 238/2008 on the retention of data generated or processed by the providers of publicly available electronic communications services or public communications networks, which also amends Law 506/2004 on the processing of personal data and privacy protection in the electronic communications sector, Official Gazette No.398 of November 3, 2009.
47 Klass v Germany (1979-80) 2 E.H.R.R. 214. The Court also mentioned Abery v Ireland (1979-80) 2 E.H.R.R. 305 ECHR; Papageorgiou v Romania (45234/89 and 71526/01) June 28, 2007 ECHR.
49 This is in tune with the Decision of the Supreme Administrative Court of Bulgaria, which held that art.16 of Bulgarian Regulation 40 regulating access to data without limitations was in violation of art.8 ECHR; Directive 2006/ 24; and arts 32 and 34 of the Bulgarian Constitution. It was, therefore, annulled. See Decision 10217 of November 12, 2008, Complaint in English, EUR, http://www.retd.org/engl-gen/number824/bulgarian-administrative-case-data-selection (Accessed September 1, 2011). This case will not be analysed here since, as of February 13, 2010, the Bulgarian Parliament approved the second reading of amendments to the Electronic Communications Act.
revoked by any state authority, the Directive’s implementation process was sent back to square one.

Although the attitude of the Romanian Constitutional Court challenged the ultimate authority of the ECJ for determining the correct interpretation of EU law, the Romanian Ministry of Information Society and Communication submitted, on June 23, 2011, new draft implementing legislation. The draft, which is almost identical to the “unconstitutional” Law 258/2008, makes it explicit that effective implementation of the Directive serves to avoid infringement proceedings taken by the Commission against Romania. 59 Proceeding these developments, the Romanian judgment reflects the general aversion of the Romanian Constitutional Court’s judges to excessive data retention legislation, which can potentially lead to the establishment of a police state, hostile to the rule of law, upon which the European Union is founded upon according to art.2 TEU. This may be correct, given that the Constitutional Court is renowned for the relatively low amount of challenges that it upholds as unconstitutional.60 Yet one cannot help but conclude that despite the Romanian plans for implementation of the Directive, the judgment struck a blow at the established dialogue between European and national courts and the latter’s acceptance of the principles of loyal co-operation (art.4(3) TEU) and primacy of EU law. Following this line of thinking, one can argue persuasively that any glimmer of co-operative federalism within the European Union have proved to be a false dawn.61 This is especially because the implementation of EU law seems, at least in this case, to have taken place out of fear that express refusal to fulfill an obligation imposed by EU law will lead to the imposition of enormous fines by the Commission following infringement proceedings under art.258 TFEU.

Germany

Soon after its Lisbon Urteil of June 30, 2009,62 the German Federal Constitutional Court (BVerfG) was required (on March 2, 2010) to make another constitutional value judgment. This time, a complaint was lodged by Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention), with the support of 35,000 citizens, against the Act for the Amendment of Telecommunications Surveillance of December 21, 2007.63 The Act, which transposed Directive 2006/24 into national law, entered into force on January 1, 2008. While avoiding a direct clash with the ECJ, the BVerfG focused on the protection of state prerogatives vis-à-vis the entrenched protection for the privacy of telecommunications under the Grundgesetz (the German Constitution—GG). It agreed that the contested national retention legislation infringed art.10(1) GG (Privacy of correspondence, posts and telecommunications) and had to be annulled. At this point, it needs to be highlighted that the BVerfG did not declare the domestic legislation in question to be unconstitutional but rather established that it encroached too severely on the protection of human rights enshrined in the Grundgesetz.64 The BVerfG did not comment on the Directive’s validity because it was the domestic law that went too far beyond the requirements established by that Directive. It therefore adopted a more rigorous “proportionality check” than that employed by the ECHR, concluding that secret processing and retention of data may only be permitted in particular cases and must always take place under judicial oversight and with effective judicial remedies available to the citizen.65 It also cited, albeit implicitly, the Lisbon Urteil with reference to the obligations of the state to its citizens. These obligations entail that the enjoyment of personal freedom may not be recorded or registered. This duty was described by the BVerfG as comprising part of Germany’s “constitutional identity”.

64 Decision of March 2, 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 568/08.
65 German Data Retention Judgment, June 30, 2009, art [212].
As such it was held to be imperative that it be preserved in both the European and international context. This notion adds to the constitutional safeguard of ultra vires review as established by the BVerfG in the Solange cases.

Contrary to the wishes of the plaintiffs, the BVerfG stressed that a referral to the ECJ was out of the question. It clarified the position by arguing that the issue in this case was neither one of the precedence of EU law over national fundamental rights, nor did it concern the validity of Directive 2006/24. This was especially so because the judgment did not declare the domestic law to be altogether void. The judgment simply related to the extent of state discretion implied in the implementation of the Directive. The decision of the BVerfG to bring the matter of the constitutionality of data retention legislation under its own jurisdiction can be characterised as reasonable, given that the Directive is limited to the duty of storage alone and does not govern access to the data or their use by national authorities. As such, the Directive allows a wide margin of discretion to the national legislature. Since the BVerfG thereby discovered the Kompetenz-Kompetenz to examine its own jurisdiction, it held that Germany was in a position to implement the Directive in such a manner that avoids any fundamental rights clashes with the Grundgesetz. It should be noted, however, that the Grundgesetz does not prohibit data storage in all circumstances. In fact, the BVerfG found that a six-month retention period is legitimate, for that transient breach of privacy does not amount to a blanket interception of the public’s communications. Yet, the Court emphasised that this is not the case when it comes to all-encompassing and intrusive legislation. Hence the ruling suspended the domestic legislation until appropriate amendments restricting its scope were introduced by the German Parliament.

By way of conclusion, it can be argued that this judgment was not aimed at raising a challenge to the application of EU law in Germany. On the contrary, the BVerfG’s reasoning was based on the Directive’s method of implementation by the German Parliament. It was this that was in breach of art.10 GG. Inevitably, the BVerfG’s rhetoric brings to mind its Solange jurisprudence. But, far from it, the German judgment encompasses both a firm judicial recognition of the grounds of adoption of the Directive (as a First Pillar instrument) and an adherence to EU harmonisation of retention of traffic data (as a means of eliminating obstacles to the internal market). All in all, the BVerfG distinguished between the internal market aspect of the Directive (data retention by service providers) and its criminal aspects (access to data and their use and exchange between law enforcement authorities). While it attributed competence to regulate the former to the European Union, it characterised the latter (in accordance to arts 7 and 13 of Directive 2006/24) as an issue that is in the competence of the Member States. This orthodox analysis of competence delimitation by the BVerfG saved it from having to refer the matter to the ECJ. The BVerfG also distanced itself from the German decision because the latter rejected altogether the obligation of data retention. Thus, the Romanian Constitutional Court’s attack was not limited to the relevant implementation process but to the Europeanisation of the system of data retention. In its view, this new process deprived the right to private and family life protected under art.8 ECtHR.

Analysis

It is evident from the discussion of the judgments related to the transposition of Directive 2006/24 that all relevant national courts employed, in one way or another, an “adequate safeguards” review. Such an approach took into account the legality, legitimate purpose and proportionality of the contested implementation measures. It is not surprising that each court called upon to review the relevant data retention legislation arrived at a different conclusion. The Irish High Court preferred to refer the case to the ECJ for an assessment of the Directive’s validity. The Romanian Constitutional Court decided to shut its eyes to EU law, expressing its general dislike of any trend towards a general system of data surveillance. The German Constitutional Court chose to adjudicate on the case by merely highlighting those aspects of the Directive that relate to the exercise of national competence. However, crucial, these judgments tell us only half the story. We
seem to have learned a lot about the mechanics of the constitutionality of national implementation laws vis-à-vis domestic and international human rights guarantees. Regrettably, we cannot claim to have received the same enlightenment about the constitutionality of Directive 2006/24, because—as with any EU legislation—questions about its validity are reserved to the ECJ. No doubt the ECJ’s insights into the substantive aspects of the Directive will be more crucial than its procedural ones as clarified in Ireland v Parliament and Council.This is important since it is obvious, from its implementation misfortunes, that Directive 2006/24 has failed to harmonise national legislation and has led to legal uncertainty.

At the time of writing, only Sweden has not transposed the Directive. However, implementation has been far from harmonious. The Commission has taken numerous actions against non-compliant Member States under art.258 TFEU, most of which have complied with the ECJ’s judgment by putting relevant legislation in place.22 As previously observed, these actions stemmed from Member States’ rejection of national implementing legislation for being in breach of the fundamental rights enshrined in the ECHR and their own national constitutions. The present author is not aware of an enforcement action against either Germany or Romania. This makes one wonder whether Member States possessing constitutional courts enjoy more latitude than their counterparts to implement and enforce EU law. For instance, Romania received a letter from the Commission as late as June 16, 2011, warning the Government of the consequences of non-implementation.

In any event, it is argued here that enforcement actions against Member States are rather unfitting, for three reasons: first, because on July 7, 2010, the European Union started negotiations for its accession to the ECHR; secondly, because it is hazardous for the Commission to rule with an iron fist by forcing Member States to adopt data retention legislation that is incompatible with their constitutions; and thirdly, because in its April 2010 plan of actions for the implementation of the Stockholm Programme, the Commission included a plan for an evaluation, followed by a possible proposal for revision, of Directive 2006/24.43

Following its April 2010 plan, the Commission held a conference on (December 3, 2010) entitled “Taking on the Data Retention Directive” as part of the ongoing evaluation process of Directive 2006/24. The conference consisted of experts from police authorities, national ministries, data protection authorities, industry, civil society and the scientific community. The Commission appeared to have been persuaded to consider a broad review of the Directive, focusing on nine variables.43 Since the Directive harmonises only the obligation of service providers to store data about their customers’ communications—something that had already taken place in some Member States for commercial purposes—a number of questions remain unanswered regarding its necessity and added value. To name but a few, taking stock of the variables presented by the Commission:

- Who qualifies for the retention of data? Since the Directive does not specify the types of national authorities competent to access retained data, there is a danger that even private parties may use retained data for purposes other than those identified by the Directive.
- To what kinds of crimes is data retention applicable and what should the threshold be for the definition of “serious crimes”? This is uncertain, especially since

---


44 European Commission, Directorate General for Home Affairs, Data Retention Directive (Brussels, December 3, 2010) at http://www.statewatch.org/privacy/2010/revineurope/novem_10/novem_10_data_retention-page.pdf [Accessed September 2, 2011]. The nine variables presented by the Commission are: (1) purpose of data retention; (2) scope; (3) data retention period; (4) definition of serious crime; (5) authorities with access; (6) mode of access and cross-border transfer; (7) operation under retention obligations; (8) cost recovery; (9) data security.

the Directive does not provide any definition of serious crime. Perhaps the Directive could borrow from the list of serious crimes provided in the 2002 Framework Decision on the European Arrest Warrant. This may be a starting point, but it is not a panacea, especially given the fact that various forms of undesirable conduct as listed in art.2(2) of the Framework Decision do not constitute any criminal offence under the laws of some Member States.64
• Who would pay the costs of retention (the criminals or the state)?65 The Directive does not provide any guidance as to reimbursement of public communications providers for additional costs they incur.
• Should the European Union adopt further legislation harmonising access to data or their use by national authorities, as well as introducing stronger safeguards against disproportionate state interference with individual freedoms? It appears that EU citizens are very much in favour of restrictions on privacy as a means of countering terrorism. A 2008 Eurobarometer survey showed that 64 per cent of survey participants were concerned as to whether their data are handled appropriately by the relevant organisations. But what is most revealing is that most EU citizens agreed that "the fight against international terrorism is an acceptable reason to restrict data protection rights". The respondents agreed that "it should be possible to monitor passenger flight details (82%), telephone calls (72%) and Internet and credit card usage (75% and 89%, respectively) when this served to combat terrorism".66

The Directive's revision prior to the ECJ's Data Retention judgment is an interesting development, given that the Directive has led Member States to an incoherent set of national measures. This was most recently emphasised in the Commission's 2011 evaluation report.67 Perhaps a Kadi-style system of targeted application may replace the Directive's current system of general application. Whatever the case may be, protection of the right to privacy has to be a top priority. The ECJ's recent case law suggests that the threshold for allowing data retention is high. For instance, in the recent case of Schreke and Effer, the ECJ delivered a remarkable judgment regarding transparency laws in the management of funding for the Common Agricultural Policy (CAP).68 This contested EU legislation required disclosure and publication on a publicly accessible website of the names, residences, and amounts awarded to farmers from CAP funds. It was held that this legislation infringed the farmers' right to privacy and personal data.69 The ECJ therefore declared Regulation 259/2008 to be invalid and also certain provisions of Regulation 1290/2005, stressing that the Council and the Commission breached the principle of proportionality.70 Will the Data Retention Directive share the same fate? Probably not. Its alleged necessity seems to outweigh any proportionality concern. One should recall that Directive 2006/24 only goes as far as harmonising the obligations of providers of publicly available electronic communications or of public communications networks to retain individual data for the purpose of the investigation, detention and prosecution of serious crime, as defined by each Member State in its

65 A constitutional challenge by Alors Telecom against the relevant implementation law was rejected in France. However, the Conseil d'Etat held on August 7, 2007 that criminals should pay the costs. The decision is available at http://www.legifrance.gouv.fr/juri/decision.php?juriId=2007DCR0079&date=20070807 (Accessed September 2, 2011).
68 Volker and Markus Scholze v Land Hessen (C-32/09 and C-33/09), November 8, 2010.
70 See also Promociunea v Moldova (C-279/06) [2008] E.C.R. I-273, [2008] 2 C.M.L.R. 12. Here, the ECJ stated that there is no obligation upon Member States to disclose personal data in civil proceedings (proportionality).
national law. As a result, the retained data shall be disclosed to the relevant public enforcement authorities in accordance with the national laws of each Member State.

Conclusion
Whatever the fate of Directive 2006/24 may be, one can hardly applaud the EU institutions for harmonising regulation all across the European Union with reference to the collection and processing of personal data in the telecommunications market. Implementation has been uneven between Member States, both with regard to retention periods and data protection safeguards. The haste of national executives to boost the European Union's profile in this area has not been met with success. National courts are acting as guardians of our constitutional ecosystem. They have compensated for the lack of parliamentary involvement in the adoption of EU legislation either by being critical of the excesses of their executives in the Council or by insisting on bringing national parliaments into the EU legislative terrain, i.e. rendering national implementation of EU law dependent upon rigid parliamentary oversight. In particular, as is the case in Germany, the Parliament has been called upon by the BVerfG to restrain the scope of pre-emptive EU legislation that may run counter to national constitutional identity, a value explicitly mentioned in art.4(2) TEU. This would take place when EU legislation is intra vires—i.e. where the European Union has been acting in compliance with the principle of conferral (art.5(1) TEU). Indeed, the increased involvement of national parliaments in the European Union's legislative process is a crucial step in the clarification and re-distribution of competences at European level.

No doubt the lack of clarity surrounding the Directive leaves a broad margin of interpretation to national legislatures. Hence Member States should be reminded that the Directive in itself neither harmonises the powers of the state to spy on its citizens nor prescribes the rights of citizens against state power abuse. What is more, the European Union possesses no coercive powers of its own. It rather relies on Member States to implement and enforce EU legislation, using—in this case—exports from both industry and law enforcement authorities. To that extent, it is apparent that Member States hold the keys to open or shut the gates of the surveillance state. For instance, in the United Kingdom, even prior to the inception of the Data Retention Directive, communications data were an essential component of prosecution evidence in 96 per cent of cases concerning serious crimes.22 On the other hand, Commission statistics from 2008 to 2009 indicate that, out of two million data requests made in compliance with Directive 2006/24, one million emanated from Poland alone.23 Mandatory and consistent retention of telecommunications data requires the establishment of sufficient safeguards covering access to that material. Five years after its adoption, the Data Retention Directive is still confronted with both procedural and substantive questions.24 It remains, therefore, as contentious and publicly controversial as any transfer of sovereignty away from Member States to EU level.

25 These include, for instance, privacy concerns vis-à-vis data protection and access to the retained data, inconsistencies between national practices concerning its scope of application and retention periods, criticism from activist groups related to its general application and prospective nature, questions of legitimacy and effectiveness, and academic queries related to the permissible degree of EU centralization. See Digital Civil Rights in Europe, “Top 10 Misleading Statements of the European Commission on Data Retention” (April 20, 2011). http://www.edril.org/edrilorg/number35/datal-retention-evaluation [Accessed September 2, 2011].