Swiss Review of International and European Law

Schweizerische Zeitschrift
für internationales und europäisches Recht

Revue suisse de droit international et européen

Volume 27 (2017), Number 4

Schulthess §

Swiss Review of International and European Law

Schweizerische Zeitschrift für internationales und europäisches Recht

Revue suisse de droit international et européen

ISSN 1019-0406 www.sriel.ch

The Review is published quarterly by the Swiss Society of International Law (Schweizerische Vereinigung für internationales Recht / Société suisse de droit international – www.svir-ssdi.ch) and supported by the Swiss Academy of Humanities and Social Sciences. The Review is available online on www.swisslex.ch and www.heinonline.org.

Submissions
Please submit manuscripts electronically to the Managing Editor (Lorenz.Langer@sriel.ch). Authors are requested to follow the Reivew's style-sheet available at www.sriel.ch. French submissions are proofread by Dr. Maria Ludwiczak.

Subscriptions
For subscriptions, please contact our publisher, Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zurich, Switzerland, Phone: +41 (0)44 209 2929, Fax: +41 (0)44 200 2928, service@schulthess.com, www.schulthess.com.
Annual subscription: CHF 258 (CHF 250 for SVIR-members); single issue: CHF 73; PrintPlu§: The PrintPlu§ subscription includes both the printed issues of the Review and digital access to its content. Annual Print Plu§ subscription: CHF 294 (CHF 261 for SVIR-members); for details, see www.schulthess.com.

Advertisements
Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Phone +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Table of Contents

Europe v. USA: Different Standards and Procedures in Human Rights Protection

Stephan Breitenmoser & Chiara Piras*

This contribution shows the important role of regional law and institutions in the development and rise of international human rights standards. By analyzing two main areas of human rights law – the prohibition of the death penalty and data protection – this article outlines how the level of protection guaranteed by the European states is far more advanced than equivalent regulations on a universal level or in other regions of the world. The examples discussed also confirm that human rights are further developed and strengthened on the European level where treaties and procedures ensure a more efficient implementation of the relevant norms and, finally, that a sharp divide gradually opens up between Europe and the United States.

Table of Contents

I. Introduction

At the June 1993 World Conference on Human Rights, representatives of 171 states unanimously adopted the Vienna Declaration and Program of Action containing the principles of universality and indivisibility of human rights. Yet, in this Declaration the states also proclaimed that regional arrangements play a fundamental role in pro-

* Stephan Breitenmoser is Professor of European Law at the Faculty of Law, University of Basel, and Judge at the Swiss Federal Tribunal of Administrative Law. Chiara Piras is a Researcher at the Faculty of Law, University of Basel, and Law Clerk at the Court of Appeals of the Canton of Basel-Country. The authors are grateful to Ann Weibel, MLaw, for her valuable support during the drafting of this text.

moting and protecting human rights and that they should reinforce universal human rights standards and their protection. The Conference endorsed efforts to strengthen these regional arrangements and to increase their effectiveness, while at the same time stressing the importance of cooperation with the United Nations human rights activities.[1]

Indeed, the dynamic evolution of human rights protection after World War II has led to a remarkable network of universal, regional and specialized human rights treaties and procedures. It has also created a close formal and informal cooperation within regional bodies. Because of different legal rules, jurisdiction and cultural understanding, this may result in a regionalism that could lead to a fragmentation of the international human rights protection system.[2]

However, in human rights law such fragmentation should not always be considered as an infringement or even a violation of the principles of universality and indivisibility. On the contrary: The specific development of higher regional standards, norms and practices may be seen as a first step in reaching a higher common standard of human rights protection. As a consequence, more and more international, constitutional and supreme courts may start applying the higher standards and follow the positive experiences of more advanced regions in the safeguarding of human rights.

Numerous examples of regional international law can, in fact, be found in European administrative law.[3] These include, in particular, the protection of fundamental

1 The Vienna Declaration and Program of Action, adopted by the World Conference on Human Rights in Vienna on 25 June 1993, formulated that «All human rights are universal, indivisible and interdependent and interrelated» (para. I.5) and that «Regional arrangements play a fundamental role in promoting and protecting human rights» (para. I.37).

2 Cf. Martti Koskenniemi, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of international Law, Report of the Study Group of the International Law Commission, UN Doc. A/CN.4/L.682 of 13 April 2006, para. 5 *et seqq.*, pp. 10 *et seqq.;* Lars Viellechner, Verfassung als Chiffre: Zur Konvergenz von konstitutionalistischen und pluralistischen Perspektiven auf die Globalisierung des Rechts, 75 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (2015), 233–258, pp. 244 *et seqq.*

3 Cf. Stephan Breitenmoser & Chiara Piras, Regionalisierung des internationalen Menschenrechtsschutzes, in: Georg Kreis (ed.), Europa und die Welt: Nachdenken über den Eurozentrismus, Basel 2012, pp. 77–108; Thomas Cottier et al., Die Rechtsbeziehungen der Schweiz und der Europäischen Union, Bern 2014, pp. 554 *et seq.;* Thomas Cottier, Die Globalisierung des Rechts – Herausforderungen für Praxis, Ausbildung und Forschung, 133 Zeitschrift des Bernischen Juristenvereins (1997), pp. 217–241, pp. 217 *et seqq.;* Karl Doehring, Völkerrecht, 2nd ed., Heidelberg 2004, at 293; Walter Kälin et al., Völkerrecht: Eine Einführung, 4th ed., Bern 2016, p. 91; Bernhard Kempen & Christian Hillgruber, Völkerrecht, 2nd ed., München 2012, pp. 304 *et seqq.;* Jürgen Schwarze, Europäisches Verwaltungsrecht, 2nd ed., Baden-Baden 2005, LII *et seqq.;* Stephen Sedley, Are Human Rights Universal, and Does it Matter?, in: Stephan Breitenmoser et al. (eds.), Human Rights, Democracy and the Rule of Law, Menschenrechte, Demokratie und Rechtsstaat, Droits de l'homme, démocratie et Etat de droit, Liber amicorum Luzius Wildhaber, Zurich/St. Gallen 2007, pp. 793–803; Alfred Verdross & Bruno Simma, Universelles Völkerrecht, Theorie und Praxis, 3rd ed., Berlin 1984, para. 30; Wolf-

rights and guaranties such as human dignity, the protection of privacy and basic procedural rights, which are, in general, of a higher standard than universal international law.[4]

This article will show and discuss the normative content of two main areas of human rights law, which may represent a fragmentation between the level of protection in Europe and their universal grade of protection in other regions,[5] in particular in the United States: These two areas being the prohibition of the death penalty and data protection.

II. The Prohibition of the Death Penalty

A. A Post-Second World War Phenomenon

Whilst the death penalty has existed since antiquity,[6] international norms addressing the limitation and abolition of the death penalty are essentially a post-Second World War phenomenon.[7] The abolition of the death penalty was first promoted on an international level during the drafting of the Universal Declaration of Human Rights between 1946 and 1948 and the recognition of «the right to life» in its Article 3.[8] After the set-up of the International Military Tribunal *(Nuremberg Tribunal)* to prosecute and punish the leaders and organizations of Nazi Germany accused of war crimes, crimes against peace and crimes against humanity, which provided for the possibility of capital punishment,[9] only a few states contemplated the abolition of the death penalty. This idea, however, gained strength in the following decades. It started with the limitation of the death penalty excluding juveniles, pregnant women and

gang Vitzthum, Völkerrecht, 7th ed., Frankfurt/Bonn 2016, p. 11; Andreas von Arnauld, Zum Status quo des europäischen Verwaltungsrechts, in: Jörg Philipp Terhechte (ed.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, pp. 89 *et seqq.;* Thomas von Danwitz, Europäisches Verwaltungsrecht, Köln 2008, pp. 210 *et seqq.*

4 Cf. Thomas Giegerich, Wirkungen und Rang der EMRK in den Rechtsordnungen der Mitgliedstaaten, in: Rainer Grote & Thilo Marauhn (eds.), EMRK/GG, Konkordanzkommentar, 2nd ed., Tübingen 2013, p. 87.

5 Cf. Koskenniemi, supra, n. 2, 95–219, at 102.

6 Cf. William A. Schabas, The Abolition of the Death Penalty in International Law, 3rd ed., Cambridge 2002, p. 3.

7 Schabas, supra, n. 6, at p. 1.

8 UN Economic and Social Council, Commission on Human Rights Drafting Committee, Draft Outline of international Bill of Rights (prepared by the Division of Human Rights), E/CN.4/AC.1/3 of 4 June 1947, Article 3; First Addendum, E/CN.4/AC.1/3/Add.1 of 11 June 1947, pp. 14–19 and Second Addendum, E/CN.4/AC.1/3/Add.2 of 9 June 1947.

9 Cf., on the other hand, Statute of the International Criminal Tribunal for the former Yugoslavia, UN Doc. S/Res/827 (1993) Annex, Article 24 (1); Statute of the International Criminal Tribunal for Rwanda, UN Doc. S/RES/955 (1994), Annex, Article 23(1). Both Tribunals can only impose terms of imprisonment.

the elderly and the restriction of the list of crimes for which the death sentence could be allowed.[10]

On a regional level, the American Convention on Human Rights prevents countries which have already abolished the death penalty from reintroducing it.[11] The African Charter on Human and Peoples' Rights does not mention the death penalty. Nevertheless, it provides for an unqualified right to life. The African Commission on Human and People's Rights adopted a resolution calling for a moratorium on the use of capital punishment.[12] The Arab Charter of Human Rights proclaims the right to life in the same manner as other international instruments, but contains three provisions recognizing the legitimacy of the death penalty in cases of «the most serious crimes». It prohibits the death penalty for political offences and excludes capital punishment for crimes committed by those under the age of eighteen, and for both pregnant women and nursing mothers for a period of up to two years following childbirth.[13] The states that still retain the death penalty find themselves increasingly subject to international pressure in favor of abolition. This becomes manifest, for

10 The UN General Assembly, *inter alia,* affirmed in Resolution 2857 (XXVI) of 20 December 1971 the desirability of abolishing the death penalty in all countries. This aspiration was reiterated in UN General Assembly Resolution 32/61 of 8 December 1977 and in the United Nations General Assembly Resolution 62/149 adopted on 18 December 2007, which called for a worldwide moratorium on executions with a view to abolishing the death penalty. In the International Covenant on Civil and Political Rights (ICCPR) of 16 December 1966, 999 U.N.T.S. 1), the Convention on the Rights of the Child (CRC) of 20 November 1989, 1577 U.N.T.S. 3) and in the United Nations Economic and Social Council (ECOSOC) Safeguards Guaranteeing Protection of the Rights of those facing the death penalty, 45th plenary meeting on 23 July 1996, Resolution 1996/15) the United Nations has established strict conditions under which it may be used by those member states, which have not yet abolished it; Human Rights Committee, *Judge v. Canada,* Communication No. 829/1998, UN Doc. CCPR/C/D/829/1998 of 5 August 2002. In this case the Human Rights Committee expressed the opinion that for countries that have abolished the death penalty there is an obligation not to expose a person to the real risk of its application. Thus, they may not remove, either by deportation or extradition, individuals from their jurisdiction, if it may be reasonably anticipated that they will be sentenced to death, without ensuring that the death sentence would not be carried out. The Second Optional Protocol to the ICCPR aiming at the Abolition of the Death Penalty of 15 December 1989, 1642 U.N.T.S. 414, commits each state party to take all necessary measures to permanently abolish the death penalty within its own jurisdiction. However, this Protocol has only been ratified by 85 states so far (cf. http://treaties.un.org); cf. William A. Schabas, The United Nations and Abolition of the Death Penalty, in: Jon Yorke (ed.), Against the Death Penalty, International Initiatives and Implications, Surrey 2008, pp. 9–43 with further references.

11 American Convention on Human Rights (1979) 1144 U.N.T.S. 123, Article 4.2.

12 Resolution urging states to envisage a moratorium on the death penalty, 13th Activity Report of the African Commission on Human and People's Rights, OAU Doc. AHG/Dec. 153(XXXVI), Annex IV, pp. 45 *et seqq*.

13 Arab Charter on Human Rights, adopted on 15 September 1994, Council of the League of Arab States (102nd sess.), Res. 5437, Articles 10, 11 and 12.

example, in some states' refusal to grant extradition, if the person concerned risks being exposed to the capital sentence.[14]

B. The Council of Europe's Campaign for a World-wide Abolition of the Death Penalty

The Council of Europe has been the driving force in the endeavors to transform Europe into a *de facto* and *de jure* death penalty free zone.[15] It monitors the situation in member states to ensure compliance with their commitments and exchanges views on the situation of the abolition of the death penalty. It also persuades governments to permanently outlaw the death penalty, adopts successive texts and supports all initiatives aiming at a worldwide moratorium on the use of the death penalty, in particular the Resolutions of the United Nations General Assembly.[16] The creation of legally binding instruments and the case-law of the European Court of Human Rights (ECtHR) has greatly contributed to achieving this aim.

1. Legal Instruments Towards the Abolition of the Death Penalty in Europe

The European Convention on Human Rights (ECHR) provided in 1950 for the possibility of imposing the death penalty in execution of a court sentence following conviction of a crime for which the death penalty was provided by law.[17] Since then, the legal situation in Europe has changed dramatically: From the late 1960s, a consensus began to emerge in Europe that the death penalty seemed to serve no purpose in a civilized society governed by the rule of law and respect for human rights. In 1982, the Council of Europe adopted Protocol No 6 to the ECHR, the first legally binding

14 Cf. Chapter II.B; Schabas, supra n. 6, at p. 2; Ulrich Häfelin et al., Schweizerisches Bundesstaatsrecht, 9th ed., Zurich 2016, pp. 107 and 179; Jörg Paul Müller & Markus Schefer, Grundrechte in der Schweiz, 4th ed., Bern 2008, p. 50; Robert Weyeneth, Die Menschenrechte als Schranke der grenzüberschreitenden Zusammenarbeit der Schweiz, recht 2014, pp. 117 and 120.

15 Cf. Roger Hood & Caroline Hoyle, The Death Penalty: A Worldwide Perspective, 5th ed., Oxford 2015, pp. 49 *et seqq.* as to the abolition of the death penalty in European countries; Jon Yorke, The Evolving Human Rights Discourse of the Council of Europe: Renouncing the Sovereign Right of the Death Penalty, in: Jon Yorke (ed.), supra n. 10, pp. 43–75 with further references.

16 Resolution adopted by the General Assembly on 20 December 2012 on the report of the Third Committee (A/67/457/Add.2 and Corr.1), UN Doc. A/RES/67/176.

17 Cf. original wording of Article 2 para. 1.

instrument providing for the abolition of the death penalty in peacetime.[18] Since then, all member states of the Council of Europe have abolished the death penalty in peacetime. The Russian Federation is an exception, as it has signed, but not yet ratified the Protocol No. 6 while, nevertheless, respecting a moratorium on the death penalty since soon after its accession to the Council of Europe in 1996. In 2003, the Council of Europe adopted the second legally binding instrument providing for the abolition of the death penalty in all circumstances, including war times: Protocol No. 13 to the ECHR.[19]

The Committee of Ministers monitors the situation in member states to ensure compliance with their commitments. It exchanges views on the state of abolition of the death penalty every six months and asks states which have not yet signed or ratified Protocols Nos. 6 and 13 to the ECHR to provide information on their intentions. It has been claimed that Europe has become a *de facto* «death penalty free area».[20] Yet the Council's objective is that Europe become a *de jure* death penalty free zone. The Committee of Ministers also issues declarations condemning executions taking place in observer states, reiterating its unequivocal opposition to capital punishment in all places and under all circumstances. The Parliamentary Assembly of the Council of Europe has also been a driving force in the movement to abolish the death penalty since the 1980s. It has gradually persuaded governments to permanently outlaw the death penalty or to commit to a moratorium on executions. The Assembly was at the origin of Protocol No 6 to the ECHR and has since adopted successive texts.[21] It has also extended its activity to those countries which have observer status at the Council of Europe, in particular Japan and the United States of America. Thus, it has repeatedly urged the U.S. government to abolish the death penalty.[22]

18 Protocol No. 6 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the abolition of the death penalty of 28 April 1983, European Treaty Series No. 114; cf. Stephan Breitenmoser, Boris Riemer & Claudia Seitz, Praxis des Europarechts, Grundrechtsschutz, Zurich 2006, p. 27; Jens Meyer-Ladewig, Martin Nettesheim & Stefan von Raumer, Europäische Menschenrechtskonvention, 4th ed., Baden-Baden 2017, pp. 446 *et seqq.;* Jörg Paul Müller & Luzius Wildhaber, Praxis des Völkerrechts, 3rd ed., Bern 2000, pp. 614 *et seqq.*

19 Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms, concerning the abolition of the death penalty in all circumstances of 3 May 2002, E.T.S. No 187; cf. Breitenmoser, Riemer & Seitz, supra n. 18, at p. 27; Häfelin et al., supra n. 14, at pp. 69 and 105 *et seq.;* Meyer-Ladewig, Nettesheim & von Raumer, supra n. 18, at pp. 462 *et seqq.;* Müller & Schefer, supra n. 14, at p. 49.

20 Cf. David Harris et al. (eds.), Law of the European Convention on Human Rights, 3rd ed., Oxford 2014, p. 963.

21 In particular, Resolution 1253 (2001, Doc. 9115) of 25 June 2001 and Recommendation 1760 (2006, Doc. 10911) of 28 June 2006 of the Council of Europe Parliamentary Assembly.

22 Cf. Resolution 1807 (2011) of 14 April 2011; Helen Keller, Todesstrafe vorbehalten. Zulässige Einschränkung internationaler Menschenrechtsgarantien durch die Vereinigten Staaten?, 23 Swiss Rev. Int'l & Eur. L. (SZIER/RSDIE) (2003), 113–142.

2. The European Court of Human Rights' Case-law

The ECtHR has ruled since 1989 that the exposure to the pervasive and growing fear of execution – the so called «death row phenomenon» – is in violation of the ECHR.[23] In addition, the Court has been asking member states, as addressed states in an extradition process, to require firm diplomatic assurances from requesting countries that persons to be extradited or expelled will not be sentenced to death.[24] This principle has been followed by courts in numerous countries, also outside of Europe, including Canada[25] and South Africa.[26] The ECtHR also held in 2005 that capital punishment in peacetime had come to be regarded as an unacceptable form of punishment which was no longer permissible under Article 2 of the Convention.[27] In 2010, the ECtHR considered that the death penalty involved the deliberate and premeditated destruction of a human being by the state authorities.[28]

23 ECtHR, *Soering v. United Kingdom,* Judgment of 7 July 1989, App. No. 14038/88. In this decision, the ECtHR found for the first time that the state's responsibility could be engaged if it decided to extradite a person who risked being subjected to ill-treatment in the requesting country. In this case, the Court held that there would be a violation of Article 3 (prohibition of torture and inhuman or degrading treatment) of the ECHR if he were to be extradited to the United States due to a real risk of being put on «death row», treatment going beyond the threshold set by Article 3; cf. Breitenmoser, Riemer & Seitz, supra n. 18, at p. 23.

24 ECtHR, *Cruz Varas v. Sweden,* Judgment of 20 March 1991, App. No. 15576/89; ECtHR, *Vilvarajah and Others v. United Kingdom,* Judgment of 30 October 1991, App. Nos. 13163/87; 13164/87; 13165/87; 13447/87; 13448/87; ECtHR, *Chahal v. United Kingdom,* Judgment of 15 November 1996, App. No. 22414/93; ECtHR, *Saadi v. Italy,* Judgment of 28 February 2008, App. No. 37201/06; ECtHR, *Baysakov and Others v. Ukraine,* Judgment of 18 February 2010, App. No. 54131/08; ECtHR, *Klein v. Russia,* Judgment of 1 April 2010, App. No. 24268/08; ECtHR, *Babar Ahmad and Others v. United Kingdom,* Judgment of 10 April 2012, App. No. 24027/07; ECtHR, *Omar Othman v. United Kingdom,* Judgment of 17 January 2012, App. No. 8139/09, this was the first time that the Court had found that an expulsion would also be in violation of Article 6, which reflects the international consensus that the use of evidence obtained through torture makes a fair trial impossible.; cf. Breitenmoser, Riemer & Seitz, supra n. 18, at p. 320.

25 Human Rights Committee, *Judge v. Canada,* supra n. 10, at para. 10.4.

26 In July 2012, the Constitutional Court of South Africa found that deporting individuals to a state in which they might face execution would violate the right to life of the persons concerned; *Minister of Home Affairs and Others, Tsebe and Others, Minister of Justice and Constitutional Development and Another, Tsebe and Others,* CCT 110/11, CCT 126/11, (2012) ZACC 16 73.

27 ECtHR, *Öcalan v. Turkey,* Judgment of 12 May 2005, App. No. 46221/99, para. 88. The Court also found that the evolution towards the complete abolition of the death penalty, in law and in practice, within all 47 Council of Europe member states had demonstrated that Article 2 ECHR had been amended to prohibit the death penalty in all circumstances.

28 ECtHR, *Al-Saadoon and Mufdhi v. United Kingdom,* Judgment of 2 March 2010, App. No. 61498/08.

C. The Complete Abolition of the Death Penalty by the EU

Today the prohibition of the death penalty is one of the essential requirements for membership not only in the Council of Europe but also for accession to the European Union (EU). The latter confirmed and reinforced this trend by adopting the EU Charter of Fundamental Rights (EU Charter). The EU Charter states in Article 2 paragraph 2 that no one shall be condemned to the death penalty or executed. The EU Charter guarantees, in accordance with the long-standing practice of the ECtHR,[29] that a person shall not be exposed to the risk of the death penalty, be it through removal, expulsion or extradition, either within or outside of Europe.[30] The countries of Europe have thus, by general practice and belief, achieved the prohibition of the death penalty, made it legally binding and given it an imperative nature. It must be concluded that the ban is part of the solid core of human rights in Europe and allows for no exceptions, therefore it must be acknowledged as regional *ius cogens*.[31]

D. The Death Penalty in the United States

In the United States, the arguments for and against the capital punishment have been subject of countless debates.[32] After the end of World War II, the number of executions carried out in the United States declined rapidly and culminated in the U.S. Supreme Court's 1972 decision *Furman*.[33] In this judgment the Court determined

29 Cf. supra n. 23 and 24.

30 Article 19 para. 2 EU Charter; for the case-law since *Soering* cf. Breitenmoser, Riemer & Seitz, supra n. 18, at p. 38 *et seqq*.

31 Cf. Breitenmoser, Riemer & Seitz, supra n. 18, at p. 23; Martina Caroni & Maya Taylan, Zwingendes Völkerrecht, recht 2015, pp. 55–66, p. 64; Fausto De Quadros, La Convention Européenne des Droits de l'Homme: un cas de ius cogens régional?, in: Ulrich Beyerlin, Michael Bothe, Rainer Hoffmann & Ernst-Ulrich Petersmann (eds.), Recht zwischen Umbruch und Bewahrung, Festschrift für Rudolf Bernhardt, Berlin/Heidelberg 1995, p. 560, with further references; Sévrine Knuchel, Jus Cogens: Identification and Enforcement of Peremptory Norms, Zurich 2015, p. 56 *et seqq.;* Eva Kornicker, Ius Cogens und Umweltvölkerrecht, Kriterien, Quellen und Rechtsfolgen zwingender Völkerrechtsnormen und deren Anwendung auf das Umweltvölkerrecht, Diss., Basel/Frankfurt am Main 1997, pp. 63 *et seqq.;* Roger Nobs, Volksinitiative und Völkerrecht, Eine Studie zur Volksinitiative im Kontext der schweizerischen Aussenpolitik unter besonderer Berücksichtigung des Verhältnisses zum Völkerrecht, St. Gallen 2006, p. 111; Chiara Piras & Stephan Breitenmoser, Das Verbot der Todesstrafe als regionales ius cogens, Aktuelle Juristische Praxis (AJP), 2011, 331–338, at 335 *et seqq.;* Tristan Zimmermann, Quelles normes impératives du droit international comme limite à l'exercice du droit d'initiative par le peuple?, AJP 2007, 748–760, at 758; more reserved Helen Keller, Volksrechte und Menschenrechte in Sachen Todesstrafe, Neue Zürcher Zeitung, 26 August 2010, p. 21.

32 Cf. a comprehensive collection of arguments discussed in the United States in Barry Latzer & David McCord, Death Penalty Cases, Leading U.S. Supreme Court Cases on Capital Punishment, 3rd ed., New York 2011, pp. 9 *et seqq*.

33 United States Supreme Court, *Furman v. Georgia,* 29 June 1972, 408 U.S. 238 (1972); cf. Keller, supra n. 22, p. 117.

that the death penalty was unconstitutional, as it was being applied in an arbitrary and discriminatory manner, contrary to the Eighth[34] and Fourteenth Amendments to the Constitution.[35]

In *Gregg*[36] the U.S. Supreme Court set forth two main features that capital sentencing procedures must employ in order to comply with the Eighth Amendment ban on «cruel and unusual punishments». First, the scheme must provide objective criteria to direct and limit the death sentencing discretion. Second, the scheme must allow the judge or jury to take into account the character and record of the individual defendant.[37]

In *Ford*[38] the Supreme Court made a preliminary finding that the Eighth Amendment bars states from inflicting capital punishment upon persons with a mental disorder.

In 2002, the Court ruled in *Atkins,*[39] that since so few states allowed execution of the mentally retarded, the practice had become «unusual». Moreover, justifications for the death penalty, such as retribution on the part of the defendant and deterrence of capital crimes by prospective offenders, did not apply to the mentally retarded. Accordingly, the Court categorically excluded such persons from execution under the Eighth Amendment.[40]

In *Thompson*[41] the Supreme Court concluded that the Eighth Amendment prohibits the execution of a person who was under 16 years of age at the time of his or her offense.[42]

In *Roper*[43] the Supreme Court ruled that the opposition to juvenile death penalty in the majority of states, the infrequency of its use even where it remains on the books and the consistency in the trend toward abolition of the practice provide sufficient evidence that society viewed juveniles as «categorically less culpable than the average criminal». Since a majority of states had rejected the imposition of the death penalty

34 The Eighth Amendment to the U.S. Constitution states: «Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.» This amendment prohibits the federal government from imposing unduly harsh penalties on criminal defendants, either as the price for obtaining pretrial release or as punishment for crime after conviction; cf. Martin Kau, in: Katharina Pabel & Stefanie Schmahl (eds.), IntKomm EMRK, Köln/Berlin/München 2015, Article 3, para. 4 and 112 *et seqq.*

35 Cf. Hood & Hoyle, supra n. 15, p. 129.

36 United States Supreme Court, *Gregg v. Georgia,* 2 July 1976, 428 U.S. 153 (1976).

37 In their concurring opinions Justice Brennan and Justice Marshall held that the «cruel and unusual punishments clause must draw its meaning from the evolving standards of decency that mark the progress of a maturing society.»

38 United States Supreme Court, *Ford v. Wainwright,* 26 June 1986, 477 U.S. 399 (1986).

39 United States Supreme Court, *Atkins v. Virginia,* 20 June 2002, 536 U.S. 304 (2002).

40 Cf. Keller, supra n. 22, p. 119 *et seq.*

41 United States Supreme Court, *Thompson v. Oklahoma,* 29 June 1988, 487 U.S. 815 (1988).

42 Cf. Keller, supra n. 22, p. 119.

43 United States Supreme Court, *Roper v. Simmons,* 1 March 2005, 543 U.S. 551 (2005).

on juvenile offenders under the age of 18, the Court held that this was required by the Eighth Amendment.[44]

E. A Lack of Consensus

While the endeavors to enforce a global ban on capital punishment are limited by the heterogeneity of the states still practicing it, like – amongst many others – the United States, their different cultural backgrounds, as well as different religious and moral conceptions and therefore a lack of consensus on this issue, Europe has shown on a regional level that common standards, procedures and values can be enforced beyond national borders. The abolishment of the death penalty in Europe shows the practical significance of the emergence of supranational[45] human rights protection mechanisms in states with a consensus on common human rights perceptions and standards.[46] On a global level, states are instead still far from a universal abolishment of the death penalty.[47]

III. Data Protection and the Fallen Concept of a «Safe Harbor»

A. Data Protection in Europe

1. Activities by the Council of Europe

In the mid-1970s, the Committee of Ministers of the Council of Europe adopted various resolutions on the protection of personal data, referring to Article 8 of the

44 Cf. for a short overview Müller & Schefer, supra n. 14, p. 50. Cf. also *Jones v. Chappell,* 31 F.Supp. 3d 1050 (C.D. Cal. 2014). 16 July 2014, as to the systemic delay in California's death penalty system rendering it unconstitutional; Patricia Egli, Das System zum Vollzug der Todesstrafe als grausame und ungewöhnliche Bestrafung, Jusletter, 30 March 2015.

45 The concept of supra-nationality is closely connected with the EU as a whole and the ECtHR in the framework of the Council of Europe due to its essential characteristics, especially the independence of its bodies and the majority principle in its decisions; cf. Stephan Breitenmoser & Robert Weyeneth, Europarecht, 3rd ed., Zurich/St. Gallen 2017, pp. 20 *et seqq.;* Matthias Herdegen, Europarecht, 19th ed., Munich 2017, pp. 76 *et seqq.;* Thomas Oppermann, Claus Dieter Classen & Martin Nettesheim, Europarecht, 7th ed., Munich 2016, pp. 21 *et seqq.*

46 As to the legal nature of the prohibition of the death penalty as ordre public, cf. Andreas Donatsch, Internationale Rechtshilfe unter Einbezug der Amtshilfe im Steuerrecht, in: Zürcher Grundrisse des Strafrechts, 2nd ed., Zurich 2015, pp. 80 and 91; Müller & Wildhaber, supra n. 18, pp. 103 *et seqq.;* Anne Peters, Völkerrecht, Allgemeiner Teil, 4th ed., Zurich 2016, p. 85 *et seq.;* Weyeneth, supra n. 14, pp. 114–125, pp. 117 and 120; Robert Weyeneth, Der nationale und internationale ordre public im Rahmen der grenzüberschreitenden Amtshilfe in Steuersachen, Diss., Basel 2017.

47 Cf. Saul Lehrfreund & Parvais Jabbar, Constitutional Developments and the Restriction of the Death Penalty: Judicial Activism in the Commonwealth, 18 Eur. Hum. Rts. L. Rev. 2013, pp. 512–519, p. 518.

ECHR.[48] In order to prevent abuses in the storing, processing and dissemination of personal information by means of electronic data banks in the private sector, the Committee of Ministers of the Council of Europe decided that legislative measures had to be taken in order to protect the privacy of individuals. In consideration of the urgency to take steps to prevent divergences between the laws of member states of the Council of Europe, and pending the elaboration of an international agreement in this field, the Committee of Ministers of the Council of Europe agreed on 26 September 1973 on Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.[49]

2. Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data

After four years of preparation, on 28 January 1981, the Council of Europe set a milestone in data protection by adopting Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[50] Convention 108 has been ratified by 47 countries so far, including all EU member states, most member states of the Council of Europe and one non- member state.[51] The Convention's potential as a universal standard and its open character still serves as a basis for promoting data protection on a global level.

Convention 108 applies to all data processing carried out by both the private and public sectors, such as data processing by the judiciary and law enforcement authori-

48 The concept of «the right to privacy» first emerged in international law in Article 12 of the Universal Declaration of Human Rights, stating that «no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.»

49 Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies. One year later, the Committee of Ministers observed that the use of electronic data banks by public authorities had given rise to increasing concern about the protection of the privacy of individuals. Given that the adoption of common principles in the field of data protection is apt to contribute towards a solution of issues in the member states of the Council of Europe and can help to prevent the creation of unjustified divergences between the laws of the member states on this subject, the Committee of Ministers issued Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector (adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies). Both recommendations advised taking all the necessary steps in the private and the public sector to put certain principles on the protection of the privacy of individuals into effect.

50 Cf. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, E.T.S. No. 108; Breitenmoser & Weyeneth, supra n. 45, No. 1300 *et seqq.*

51 Uruguay, the first non-European country, acceded in August 2013, and Marocco, Mauritius and Senegal are in the process of formalizing accession.

ties.[52] It protects the individual against abuses, which may accompany the collection and processing of personal data, and seeks, at the same time, to regulate the trans-border flow of personal data. The Convention contains several basic principles for data protection which each state must incorporate into its domestic law before the Convention enters into force. According to Convention 108, data protection primarily deals with the protection of natural persons; however, the contracting parties may extend data protection to legal persons, such as business companies and associations in their domestic law.

The Convention has played a major role in setting up legislative policies for most member states of the Council of Europe. In this context, the issue of data protection has been regarded from the outset as a matter of great structural importance for a modern society in which the processing of personal data is assuming an increasingly important role. In 1999, Convention 108 was amended to enable the EU to become a party.[53] In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on trans-border data flows to non-parties, so-called third countries, and on the mandatory establishment of national data protection supervisory authorities.[54]

Due to the emerging privacy challenges resulting from the increasing use of new information and communication technologies, the globalization of processes and the even greater flows of personal data, the Convention has been revised.[55] This revision will, at the same time, strengthen both the Convention's evaluation and follow-up mechanism. Thus, on 18 December 2012, the consultative committee of the Convention presented propositions for a modernization of it;[56] on 23 November 2014, the ad hoc Committee on data protection presented its draft explanatory report of the modernized version of the Convention 108,[57] and on 3 May 2016, the Committee pro-

52 Regarding the collection and processing of personal data, the principles laid down in Convention 108 concern, in particular, fair and lawful collection and automatic processing of data, stored for specified legitimate purposes, be adequate, relevant and not excessive as well as accurate (principle of proportionality).

53 Council of Europe, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (E.T.S. No 181) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; cf. Article 23 (2) of the Convention 108 in its amended form.

54 Council of Europe, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and trans-border data flows.

55 Cf. the Judgments by the Strasbourg Court affirming the need for a strong protection of individuals with regard to the processing of personal data: ECtHR, *Szabó and Vissy v. Hungary,* Judgment of 12 January 2016, App. No. 37138/14 and ECtHR, *Zakharov v. Russia,* Judgment of 4 December 2015, App. No. 47143/06.

56 Propositions of a modernization of the Convention by the consultative committee of the Convention, 18 December 2012, T-PD_2012_04_rev4_E.

57 Draft explanatory report of the modernized version of the Convention 108 by the ad hoc Committee on data protection of 23 November 2014, CAHDATA(2014)06.

duced a consolidated version of the modernization proposals.[58] The draft has been discussed in the competent rapporteur group for over a year now.[59] In the meantime, the EU adopted a new data protection regime, which will be applied by the (more homogeneous) 28 EU member states by 25 May 2018. The new EU data protection rules are more far reaching and thus partly incompatible with the old standards of the original 1981 Convention and its Protocol.[60] An early adoption of the revised Convention 108 will therefore avoid the risk of potential inconsistencies between the legal frameworks of the Council of Europe and the EU and ensure that the Convention 108 will continue to represent the best treaty-based international data protection standards.[61]

3. Data Protection Afforded by the European Court of Human Rights

The collection, storage and disclosure of information about an individual by the state can interfere with the right to respect for private life enshrined in Article 8 ECHR. Such an interference breaches Article 8 ECHR, unless it is «in accordance with the law», pursues one or more of the legitimate aims referred to in paragraph 2 of Article 8 and is, in addition, «necessary in a democratic society» to achieve those aims.[62]

58 Consolidated version of the modernization proposals of Convention 108 with reservations by the ad hoc Committee on data protection of 3 May 2016, CAHDATA(2016)01. Switzerland ratified the Convention No. 108 on 2 October 1997 and its Additional Protocol on 20 December 2007. The Convention entered into force for Switzerland on 1 February 1998 and its Additional Protocol on 1 April 2008.

59 Cf. the speeches and presentations of the Director Jörg Polakiewicz on the 53rd meeting of the Committee of Legal Advisers on Public International Law (CAHDI) of 23 March 2017.

60 Cf. Chapter III.A.5.

61 Cf. also the Opinion 2/13 of the CJEU of 18 December 2014: Accession by the European Union to the ECHR, EU:C:2014:2454, n. 187 *et seqq.,* as to the power of EU member states to lay down higher standards of protection of fundamental rights. Jörg Polakiewicz, Outside, but not that far, Schriften des Europainstitus der Universität des Saarlandes, vol. 4, 2017, pp. 381–406.

62 Cf. ECtHR, *Leander v. Sweden,* Judgment of 26 March 1987, App. No. 9248/81, in which the ECtHR ruled that the storing and the release of personal information contained in a secret police-register was not a violation of the right to respect for private life, since the interference couldn't be said to have been disproportionate to the legitimate aim pursued; in ECtHR, *Amann v. Switzerland,* Judgment of 16 February 2000, App. No. 27798/95, the ECtHR decided that the Public Prosecutor Office's interception and recording of a telephone call received by the applicant from a person at the former Soviet embassy in Berne couldn't be considered to have been «in accordance with the law» since – at that time – Swiss law did not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in this area; in ECtHR, *S. and Marper v. United Kingdom,* Judgment of 4 December 2008, App. Nos. 30562/04 and 30566/04, the ECtHR had to consider whether the retention by the authorities of fingerprints, DNA profiles and cellular samples of persons who were suspected but not convicted of offences constituted a justified interference with their private life and ruled that there was no fair balance between the competing public and private interests in this case and that the United Kingdom had overstepped any acceptable margin of appreciation (para. 125); Harris, O'Boyle, Bates, Buckley, supra n. 20, p. 559.

There is a variety of case law of the ECtHR with reference to the admissibility of access to personal data,[63] the balancing of data protection with the freedom of expression,[64] on challenges in online data protection,[65] correspondence,[66] criminal record databases,[67] GPS data,[68] identity,[69] information concerning professional activities,[70] interception of communication,[71] the obligations for duty bearers,[72] photos,[73] the

63 Cf. ECtHR, *Leander v. Sweden,* supra n. 62; ECtHR, *Gaskin v. United Kingdom,* Judgment of 7 July 1989, App. No. 10454/83; *Odièvre v. France,* Judgment of 13 February 2003 (GC), App. No. 42326/98; ECtHR, *K.H. and Others v. Slovakia,* Judgment of 28 April 2009, App. No. 32881/04; ECtHR, *Godelli v. Italy,* Judgment of 25 September 2012, App. No. 33783/09.

64 ECtHR, *Von Hannover v. Germany,* Judgment of 24 June 2004, App. No. 59320/00; ECtHR, *Axel Springer AG v. Germany,* Judgment of 7 February 2012 (GC), App. No. 39954/08; ECtHR, *Von Hannover v. Germany (No. 2),* Judgment of 7 February 2012 (GC), App. Nos. 40660/08 and 60641/08.

65 ECtHR, *K.U. v. Finland,* Judgment of 2 December 2008, App. No. 2872/02.

66 ECtHR, *Malone v. United Kingdom,* Judgment of 2 August 1984, App. No. 8691/79; ECtHR, *Leander v. Sweden,* supra n. 62; ECtHR, *Gaskin v. United Kingdom,* supra n. 63; ECtHR, *McMichael v. United Kingdom,* Judgment of 24 February 1995, App. No. 16424/90; ECtHR, *Amann v. Switzerland,* supra n. 62; ECtHR, *Rotaru v. Romania,* Judgment of 4 May 2000 (GC), App. No. 28341/95; ECtHR, *M.G. v. United Kingdom,* Judgment of 24 September 2002, App. No. 39393/98; ECtHR, *Turkey v. Slovakia,* Judgment of 14 February 2006, App. No. 57986/00; ECtHR, *Cemalettin Canli v. Turkey,* Judgment of 18 November 2008, App. No. 22427/04; ECtHR, *S. and Marper v. United Kingdom,* supra n. 62; ECtHR, *Haralambie v. Romania,* Judgment of 27 October 2009, App. No. 21737/03; ECtHR, *Dalea v. France,* Judgment of 2 February 2010, App. No. 964/07; ECtHR, *Shimovolos v. Russia,* Judgment of 21 June 2011, App. No. 30194/09; ECtHR, *Khelili v. Switzerland,* Judgment of 18 October 2011, App. No. 16188/07; ECtHR, *Bernh Larsen Holding SA and Others v. Norway,* Judgment of 14 March 2013, App. No. 24117/08.

67 ECtHR, *B.B. v. France,* Judgment of 17 December 2009, App. No. 5335/06; ECtHR, *M.M. v. United Kingdom,* Judgment of 13 November 2012, App. No. 24029/07.

68 ECtHR, *Uzun v. Germany,* Judgment of 2 September 2010, App. No. 35623/05.

69 ECtHR, *Odièvre v. France,* supra n. 63; ECtHR, *Ciubotaru v. Modova,* Judgment of 27 April 2010, App. No. 27138/04; ECtHR, *Godelli v. Italy,* Judgment of 25 September 2012, App. No. 33783/09.

70 ECtHR, *Niemietz v. Germany,* Judgment of 16 December 1992, App. No. 13710/88; ECtHR, *Michaud v. France,* Judgment of 6 December 2012, App. No. 12323/11.

71 ECtHR, *Malone v. United Kingdom,* supra n. 66; ECtHR, *Kruslin v. France,* Judgment of 24 April 1990, App. No. 11801/85; ECtHR, *Halford v. United Kingdom,* Judgment of 25 June 1997, App. No. 20605/92; ECtHR, *Lambert v. France,* Judgment of 24 August 1998, App. No. 23618; ECtHR, *Amann v. Switzerland,* supra n. 62; ECtHR, *Cotlet v. Romania,* Judgment of 3 June 2003, App. No. 38565; ECtHR, *Copland v. United Kingdom,* Judgment of 3 April 2007, App. No. 62617/00; ECtHR, *Liberty and Others v. United Kingdom,* Judgment of 1 July 2008, App. No. 58243; ECtHR, *Szuluk v. United Kingdom,* Judgment of 2 June 2009, App. No. 36936/05.

72 ECtHR, *I. v. Finland,* Judgment of 17 July 2008, App. No. 20511/03; ECtHR, *B.B. v. France,* supra n. 67; ECtHR, *Mosley v. United Kingdom,* Judgment of 10 May 2011, App. No. 48009/08.

73 ECtHR, *Von Hannover v. Germany,* supra n. 64; ECtHR, *Sciacca v. Italy,* Judgment of 11 January 2005, App. No. 50774/99.

right to be forgotten,[74] the right to object,[75] sensitive categories of data,[76] surveillance methods,[77] video surveillance[78] and voice samples.[79] Furthermore, the ECtHR has ruled that the right to access to personal data can be derived from the right to respect for private life and it recognized the interest of a person to obtain information on his origins.[80]

As to DNA samples, the ECtHR expressed in its judgment *Van der Velden*[81] the view that cellular material went beyond the scope of identifying features like fingerprints and that given the use such material could have in the future, its systematic retention was sufficiently intrusive to constitute an interference with Article 8 ECHR. In the *Marper* case,[82] which concerned the retention of fingerprints, DNA samples and profiles of individuals suspected of wrongdoing but not convicted of any offence,[83] the Grand Chamber of the ECtHR unanimously held that the «blanket and indiscriminate» nature of the retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences failed to strike a fair balance between the competing public and private interests involved and constituted therefore a disproportionate interference with the applicants' right to respect for private life.[84]

74 ECtHR, *Segerstedt-Wiberg and Others v. Sweden,* Judgment of 6 June 2006, App. No. 62332/00.

75 ECtHR, *Leander v. Sweden,* supra n. 62; ECtHR, *M.S. v. Sweden,* Judgment of 27 August 1997, App. No. 20837/92; ECtHR, *Rotaru v. Romania,* supra n. 66; ECtHR, *Mosley v. United Kingdom,* supra n. 72.

76 ECtHR, *I. v. Finland,* supra n. 72; ECtHR, *S. and Marper v. United Kingdom,* supra n. 62; ECtHR, *Michaud v. France,* supra n. 70.

77 ECtHR, *Klass and Others v. Germany,* Judgment of 6 September 1978, App. No. 5029/71; ECtHR, *Rotaru v. Romania,* supra n. 66; ECtHR, *Taylor-Sabori v. United Kingdom,* Judgment of 22 October 2002, App. No. 47114/99; ECtHR, *Allan v. United Kingdom,* Judgment of 5 November 2002, App. No. 48539/99; ECtHR, *Vetter v. France,* Judgment of 31 May 2005, App. No. 59842/00; ECtHR, *Bykov v. Russia,* Judgment of 10 March 2009 (GC), App. No. 4378/02; ECtHR, *Kennedy v. United Kingdom,* Judgment of 18 May 2010, App. No. 26839/05; ECtHR, *Uzun v. Germany,* supra n. 68; ECtHR, *Association «21 Décembre 1989» and Others v. Romania,* Judgment of 24 May 2011, App. Nos. 33810/07 and 18817/08; ECtHR, *Sher and others v. United Kingdom,* Judgment of 20 October 2015, App. No. 5201/11; ECtHR, *Zakharov v. Russia,* supra n. 55; ECtHR, *Szabó and Vissy v. Hungary,* supra n. 55 as to a legislation on secret anti-terrorist surveillance.

78 ECtHR, *Peck v. United Kingdom,* Judgment of 28 January 2003, App. No. 44647/98; ECtHR, *Köpke v. Germany,* Judgment of 5 October 2010, App. No. 420/07.

79 ECtHR, *P.G. and J.H. v. United Kingdom,* Judgment of 25 September 2001, App. No. 44787/98; ECtHR, *Wisse v. France,* Judgment of 20 December 2005, App. No. 71611/01.

80 ECtHR, *Gaskin v. United Kingdom,* supra n. 63; ECtHR, *Odièvre v. France,* supra n. 63.

81 ECtHR, *Van der Velden v. Netherlands,* Judgment of 7 December 2006, App. No. 29514/05.

82 ECtHR, *S. and Marper v. United Kingdom,* supra n. 62.

83 As to the privacy rights and the retention of DNA profiles of persons suspected, but not convicted of a criminal offence on a national database, cf. Hilary Biehler, The Right to Privacy and the Retention of DNA Profiles: Getting the Balance Right, 19 Eur. H. Rts. L. Rev. (2014), pp. 479–489, pp. 482 *et seqq.*

84 ECtHR, *S. and Marper v. United Kingdom,* supra n. 62, para. 101.

In the case *Z. v. Finland,*[85] the applicant complained that her medical record,[86] including details of her HIV status, had been disclosed and published during a criminal trial. The ECtHR accepted that the interest in protecting the confidentiality of medical data can be outweighed by the interest in investigating and prosecuting a crime. On the other hand, it found that making medical data accessible to the public and publishing the applicant's identity and medical condition in the Court of Appeal's judgment was not justified and, therefore, gave rise to a violation of Article 8 ECHR.

In the case of *G.S.B.,*[87] which concerned the transmission of the applicant's bank account details to the U.S. tax authorities in connection with an administrative cooperation agreement between Switzerland and the United States,[88] the Court accepted that Switzerland had a major interest in acceding to the U.S. request for administrative cooperation in order to enable the U.S. authorities to identify any assets which might have been concealed in Switzerland. Furthermore, it was recognized that the U.S. tax authorities' allegations against Swiss banks were liable to jeopardize the very survival of the applicant bank, a major employer and player in the Swiss economy.[89] Given Switzerland's interest in finding an effective legal solution in cooperation with the United States, it pursued – so the Court – a legitimate aim within the meaning of Article 8 paragraph 2 of the ECHR.[90]

4. Data Protection Under the Aegis of the EU

At the end of 1990, the European Commission seemed concerned that a lack of consistency in data protection across its member states could hamper the development of the internal market in a range of areas. It therefore submitted a proposal for a directive in order to harmonize the national laws on data protection in the private and most parts of the public sector.[91]

85 ECtHR, *Z. v. Finland,* Judgment of 25 February 1997, App. No. 22009/93.

86 Cf. as to health data also ECtHR, *M.S. v. Sweden,* supra n. 75; ECtHR, *L.L. v. France,* Judgment of 10 October 2006, App. No. 7508/02; ECtHR, *I. v. Finland,* supra n. 72; ECtHR, *Biriuk v. Lithuania,* Judgment of 25 November 2008, App. No. 23373/03; ECtHR, *Szuluk v. United Kingdom,* supra n. 71.

87 ECtHR, *G.S.B. v. Switzerland,* Judgment of 22 December 2015, App. No. 28601/11.

88 Cf. also ECtHR, *M.N. and others v. San Marino,* Judgment of 7 July 2015, App. No. 28005/12, in which the Court established that information retrieved from banking documents «undoubtedly» amounted to personal data concerning an individual – and were therefore protected by Article 8 ECHR – irrespectively of it being sensitive information or not (para. 51–55).

89 ECtHR, *G.S.B. v. Switzerland,* supra n. 87, para. 83.

90 ECtHR, *G.S.B. v. Switzerland,* supra n. 87, para. 92.

91 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) dated 25 January 2012 COM(2012) 11 final, p. 18.

5. Legislative and Political Instruments on Data Protection

The original treaties of the European Communities did not contain any reference to human rights or their protection. In 1995, after four years of negotiation, the EU set a milestone in the history of personal data protection by adopting the Data Protection Directive 95/46/EC.[92] As the aim of adopting the Data Protection Directive was harmonization of data protection law on the national level, the directive affords a degree of specificity comparable to that of the (then) existing national data protection laws. For the Court of Justice of the EU (CJEU), «Directive 95/46 is intended (...) to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all member states».[93] Consequently, the EU member states had only limited freedom to maneuver when implementing the Directive. The Directive encompassed all key elements of Article 8 ECHR. It was based on the 1980 Organization for Economic Co-operation and Development (OECD) «Recommendations of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data»,[94] which, although not-binding, have also been very influential, particularly in countries outside Europe such as the United States, Canada, Australia and Japan. All EU member states have transposed the Directive into national law, including the new member states, as well as the non-EU member states that are part of the European Economic Area (EEA),[95] namely Iceland, Liechtenstein and Norway, and Switzerland with regard to its bilateral and sectorial treaties with the EU. Moreover, the Commission found itself compelled to launch legal actions for improper implementation of the Directive. The first legal action after the adoption of the Directive was directed against Germany and led to a ruling by the CJEU in March 2010[96] stating that the requirement of a «complete independence» for a supervisory authority means that it should be free from any external influence.[97]

92 Data Protection Directive 95/46/EC, OJ L 281, 23 November 1995, p. 31.

93 CJEU, joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* Judgment of 24 November 2011, EU:C:2011:777, para. 28–29.

94 OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data of 23 September 1980, C(80)58/FINAL, which have been amended on 11 July 2013, C(2013)79.

95 Agreement on the European Economic Area, OJ L 1, 3 January 1994, p. 3, which entered into force on 1 January 1994. Cf. the Decision of the EEA joint Committee No 144/2017 of 7 July 2017 amending Annex XI (Electronic communication, audiovisual services and information society) to the EEA Agreement with regard to the incorporation of the EU-U.S. Privacy Shield into the EEA Agreement.

96 CJEU, C-518/07, *Commission supported by European Data Protection Supervisor v. Federal Republic of Germany,* Judgment of 9 March 2010, EU:C:2010:125.

97 CJEU, C-518/07, *Commission v. Germany,* supra n. 96, at para. 30; Cf. also CJEU, C-614/10, *Commission v. Austria,* Judgment of 16 October 2012, EU:C:2012:631 and CJEU, C-288/12, *Commission v. Hungary,* Judgment of 8 April 2014, EU:C:2014:237.

Besides the Directive 95/46/EC and other regulations,[98] the EU Charter is one of the most significant instruments for data protection in Europe. The EU Charter not only guarantees respect for private and family life in Article 7, but also establishes the right to data protection in Article 8, explicitly raising the level of protection to that of a fundamental right in EU law. The EU Charter, which has been integrated into the Lisbon Treaty, has a legally binding effect on the institutions and bodies of the EU, and on the member states when implementing EU law. Consequently, EU institutions, as well as member states, must observe and guarantee this right, which also applies to member states when implementing Union law.[99] Formulated several years after the Data Protection Directive, Article 8 of the EU Charter must be understood as embodying pre-existing EU data protection law. The EU Charter, therefore, not only explicitly mentions a right to data protection in Article 8 paragraph 1, but also refers to key data protection principles in paragraph 2 of the norm. Finally, paragraph 3 ensures that an independent authority will control the implementation of these principles.[100]

98 Cf. also Regulation (EU) No 603/2013 of the European Parliament and the Council of 26 June 2013 on the establishment of «Eurodac» for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29 June 2013, p. 1; cf. also Articles 28 *et seqq.* of the Regulation (EU) No. 794/2016 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24 May 2016, p. 53.

99 Cf. Article 51 of the EU Charter. To the scope of application of the EU Charter, cf. CJEU, C-617/10, *Åklagaren v. Hans Åkerberg Fransson,* Judgment of 26 February 2013, EU:C:2013:105.

100 Before the enforcement of the Lisbon Treaty on 1 December 2009, the legislation concerning data protection in the area of freedom, security and justice (AFSJ) was divided between the first pillar (data protection for private and commercial purposes, with the use of the supranational community method) and the third pillar (data protection for law enforcement purposes, at traditional intergovernmental level). As the pillar structure disappeared with the Lisbon Treaty, the development of a clearer and more effective data protection system gained a stronger basis. Nevertheless, the old pillar structure is still visible in different legislative instruments which are still in force. Besides the above-mentioned Directive 95/46/EC on data protection, the most significant of the former first-pillar instruments are Directive 2002/58/EC on e-privacy (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [Directive on privacy and electronic communications], OJ L 201, 31 July 2002, p. 37), which was modified in 2009, Directive 2006/24/EC on data retention (Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54, 13 April 2006, p. 54) which was declared invalid by the Court of Justice on 8 April 2014, and Regulation (EC) No. 45/2001 on processing of personal data by Community institutions and bodies. A former third-pil-

On 25 January 2012, the European Commission proposed a comprehensive and wide-ranging review of the EU's 1995 data protection rules to strengthen online privacy rights. This was due to rapid technological developments and new challenges for data protection through social networking sites, cloud computing, location-based services and smart cards, all consequences of globalization, as well as the result of the current fragmentation of data protection in the different member states of the EU. The proposals presented by the European Commission consisted of two main changes:

(1) a new General Data Protection Regulation to supersede Directive 95/46/EC, in order to modernize the principles enshrined in the Directive and for the private sector and most of the public sector in the member states,[101] and
(2) a new Directive[102] to replace the Council Framework Decision 2008/977/JHA for the area of criminal law enforcement.[103]

lar instrument which is noteworthy is the Council Framework Decision of November 2008 on the protection of personal data processed in the framework of police and criminal justice, a sector not covered by the Directive 95/46/EC. The Framework decision only applies to police and judicial exchange among member states, EU authorities and associated systems, excluding domestic data. Moreover, Article 16 of the Treaty on the Functioning of the European Union (TFEU) provides that everyone has the right to the protection of personal data concerning them. It also states that the Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the member states when carrying out activities that fall within the scope of EU law. Finally, in December 2009, the European Council approved a new multi-annual program regarding the AFSJ for the period of 2010 to 2014: the so-called Stockholm Program which was followed by two communications of the Commission adopted on 11 March 2014 to set out political priorities for the post-Stockholm Program. Shortly after, on 2 April 2014, the Parliament adopted a resolution on the mid-term review of the Stockholm Program, whilst the European Council defined in its conclusions of 26–27 June 2014 the strategic guidelines for legislative and operational planning for the coming years within the AFSJ pursuant to Article 68 TFEU. One of the key objectives was a better protection of personal data in the EU.

101 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of 25 January 2012, COM(2012) 11 final.

102 Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data of 25 January 2012, COM(2012) 10 final.

103 Cf. also Federico Ferretti, Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?, 51 Common Market Law Review (2014), pp. 843–868, pp. 851 *et seqq.* In the light of the Snowden revelations in 2013, the 7th hearing of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) Inquiry on Mass Surveillance of EU Citizens took place on 14 October 2013 in Brussels. The inquiry was mandated by the European Parliament Resolution of 4 July 2013 on the U.S. National Security Agency (NSA) surveillance program, surveillance bodies in various member states and their impact on EU citizens' privacy, 2013/2682(RSP). The resolution, *inter alia,* instructed LIBE «to conduct an in-depth inquiry into the matter in collaboration with national parliaments and the EU–U.S. expert group set up by the

The new Regulation[104] entered into force on 24 May 2016 and shall apply from 25 May 2018. The new Directive[105] entered into force on 5 May 2016 and EU member states have to transpose it into their national law by 6 May 2018. The main changes are the following:

(1) an expanded territorial reach, catching data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behavior (within the EU) of, EU data subjects;
(2) accountability and privacy by design, placing accountability obligations on data controllers to demonstrate compliance;
(3) Data Protection Officers as part of the accountability program of data controllers and processors;
(4) direct obligations for data processors, which include an obligation to maintain a written record of processing activities carried out on behalf of each controller, designate a data protection officer where required, appoint a representative (when not established in the EU) in certain circumstances and notify the controller on becoming aware of a personal data breach without undue delay.

The new rules mean that the new EU Regulation and Directive will not only be applicable for companies based in the EU (or their subsidiaries in the EU), but also for third country-based companies that are offering goods or services to EU data subjects. Although there are still a number of open questions along the way, it is certain that numerous U.S. or Swiss organizations that have no local presence in the EU will also be in scope of the EU legislation.

Historically, the Swiss and the EU data protection legislations are closely tied. This is mainly due to the mechanism developed by the EU to provide for legal certainty as to the transfer of personal data to a third country from the EU. According to Article 25(6) of the Directive 95/46/EC, the European Commission may determine – and EU member states are bound by such decision – that a third country

Commission and to report back» by the end of the year. The focus of the 7th hearing was «on the question of whether the alleged surveillance activities would, if confirmed, be in violation of the law, whether at international, Council of Europe, EU or national level».

104 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, p. 1.

105 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, p. 89.

ensures an adequate level of protection of personal data transferred from the EU («Commission adequacy finding»). On 26 July 2000, the Commission issued Decision 2000/518/EC stating that for all the activities falling within the scope of the Directive, Switzerland was considered as providing an adequate level of protection.[106] Hence the draft of a revised Swiss Data Protection Act was based in due consideration of the EU data protection regulation. According to the envisaged timeline, the revised Swiss Data Protection Act should be enacted around the same period as the EU legislation, in 2018.[107]

6. Judgments by the Court of Justice of the EU

In the last years, the Court of Justice of the EU has had the chance to rule over data protection issues on several occasions: In a multitude of cases, the Court was able to work out the concept of personal data,[108] establish rules for the processing of personal data[109] and work out criteria for making data processing legitimate.[110]

In the case of *Lindqvist,*[111] the Court had to rule on the publication of personal data on the internet and define the transfer of personal data to third countries. Additionally, the Court had to establish rules on various aspects of data protection: The

106 OJ L 215, 25 August 2000, p. 1.

107 Bruno Baeriswyl, Auf dem Weg zu einem neuen DSG, digma 2017, p. 4 *et seqq.;* Sandra Husi-Stämpfli, DSG-Revision: Schritt in die richtige Richtung, digma 2017, p. 50 *et seqq.;* David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter, 20 February 2017, p. 42; Beat Rudin, Anpassungsbedarf in den Kantonen, digma 2017, p. 58 *et seqq.*

108 CJEU, C-342/12, *Worten,* Judgment of 30 May 2013, EU:C:2013:355; CJEU, C-141/12 and C-372/12, *YS and Others,* Judgment of 17 July 2014, EU:C:2014:2081.

109 CJEU, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy,* Judgment of 16 December 2008, EU:C:2008:727; CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer Netherlands,* Judgment of 7 May 2009, EU:C:2009:293; CJEU, C-518/07, *Commission v. Germany,* supra n. 96; CJEU, C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen,* Judgment of 9 November 2010, EU:C:2010:662; CJEU, C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito and Federación de Comercio Electrónico y Marketing Directo v. Administración del Estado,* supra n. 93; CJEU, T-190/10, *Egan and Hackett v. Parliament,* Judgment of 28 March 2012, EU:T:2012:165; CJEU, C-614/10, *Commission v. Austria,* supra n. 97; CJEU, C-119/12, *Josef Probst v. mr.nexnet GmbH,* Judgment of 22 November 2012, EU:C:2012:748; CJEU, C-342/12, *Worten,* supra n. 108; CJEU, C-473/12, *IPI,* Judgment of 7 November 2013, EU:C:2013:715; CJEU, C-486/12, *X,* Judgment of 12 December 2013, EU:C:2013:836; CJEU, C-288/12, *Commission v. Hungary,* supra n. 97; CJEU, C-683/13, *Pharmacontinente – Saúde e Higiene and Others,* order of 19 June 2014, EU:C:2014:2028.

110 CJEU, C-342/12, *Worten,* supra n. 108; CJEU, C-683/13, *Pharmacontinente – Saúde e Higiene and Others,* supra n. 109.

111 CJEU, C-101/01, *Lindqvist,* Judgment of 6 November 2003, EU:C:2014:2028.

processing of data by the internet[112] and by internet service providers,[113] by publicly available electronic communication services,[114] the rights to access of a data subject[115] and to access to documents,[116] the obligation to inform a subject of the processing of his data[117] and on the retention,[118] disclosure and erasure of personal data.[119] A number of cases raised data protection issues associated with rights enshrined in the EU Charter.[120] Moreover, the Court ruled on several actions for failure of member states to fulfill their treaty obligations in connection with data protection issues,[121] and on further data protection issues arising from other specific areas of the treaties, such as

112 CJEU, C-461/10, *Bonnier Audio AB, Earbooks AB, norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB,* Judgment of 19 April 2012, EU:C:2012:219.

113 CJEU, C-275/06, *Productores de Musica de España (Promusicae) v. Telefonica de España SAU,* Judgment of 29 January 2008, EU:C:2008:54; CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL,* Judgment of 24 November 2011, EU:C:2011:771.

114 CJEU, C-293/12 and C-594/12*, Digital Rights Ireland, Seitlinger and Others,* Judgment of 8 April 2014, EU:C:2014:238.

115 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer Netherlands,* supra n. 109; CJEU, T-190/10, *Egan and Hackett v. Parliament,* supra n. 109; CJEU, C-486/12, *X,* supra n. 109; CJEU, C-141/12 and C-372/12, *YS and Others,* supra n. 108; cf. the Opinion of Advocate General Kokott on CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner,* delivered on 20 July 2017, EU:C:2017:582, on the question whether an examination script may constitute personal data.

116 CJEU, C-28/08 P, *Commission v. The Bavarian Lager Co. Ltd, European Data Protection Supervisor,* Judgment of 29 June 2010, EU:C:2010:378; CJEU, T-82/09, *Dennekamp v. Parliament,* Judgment of 23 November 2011, EU:T:2011:688; General Court, T-214/11, *ClientEarth and PAN Europe v. EFSA (on appeal),* Judgment of 13 September 2013, EU:T:2013:483.

117 CJEU, C-473/12, *IPI,* supra n. 109.

118 CJEU, C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger and Others,* supra n. 114; CJEU, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Postoch telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others,* Judgment of 21 December 2016, EU:C:2016:970.

119 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer Netherlands,* supra n. 109.

120 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Germany,* Judgment of 16 December 2008, EU:C:-2008:724; CJEU, C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen,* supra n. 109; CJEU, C-291/12, *Schwarz,* Judgment of 17 October 2013, EU:C:2013:670; CJEU, C-293/12 and C-594/12*, Digital Rights Ireland, Seitlinger and Others,* supra n. 114.

121 CJEU, C-518/07, *Commission v. Germany,* supra n. 96; CJEU, C-28/08 P, *Commission v. The Bavarian Lager Co. Ltd, European Data Protection Supervisor,* supra n. 116; CJEU, C-614/10, *Commission v. Austria,* supra n. 97; CJEU, C-270/11, *Commission v. Sweden,* Judgment of 30 May 2013, EU:C:2013:339; CJEU, C-288/12, *Commission v. Hungary,* supra n. 97.

the transfer of medical data,[122] the publication of information on beneficiaries of agricultural aid[123] and on the activities of the European Anti-Fraud Office.[124]

In the case of *European Parliament v. Council of the European Union,*[125] the Court annulled the Council's decision concerning the conclusion of an agreement between the European Community and the United States on the processing and transfer to the U.S. Bureau of Customs and Border Protection of personal passenger name records data and the Commission's decision on the adequate protection of those data.

In the case *Rechnungshof,*[126] the Court had to rule on the protection of individuals regarding the processing of personal data under the Directive 95/46/EC with regard to the disclosure of data on the income of employees of institutions subject to control by the Rechnungshof.

In the case of *Google Spain,*[127] the Court ruled on the material and territorial scope of data protection concerning internet search engines, the processing of data contained on websites and the searching for, indexing and storage of such data. Also, the Court had to decide on the responsibility of the operator of said engine.

The decision in the case of *Schrems,*[128] which provided a multitude of topics for discussion, will be outlined below.

122 European Union Civil Service Tribunal, F-46/09, action under Articles 236 EC and 152 EA, *Candidate for a post as a member of the contract staff at the European Parliament v. European Parliament,* Judgment of 5 July 2011, EU:F:2011:101.

123 CJEU, C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen,* supra n. 109.

124 Court of first Instance, T-259/03, *Nikolaou v. Commission,* Judgment of 12 September 2007, EU:T:2007:254.

125 CJEU, joined cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union,* Judgment of 30 May 2006, EU:C:2006:346. The Court ruled that the transfer of passenger name records data constituted «processing operations concerning public security and the activities of the State in areas of criminal law». This trespassed the limits of Article 3(2) of the Data Protection Directive, which specifically excludes the processing of data relating to activities provided for under the second and third pillars.

126 CJEU, joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and between Christa Neukomm, Joseph Lauermann and Österreichischer Rundfunk,* Judgment of 20 May 2003, EU:C:2003:294.

127 CJEU, C-131/12, *Google Spain,* Judgment of 13 May 2014, EU:C:2014:317; cf. Julie Dupont-Lassalle, Beaucoup de bruit pour rien?, La précarité du «droit à l'oubli numérique» consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain, 26 Revue trimestrielle des droits de l'homme (2015), pp. 987–1019, pp. 994 *et seqq.*

128 CJEU, C-362/14, *Schrems v. Data Protection Commissioner,* Judgment of 6 October 2015, EU:C:2015:650. Cf. BGer 1B_185/2016, 1B_186/2016, 1B_188/2016 (16 November 2016), as to Facebook Switzerland.

B. U.S. Legal System on Data Protection

Unlike European jurisdictions, the United States does not have a dedicated data protection law.[129] The right to privacy in the United States protects only against the federal government's intrusion into an individual's private affairs. Hence, the legislation specific to the issue of personal data protection is limited to data processed by and in custody of the federal government. In the private sector, data protection is primarily regulated by industry, on a sector-by-sector basis with numerous sources of privacy law.[130] Therefore, industries in the United States are mostly self-regulated, including most private corporations, data-mining businesses, personal data repositories and internet-based social-networking sites, although there are multiple privacy laws at the state level.[131]

1. Constitutional Level

In the U.S. legal system, the main source serving as a basis for data protection guarantee on a constitutional level is the Fourth Amendment.[132] It guarantees the «right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures», which is understood to encompass certain data attributed to a person, such as telephone or banking records.[133] Nevertheless, these guarantees only apply if the individual had a «legitimate expectation of privacy»,[134] which excludes all cases where an individual has voluntarily turned over the information in question to a third party. This broad exemption has been scrutinized lately by the courts considering the changing electronic and technical environment: In the case of *ACLU v. Clapper*[135] it was recognized that «surveillance capabilities are vast» and that «it is difficult if not impossible to avoid exposing a wealth of information about oneself to those surveillance», and hence lose the «legitimate expectation of privacy».[136]

129 Cf. McKay Cunningham, Complying with international data protection law, University of Cincinnati Law Review, vol. 2, No. 84, 20 June 2015, pp. 2 *et seq.*

130 Cf. Jacqueline Klosek, Data protection in the information age, Westport 2000, pp. 130 *et seqq.*

131 Cf. Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards, 25 Yale J. Int'l L. (2000), p. 27 *et seqq.* with further references.

132 Cf. Ian Brown, Keeping Our Secrets?, Designing Internet Technologies for the Public Good, 19 Eur. H. Rts. L. Rev. (2014), pp. 369–377, p. 375.

133 U.S. Supreme Court, *Smith v. Maryland,* 20 June 1979, 442 U.S. 735 (1979), and U.S. Supreme Court, *United States v. Miller,* 21 April 1976, 425 U.S. 435 (1976).

134 U.S. Supreme Court, *Katz v. United States,* Judgment of 18 December 1967, 389 U.S. 347 (1967).

135 U.S. Court of Appeals for the second circuit, *ACLU v. Clapper,* Judgment of 7 May 2015, No. 14–42.

136 Cf. also U.S. Court of Appeals for the second circuit, *United States v. Stavros M. Ganias,* No. 12–240 (2d Cir. 17 June 2014), as the Fourth Amendment has been applied to create a potential «right to deletion» of outdated data held by U.S. law enforcement agencies.

2. Privacy Act of 1974

Amongst the U.S. laws, the Privacy Act of 1974[137] is the closest analogue to a European data protection law. It seeks to comprehensively regulate personal data processing, even if only with respect to federal government departments and agencies. It regulates the collection, use, and disclosure of all types of personal information, by all types of federal agencies, including law enforcement agencies. The Privacy Act contains most of the elements of the EU right to personal data protection, yet only on a very general level. Nevertheless, its guaranties apply only to information contained within a «system of records,» which is defined by the statute and the courts as only including a system from which the government agency retrieves information based on a personal identifier, like a name or social security number.[138] The Privacy Act requires transparency in personal data processing: When information is collected from individuals, they must be told of the nature of the governmental[139] and personal information stored by government agencies and whether it is used to make determinations about individuals. This information has to be maintained with «such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination».[140] As for proportionality, the Privacy Act requires that the agency «maintains in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President».[141] Moreover, special protection is afforded to the sensitive data category of information on how individuals exercise their freedom of expression and association. Nevertheless, the protection of this sensitive data category of the First Amendment responsibilities does not apply to «an authorized law enforcement activity».[142] Finally, the Privacy Act gives individuals the right of access to their records and the right to request correction of «any portion thereof which the individual believes is not accurate, relevant, timely or complete».[143] Legal oversight under the Privacy Act is conducted largely by private litigants and the courts: The Privacy Act gives individuals the right to sue the government for violations of their Privacy Act rights and to obtain damages or injunctive relief.[144]

137 Privacy Act of 1974, 5 U.S.C. para. 552a.
138 Cf. *e.g.* U.S. Court of Appeals, District of Columbia Circuit, *Henke v. U.S. Department of Commerce,* Judgment of 17 May 1996, 83 F.3d 1453 (D.C. Cir. 1996).
139 Cf. 5 U.S.C. para. 552a(e)(3).
140 Cf. 5 U.S.C. para. 552a(e)(5).
141 Cf. 5 U.S.C. para. 552a(e)(1).
142 Cf. 5 U.S.C. para.552a(e)(7).
143 Cf. 5 U.S.C. para. 552a(d).
144 Cf. 5 U.S.C. para. 552a(g).

3. Computer Matching and Privacy Protection Act

The Computer Matching and Privacy Protection Act of 1988[145] complements the Privacy Act by describing the way computer matching involving federal agencies could be performed and by adding certain protections for individuals applying for and receiving federal benefits. The Act adds procedural requirements for agencies to follow when engaging in computer-matching activities, providing matching subjects with opportunities to receive notice and refuting adverse information before having a benefit denied or terminated. It also requires that agencies engaged in matching activities establish Data Protection Boards to oversee those activities. Subsequently, the U.S. Congress enacted the Computer Matching and Privacy Protection Amendments of 1990,[146] which further clarified the due process provisions.

4. Legislative Initiatives

On 21 October 2015, the U.S. House of Representatives passed the draft Judicial Redress Act of 2015, which aims to mitigate a main procedural shortcoming of the Privacy Act of 1974, namely its non-applicability to non-U.S. citizens or residents. It authorizes the U.S. Department of Justice (DoJ) to designate foreign countries or regional economic integration organizations, whose natural citizens will then be allowed to bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records maintained by an agency. The entry into force of the Judicial Redress Act also paved the way for the signature of the EU-U.S. Data Protection Umbrella Agreement.[147] Whilst a step in the right direction, the Redress Act still lags significantly behind granting equal rights to U.S. and EU citizens under the U.S. legislation.

5. Privacy Rights and Surveillance Activities by U.S. Authorities

The Snowden revelations have shown that it is common practice in the United States for corporations established, controlled by or active in the United States to be ordered by the U.S. authorities to produce data from servers they own or operate in other countries. Furthermore, the U.S. authorities can order the corporations to not inform either the authorities in the countries from which they pull the data, the en-

145 Pub. L. No 100-503.

146 Pub. L. No 101-508.

147 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 10 December 2016, p. 3; cf. Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama; Brussels, 24 February 2016.

tities whose data they are handing over, or the data subjects of such data disclosures.[148] The surveillance of communications in the interest of protecting national security, conducted by the U.S. National Security Agency (NSA) both within and outside the United States, especially through the bulk phone metadata surveillance program[149] and, in particular, surveillance under the Foreign Intelligence Surveillance Act (FISA),[150] have a clear impact on an individual's right to privacy. The judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) were largely kept secret, thus not allowing affected persons to know the law with sufficient precision.[151] The current oversight system of the NSA's activities fails to effectively protect the rights of the persons affected;[152] as a matter of fact, persons affected have no access to effective remedies in case of abuse.[153]

The increasing level of surveillance by arms of the state is also the subject of growing concern in the United States. In the decision *U.S. v. Jones,* the U.S. Supreme Court acknowledged that «the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse».[154] This view has been confirmed in the more recent decision *Riley v. California,*[155] in which it was held that the police forces may not, in general, search for digital information on a mobile phone seized from an arrestee without a warrant.

148 Cf. Ian Brown & Douwe Korff, Foreign Surveillance: Law and Practice in a Global Digital Environment, 3 Eur. H. Rts. L. Rev, (2014), pp. 243–251, p. 249.

149 Section 215 of the U.S. Patriot Act.

150 Section 702 of the Foreign Intelligence Surveillance Act (FISA).

151 In order to justify such methods, the United States have repeatedly taken the position that Article 17 ICCPR, which determines that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation, does not apply with respect to individuals under its jurisdiction, but outside its territory. This interpretation of the ICCPR is in contrast with the interpretation of Article 2, para. 1 ICCPR supported by the Human Rights Committee's established jurisprudence, the jurisprudence of the International Court of Justice and state practice; cf. Human Rights Committee, Concluding Observations on the Fourth Report of the United States of America, adopted by the Committee at its 110th session, 10–28 March 2014, advanced unedited version, para. 4.

152 Cf. Presidential Policy Directive/PPD-28, which extends some safeguards to non-U.S. citizens «to the maximum extent feasible consistent with the national security» with only limited protection against excessive surveillance.

153 Human Rights Committee, supra n. 151, para. 22. A further example of the U.S. cross-border data gathering is the inception of the Foreign Account Tax Compliance Act (FATCA) in 2010, which requires large-scale data transfers concerning U.S. citizens holding accounts in foreign countries to the U.S. tax authorities. This has been criticized as not compatible with the level of European data protection; cf. 19th annual report of the Swiss Federal Data Protection Commissioner 2011/2012, para. 1.9.1., p. 88.

154 U.S. Supreme Court, *U.S. v. Jones,* 132 S. Ct. 945, Judgment of 23 January 2012.

155 U.S. Supreme Court, *Riley v. California,* 134 S. Ct. 2473, Judgment of 25 June 2014.

C. Data Transfers from Europe to the United States

1. Cross-border Data Flows Between Europe and the United States

In Europe, the legal frameworks for trans-border data protection flows are the ECHR,[156] Convention 108[157] and Directive 2016/680,[158] while the Organization of American States (OAS) has set policy options for member states including guidelines on trans-border data protection.[159] In the wake of 9/11, the United States has sought to conclude agreements with other states and regional bodies to facilitate sharing of personal data for law enforcement purposes. In particular, the EU and the United States have concluded agreements covering the transfer of Passenger Name Record (PNR) data of airline passengers[160] and financial messaging data (SWIFT).[161] In the private sector, the regulatory mechanism with regard to trans-border data flows between the EU and the United States as well as with Switzerland[162] were directed by the «Safe Harbor» agreement.

2. The Fallen Concept of a «Safe Harbor»

With its Decision 2000/520, the European Commission decided in 2000 that the EU concept of «Safe Harbor» provided a legitimate basis for transferring personal data from the EU to recipients in the United States who have submitted themselves to the framework. U.S. companies could self-certify themselves under U.S. law that they will comply with the data processing principles defined by the framework. Many

156 Article 8.

157 Article 12 (1).

158 Article 35 *et seqq.*

159 Permanent Council of the OAS, Committee on Juridical and Political Affairs, Preliminary Principles and Recommendations on Data Protection, CP/CAJP-2921/10, 17 October 2011, principle No 8.

160 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the U.S. Department of Homeland Security of 11 August 2012, OJ L 215, 11 August 2012, p. 5. See also Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Cf. Opinion of Advocate General Paolo Mengozzi in the Request for an Opinion 1/15 by the CJEU delivered on 8 September 2016, EU:C:-2016:656; Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 2011/C 181/02 of 22 June 2011.

161 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program of 27 July 2010, OJ L 8, 13 January 2010, p. 11.

162 U.S.-Swiss Safe Harbor Privacy principles issued by the U.S. Department of Commerce on 16 February 2009, CC 0.235.233.6.

EU companies relied on the «Safe Harbor» privacy framework in order to transfer personal data to the United States.

With its judgment of 6 October 2015, the Court of Justice of the EU put a sudden end to the applicability of the «Safe Harbor» agreement. Subject of the procedure in the *Schrems* case was whether U.S. law and practice ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46.[163] The Court elaborated that it was incumbent upon the Commission, after it had adopted a decision pursuant to Article 25 paragraph 6 of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question was still factually and legally justified. Such a check – so the Court – is required, in any event, when evidence gives rise to doubt in that regard.[164]

The Court found that the Commission's Decision 2000/520 did not refer either to the existence in the United States of rules intended to limit any interference, or to effective legal protection against the interference.[165] According to the Court's settled case-law, the EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the EU Charter must lay down clear and precise rules governing the scope and application of a measure. The legislation must also contain minimum safeguards, so that the persons whose personal data is concerned have sufficient guaranties enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of it.[166] Therefore, the Court emphasized that legislation has to be limited to what is strictly necessary when it authorizes storage of all the personal data of all the persons whose data has been transferred from the EU to the United States. There shall be no differentiation, limitation or

163 CJEU, C-362/14, *Schrems,* supra n. 128, para. 67. In this Opinion delivered on 23 September 2015 Advocate General Yves Bot took the view that the existence of a decision by the Commission finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the national supervisory authorities' powers under the directive on the processing of personal data. According to the Advocate General, where systemic deficiencies are found in the third country to which the personal data is transferred, the member states must be able to take the measures necessary to safeguard the fundamental rights protected by the Charter of Fundamental Rights of the EU, which include the right to respect for private and family life and the right to the protection of personal data. The Advocate General considered furthermore that the access enjoyed by the U.S. intelligence services to the transferred data constituted an interference with the right to respect for private life and the right to protection of personal data, which are guaranteed by the Charter. Likewise, the inability of citizens of the EU to be heard on the question of the surveillance and interception of their data in the United States amounted, in the Advocate General's view, to an interference with the right of EU citizens to an effective remedy, protected by the Charter. According to the Advocate General, that interference with fundamental rights was contrary to the principle of proportionality, in particular because the surveillance carried out by the U.S. intelligence services was a mass and indiscriminate surveillance. He considered that the Commission decision was invalid.

164 CJEU, C-362/14, *Schrems,* supra n. 128, para. 76–77.

165 CJEU, C-362/14, *Schrems,* supra n. 128, para. 88.

166 CJEU, C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger and Others,* supra n. 114, para. 54 and 55 and the case-law cited.

exception in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use.[167] In particular, the Court held legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU Charter.[168] Accordingly, the Court underscored the fact that Article 3 paragraph 1 (b) of Decision 2000/520 needed to be interpreted in accordance with the objective of protecting personal data pursued by Directive 95/46, and also in the light of Article 8 of the EU Charter. That being so, the Court concluded that in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25 paragraph 6 of Directive 95/46. Read in the light of the EU Charter, Article 3 of the decision was held invalid,[169] and thus, the Safe Harbor decision 2000/520 was held invalid.[170]

D. An Unbridgeable Gap?

Since the Court's invalidation of the Safe Harbor decision 2000/520, the European Commission and the United States have agreed on a new framework for transatlantic data flows: The EU-U.S. Privacy Shield. It was formally approved by the European Commission on 12 July 2016,[171] finding that the Privacy Shield Framework provides adequate protection for EU residents to permit transfer of their personal data from the EU to the United States. Although the Privacy Shield implements certain principles, similar to Safe Harbor, it differs in several respects: The Privacy Shield Framework establishes seven Privacy Shield Principles and sixteen additional principles, resulting in stronger obligations on U.S. companies handling personal data, defined means of redress available for EU individuals, enforcement commitments from U.S. agencies, safeguards on U.S. government access, and continuing monitoring of the program itself. Nevertheless, the new Privacy Shield must still be criticized for failing

167 CJEU, C-362/14, *Schrems,* supra n. 128, para. 91–94. Cf., to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 201, 31 July 2002, p. 37); CJEU, C-293/12 and C-594/12, *Digital Rights Ireland and Others,* supra n. 114, para. 57 to 61. Cf. also BVGer, *A.-F. v. Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF),* A-4941/2014 (9 November 2016).

168 CJEU, C-293/12 and C-594/12*, Digital Rights Ireland and Others,* supra n. 114, para. 39.

169 CJEU, C-362/14, *Schrems,* supra n. 128, para. 102–104.

170 CJEU, C-362/14, *Schrems,* supra n. 128, para. 106.

171 Commission implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. Privacy Shield, OJ L 207, 1 August 2016, p. 1.

to sufficiently protect the privacy rights of EU nationals, though it is generally seen as an improvement in comparison to the «Safe Harbor» agreement.[172]

IV. Conclusion

The purpose of this article was to present the important role of regional law and institutions in the development and rise of international human rights standards and to outline how the level of protection guaranteed by the European states is far more advanced than equivalent regulations on a universal level or in other regions of the world. Whilst a universal approach to human rights protection often carries the expectation of a homogeneous, effective and uniform legislative method, solutions on a universal stage are in practice lagging behind the developments accomplished on the regional level in Europe. The examples discussed in this article show that the most sustainable approach for regulating matters of human rights protection regularly takes up the advantages of institutional frames that are narrower and more precise than the universal ones. Further, it has been shown that, as to the level of protection of human rights, a sharp divide gradually opened up between the EU and the United States. As a consequence of the diverse shortcomings of universally applicable human rights conventions, the European human rights protection mechanisms have shown that states are apt to develop a network of numerous and more far-reaching agreements on the protection of human and minority rights on a regional level, bringing Europe steps ahead of other regions of the world in general, and the United States in particular. However, we have seen that even in Europe there is a risk of fragmentation in the human rights protection level guaranteed by the different organizations.

By continuously increasing the level of safeguard provided in Europe, both the member states of the Council of Europe and the EU are sending a strong signal to the international community. Far from being merely an «academic» aspect of the legal

172 Cf. also BGer 4A_83/2016 (22 September 2016), consid. 3.1., in which the Court proceeded on the assumption that the United States did not ensure the same level of protection of personal data as provided by Swiss law. Starting 12 April 2017, organizations can self-certify to the Swiss-U.S. Privacy Shield Framework, which replaces the Safe Harbor Agreement between Switzerland and the United States. The Swiss Federal Data Protection and Information Commissioner (FDPIC) considered that the new framework guarantees an adequate level of data protection. He has approved the level based on the wording of the Swiss–U.S. Privacy Shield and has amended his list under Article 7 of the Ordinance to the Data Protection Act for the benefit of companies certified in this connection. The changes include a stricter application of data protection principles by participant companies and improved management and supervision of the framework by the U.S. authorities. Persons concerned are given specific instruments to enable them to find out directly from certified U.S. companies or the competent authorities about data processing and to ensure that any required corrections or deletions are made. People can also indirectly influence the processing of their data by the U.S. security services via an ombudsman procedure. In addition, the U.S. authorities have given assurances that they will act to enforce and evaluate the new instruments.

craft, fragmentation[173] has emerged naturally with the increase of international legal activity in the area of human rights which may only be controlled by the use of regional cooperation and coordination. In this regard, regional cooperation and coordination is not to be understood in terms of exceptions to international law but as a varying, context-sensitive implementation and application of common standards. It indicates that local modes of problem-solving are, in general, efficient since they are based on a better understanding of the specific circumstances and are therefore a better place to take account of local peculiarities, cultural or otherwise.[174]

We conclude that human rights are and should be further developed and strengthened on a regional level. This may ensure a more efficient or equitable implementation of the relevant norms. The resulting fragmentation may then constitute an opportunity to develop and consolidate higher standards in regional human rights protection that will affect and assist the development of sustainable human rights protection mechanisms on an international level. Therefore, the Vienna Declaration's calling on states to endorse efforts to strengthen regional arrangements and to increase their effectiveness, while at the same time stressing the importance of international cooperation, has lost nothing of its relevance since its declaration in 1993.

173 Cf. Koskenniemi, supra n. 2.

174 Cf. Christoph Schreuer, Regionalism v. Universalism, 6 Eur. J. Int'l L. (1995), pp. 477–499, p. 477.

Contributions

Recent Practice