Saar Blueprints

Oskar Josef Gstrein

Regulation of Technology in the EU
and beyond -
The state of play in autumn 2015

Programm für lebenslanges Lernen

03 / 2015 EN

About the author

Oskar Josef Gstrein (gstrein@europainstitut.de) is research assistant of Prof. Thomas Giegerich, LL.M. at the Jean-Monnet Chair for European Integration at the Europa-Institut of the Saarland University. He is author of several articles in the field of European institutional law, European human rights protection and privacy issues. His PhD-Thesis is on the topic "The Right to be Forgotten as a Human Right".

Preface

This publication is part of an e-paper series (Saar Blueprints), which was created as part of the Jean-Monnet-Saar activity of the Jean-Monnet Chair of Prof. Dr. Thomas Giegerich, LL.M. at the Europa-Institut of Saarland University, Germany. For more information and content visit http://jean-monnet-saar.eu/.

Editor

Lehrstuhl Prof. Dr. Thomas Giegerich
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

ISSN

2199-0050 (Saar Blueprints)

Citation

Gstrein, Oskar Josef, Regulation of Technology in the European Union and beyond – The state of play in autumn 2015, 03/2015 EN, available at: http://jean-monnet-saar.eu/?page_id=67

A. Introduction

Just recently the European Commission has confirmed that the establishment of the so called "Connected Digital Single Market" in the European Union remains second in the list of top priorities during its term ending in 2019.[1] This is probably the strongest indicator that the Commission has deliberately chosen the field of technology regulation to be its showcase when being asked what it has achieved during its term. While other topics, such as the yet unsolved refugee crisis, the stability of the Euro area and climate change seem only to be connected with misery and cumbersome political negotiations,[2] technology regulation appears more likely to produce countable and productive outcomes.

Despite this hope it should be borne in mind that Europe and especially the European Union still has difficulties in finding a clear stance on what the regulation of technological development should ultimately achieve. The different nuances of the complex picture showing the perception of technology on the continent at the start of the 21st century can be divided into two categories:

On the one hand there is a craving for the economic and social fruits resulting from the positive effects of the development of technology. Data is being seen as a valuable resource, as the "commodity of the future",[3] which is as real and valuable as "coal and steel"[4] as German Chancellor Angela Merkel said recently. On the other hand, though, there is profound skepticism how the advancement and ongoing implementation of technology will influence the lives of Europeans. Since most of the companies who are shaping development in the sector have their origins in countries outside of Europe one can observe a certain skepticism and unwillingness of "consumers" to adopt their lifestyles to products and services which are to a very large extent being produced and developed far away. This skepticism has deepened since the broader population has become aware of the fact that some of these products and services can easily be adopted to create comprehensive personal profiles which might be (ab-)used for surveillance by public or private entities.[5] Eurostat published in

[1] *Juncker*, *Timmermanns*, "Letter of Intent to President Martin Schulz and to Prime Minister Xavier Bettel", p. 29; http://ec.europa.eu/priorities/soteu/docs/state_of_the_union_2015_en.pdf - accessed on 16.09.2015; Cf. http://ec.europa.eu/priorities/digital-single-market/index_en.htm - accessed on 15.09.2015.

[2] Cf. the remarks of *President Juncker* at the State of the Union 2015, http://ec.europa.eu/priorities/soteu/docs/state_of_the_union_2015_en.pdf - accessed on 16.09.2015, p. 6-18, 22 ff.

[3] *Funk*, „Merkel: Daten sind der Rohstoff der Zukunft", Tagesspiegel, 12.09.2015, http://bit.ly/1KhlNqK - accessed on 16.09.2015.

[4] Ibidem.

[5] Cf. for instance *Schneier*, "Data and Goliath", W.W.Norton & Company, 2015;

June 2015 a Special Eurobarometer on data protection claiming: “Two-thirds of respondents are concerned about not having complete control over the information they provide online.”[6]

Furthermore, even in Europe itself the positions of member states differ significantly. The recently appointed UN Special Rapporteur for Privacy, Joseph Cannataci, called “the British surveillance oversight as being ‘a joke’, and said the situation is worse than anything George Orwell could have foreseen.”[7]

To bridge the gap between these two categories is the task of legislators in the European Union who need to align economic and social interests, human rights and the sovereignty and security needs of the people on the continent. In other words: “Digital assertiveness depends crucially on the willingness of member states to expand the quantity and quality of European law.”[8] The aim of this paper is to provide a concise overview where we stand in this process at the beginning of autumn 2015.

B. Data Protection Regulation

The attempt to develop a new regulatory framework for technological development in the European Union is certainly spearheaded by the Proposal for a General Data Protection Regulation which was issued on the 25th of January 2012.[9] It took some time, but the European Parliament and the Council now both have produced their own amended versions of the document.[10] Currently, the so called “trialogue negotiations” are being held between the Commission, the Council and the European Parliament[11] who are supposed to be

[6] Eurostat, “Special Eurobarometer 431 – Data Protection Summary”, p. 4, via http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf - accessed on 30.09.2015.
[7] *Alexander*, “Digital surveillance 'worse than Orwell', says new UN privacy chief”, The Guardian 24.08.2015, http://bit.ly/1fBxFvs - accessed on 16.09.2015.
[8] *Bennediek*, *Berlich*, *Metzger*, „The European Union’s Digital Assertiveness“, SWP Comments 2015/C 43, http://bit.ly/1ivIWzN – accessed on 16.09.2015, September 2015, p.8.
[9] Proposal for a regulation of the European Parliament and 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), COM/2012/011 final - 2012/0011 (COD), http://eur-lex.europa.eu/legal-content/en/NOT/?uri=CELEX:52012PC0011 – accessed on 16.09.2015.
[10] Cf. for an overview Council of the EU, Interinstitutional File 2012/0011(COD), 08.07.2015, http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf - accessed on 16.09.2015. A comprehensive collection of the relevant documents can be found at http://www.delegedata.de/european-data-protection-reform-resource-database/ - accessed on 16.09.2015.
[11] A tentative roadmap of the negotiation process can be found via https://edri.org/gdpr-document-pool/ - accessed on 05.10.2015.

completed by the end of 2015[12] and should result in agreement on the legislative act which is to replace Directive 95/46/EC.[13]

Despite this generally positive development it seems as if the road to a finalized version of the regulation still could turn out to be quite far. The European Data Protection Supervisor Giovanni Buttarelli issued an opinion on the 27th of July 2015 highlighting several of the remaining challenges.[14] He pointed out that a new regulation needs to be "a better deal for the citizens" (clear definitions, processing of data must be lawful and justified, better supervisory mechanisms),[15] practicable (effective safeguards, striking the balance between individual rights and the public interest, effective supervision)[16] and future-proof.[17]

In Germany national and regional data protection authorities[18] as well as experts[19] voice concern when it comes to the standard of protection by the new regulation. Also Non-Governmental Organisations (NGOs) are watching the negotiation process closely and critically.[20]

Especially the position of the Council is being criticized for being too friendly to data processing businesses. However, when it comes to the position of the Parliament it needs to be highlighted that a few important events like the Court of Justice's (ECJ) "Google Spain" judgment[21] occured after the EP took its first vote on the proposal.

Analyzing the implementation of "the right to be forgotten" or more precisely the right to delist personal information from the index of a search engine[22] in particular it seems at the time of writing that the current drafts of the new regulation do not seem to reflect this individual right at all. Considering at the same time that new cases are pending before the ECJ this can

---

[12] For an overview see https://edri.org/gdpr-document-pool/ - accessed on 16.09.2015; *Will*, "Schlussrunde bei der Datenschutz-Grundverordnung?", Zeitschrift für Datenschutz, 08/2015, p. 345 – 346, p.345.

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31 - 50.

[14] European Data Protection Supervisor, Opinion 3/2015, "Europe's big opportunity", can be found at http://bit.ly/1SJrGSq - accessed on 18.09.2015.

[15] Ibidem, p. 5.

[16] Ibid., p. 6.

[17] Ibid., p 7.

[18] *Bergemann*, „Datenschutzreform: Deutsche Datenschützer zerpflücken Position der EU-Regierungen", via http://bit.ly/1SJrGSq - accessed on 18.09.2015.

[19] *Schaar*, „Europäischer Datenschutz: Bitte nicht aufweichen!", via http://www.eaid-berlin.de/?cat=8 – accessed on 18.09.2015; *Weichert*, „Europas Datenschutz", Datenschutz Nachrichten 03/2015, p. 112 – 117, p. 114 – 116, via http://bit.ly/1imQvYR - accessed on 18.09.2015.

[20] Cf. European Digital Rights platform via http://protectmydata.eu/, accessed on 18.09.2015.

[21] ECJ, C-131/12, "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González", ECLI:EU:C:2014:317.

[22] Art 29 Working Group, Press Release from 18.06.2015 on the Implementation of the Google Spain judgement via http://bit.ly/1OoWVnP - accessed on 21.09.2015.

hardly be understood.[23] Such hesitation results in the danger that the ECJ will become a "co-legislator" in the field of technology regulation.

When it comes to issues like the extraterritorial application of European data protection law,[24] the establishment of the so-called "one-stop shop" mechanism to create a single authority which is responsible for supervision[25] or the much discussed "risk-based approach", the details behind the concepts laid down in the regulation seem to remain vague. This becomes especially visible with regard to the risk-based approach which should constitute a tool helping to create more responsibility for data processing in particularly sensitive contexts.[26] On the other hand this approach would also facilitate the processing of data in situations where the consequences or contexts may not be critical at all (e.g. the small barber-shop around the corner wants to setup a newsletter for its costumers). However, despite being an interesting and pragmatic idea it remains to be seen whether Parliament and Council will be able to agree on a consistent and coherent categorization of risks so that improved safeguards can be guaranteed by data processors.[27]

Finally, it seems as if the ambitious agenda of the European Union puts very much pressure on the negotiating bodies. This may help them in finding compromises more quickly. However, some innovative legal concepts are almost created "on the fly" and sometimes implemented in the text without having received the necessary fine-tuning. Important decisions on basic problems concerning in the context of the processing of personal data are yet to be made and it is unclear whether they can be achieved at all. Hence, the negotiations may ultimately produce a new, but incoherent and not necessarily better regulative framework. Whether regulation that has been drafted in the spirit of "done is better than perfect" will live up to public expectations is questionable. And it is also unclear whether at the end of the year the political actors in the member states will show the willingness to make ends meet when it comes to replacing familiar national data protection legislation by a common European approach which some might consider as a symbol of further centralization in the European Union.

---

[23] Cf. a new reference by the Italian Supreme Court in the case C-398/15, Manni. The reference was not widely published at the writing of this article. For an overview see *Ausloos*, "CJEU is asked to rule on the 'Right to be Forgotten' again" via http://bit.ly/1gx7UNk - accessed on 18.09.2015.

[24] Especially the conflicts arising between the fields of fundamental rights protection and private international law. *Kuner*, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", University of Cambridge Faculty of Law Research Paper No. 49/2015, p. 11, 17 via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644237 – accessed on 18.09.2015.

[25] *Will*, p. 346.

[26] *Veil*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, p. 347 – 353, p. 348.

[27] Ibidem, p. 353.

C. Territoriality, the future of Safe Harbor and the "Umbrella Agreement"

The "Safe Harbor" agreement can best be understood as a bridge guaranteeing fundamental rights protection between the EU and the United States (US). It was initiated by the American authorities as a reaction to the adoption of Directive 95/46/EC.[28] Since the EU Commission did not regard the protection of personal data in the US as being "adequate" under European standards the US Department of Commerce developed the Safe Harbor regime.[29]

The concept is simple: If an undertaking wants to transfer personal data (referring to employees, customers, business partners, etc.) across the Atlantic it needs to adhere to the Safe Harbor principles and notify the Department of Commerce thereof.[30] One of the biggest problems of the system has always been the process of "self-certification" of the participants in view of allegations by some European DPAs that US-authorities are negligent when it comes to the controlling the actual compliance of the participants of the system.[31] However, ultimately the Snowden revelations[32] made clear that the system needed to be reformed.[33]

Since that time there were discussions on whether the European Union should have backed out of the Safe Harbor regime or not. The Commission opted for the initiation of a re-negotiation process which it considered as a sufficient reaction.[34] On 27.11.2013 it published 13 "recommendations" on how to improve the Safe Harbor system with regard to transparency, redress, enforcement and access to the privately processed data by US

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[29] http://www.export.gov/safeharbor/index.asp - accessed on 21.09.2015; *Peltz-Steele*, "The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation", Journal of Internet Law, Volume 19 Number 1, July 2015.
[30] For details see http://www.export.gov/safeharbor/eu/eg_main_018475.asp - accessed on 21.09.2015.
[31] *Spies*, *Schröder*, „Cloud Computing und EU/US Safe Harbor Principles – US-Handelsministerium bezieht Stellung", ZD-Aktuell 2013, p. 03566.
[32] Cf. *Greenwald*, „No place to hide", Metropolitan Books, New York, 2014.
[33] *Spies*, *Schröder*, p. 03566.
[34] Opinion of AG Bot, C-362/14, 23.09.2015, „Maximilian Schrems v. Data Protection Commissioner", Mn. 224: "In addition, the Commission expressly acknowledged at the hearing that, under Decision 2000/520, as currently applied, there is no guarantee that the right of citizens of the Union to protection of their data will be ensured. However, in the Commission's submission, that finding is not such as to render that decision invalid. While the Commission agrees with the statement that it must act when faced with new circumstances, it maintains that it has taken appropriate and proportionate measures by entering into negotiations with the United States in order to reform the safe harbour scheme."

authorities.[35] In the second half of 2015 it seems that the parties will have an updated agreement soon, although no details of that agreement have been published yet.[36]

In the meantime it was announced quite unexpectedly that a parallel agreement between the EU and the US has been negotiated and initialled, but not yet signed or ratified. The so-called "Umbrella agreement" deals with the protection of personal data when transferred between law enforcement authorities.[37] Although the text of the agreement had not been published at the time of writing a leaked version has become available on the Internet.[38] It has already been commented on by Peter Schaar, the former Federal Commissioner for Data Protection and Freedom of Information in Germany. Although there seems to be progress when it comes to the issue of judicial, and not only administrative, redress for EU citizens in the US some shortcomings still remain.[39] The agreement will not provide the same level of protection for EU citizens as US nationals enjoy in general and "it should be noted that the agreement shall apply only to judicial and police authorities, but not to authorities with the task to guarantee the 'national security'. US intelligence agencies like the NSA and the CIA share personal data with law enforcement agencies, even if they have received these [sic] information from their European partners. […] Last but not least the agreement does not cover data US and European authorities collect on the basis of national laws, i.e. the Foreign Intelligence Surveillance Act (FISA) or similar European legislation."[40] Another critical issue is the question of oversight over the authorities in the respective countries.[41]

Furthermore, the envisaged agreement has also already been reacted on by the American civil society.[42] In a letter to Representatives Goodlatte and Conyers, Jr. from the US House of Representatives Committee on the Judiciary the organization the NGO epic.org pointed out that the Privacy Act of 1974 which would have to be amended in order to implement the provisions of the umbrella agreement is one of the very few statutes in the US in the field which is distinguishing between US citizens and foreigners who do not permanently reside in the US.[43] This had to be considered as an obsolete and overcome legislative technique since

[35] European Commission, Memo on "Restoring Trust in EU-US data flows - Frequently Asked Questions", 27.11.2013 via http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm - accessed on 21.09.2015.
[36] European Commission, „Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement", Press Release from 08.09.2015 via http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm - accessed on 21.09.2015.
[37] Ibidem.
[38] Via http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf - accessed on 21.09.2015.
[39] *Schaar*, „Leaky Umbrella", via http://www.eaid-berlin.de/?p=779 – accessed on 21.09.2015.
[40] Ibidem.
[41] Ibid.
[42] Cf. https://epic.org/privacy/intl/data-agreement/ - accessed on 25.09.2015.
[43] *Rotenberg* et al., „Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015", via https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf - accessed on 25.09.2015.

more modern texts do not include a distinction of that sort. Hence, the suggestion is to amend the definition of "individual" so that it also covers foreign citizens.[44]

Whether the political decision-making process will adopt this approach remains to be seen.[45] In conclusion it can be stated that while the negotiation efforts have started to bear fruits some work still remains to be done. Looking at it pragmatically, however, terminating the Safe Harbor regime is not an option for the parties since both European and American companies have become highly dependent on a robust framework for the transfer of personal data across the Atlantic. In October 2015 there were approximately 4,400 companies participating in the system.

However, this view was not shared by General Advocate Yves Bot who stated in his Opinion in the case of Maximilian Schrems v. Data Protection Commissioner: "In addition, I consider that, faced with such findings, the Commission ought to have suspended the application of Decision 2000/520. The objective of protecting personal data pursued by Directive 95/46 and Article 8 of the Charter places obligations not only on the Member States but also on the EU institutions, as follows from Article 51(1) of the Charter."[46] This statement as such is not binding on the European institutions and member states. However, it considerably increased pressure on the negotiators to produce quickly a useful result in the process of renewal of the EU-US legal framework. The US Mission to the EU published a statement on the opinion of Bot on 28.09.2015 in which it tried to relativize some of his statements. Particularly the assessments regarding fact finding by the Irish High Court, the comments on the surveillance activities of the US and the notion of the Safe Harbor regime as such were challenged.[47] On 29.09.2015 Schrems shared via Twitter that the final ruling by the ECJ was due on 06.10.2015.[48]

It was highly questionable whether the ECJ would be deciding less than two weeks after the General Advocate's opinion in such a high profile case. But the judges in Luxembourg did not disappoint data protection activists in Europe.[49] In their ruling they followed the path blazed

---

[44] Ibidem, p.2.
[45] *Reding*, "Bridging the Transatlantic Digital Divide", Project Syndicate via http://bit.ly/1G0jYgW - accessed on 28.09.2015.
[46] Opinion of AG Bot, C-362/14, 23.09.2015, „Maximilian Schrems v. Data Protection Commissioner", Mn. 226.
[47] US mission to the EU, "Safe Harbor Protects Privacy and Provides Trust in Data Flows that Underpin Transatlantic Trade" via http://useu.usmission.gov/st-09282015.html - accessed on 29.09.2015.
[48] Twitter Account of Max Schrems via https://twitter.com/maxschrems/status/648610208118370308 – accessed on 29.09.2015; Cf. also the announcement on the website of the court http://bit.ly/1KIdt6u - accessed on 29.09.2015.
[49] *McNamee*, "Fifteen years late, Safe Harbor hits the rocks" via https://edri.org/safeharbor-the-end/ - accessed on 06.10.2015; *Biselli,* "Europäischer Gerichtshof: Safe Harbor ist ungültig! Schluss mit der blauäugigen Datenübertragung in die USA." via https://netzpolitik.org/2015/europaeischer-gerichtshof-

by Bot and held that "[...] even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive. Nevertheless, the Court points out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid. Consequently, where a national authority or the person who has brought the matter before the national authority considers that a Commission decision is invalid, that authority or person must be able to bring proceedings before the national courts so that they may refer the case to the Court of Justice if they too have doubts as to the validity of the Commission decision. It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid."[50] This marked the end of Safe Harbor as it was known from 26.06.2000 to 06.10.2015.

The decision can be understood in several ways. Frist, it is obvious that the court once more reinforces art 19(1) sentence 2 of the Treaty on the EU which declares that it is the only institution which is allowed to interpret EU law authentically. As a consequence the court weakens the powers of the Commission which tries to centralize data protection issues in Europe. The ECJ even explicitly stated that the Commission has overstepped its competences with the Safe Harbor Decision 2000/520.[51] Hence, national DPAs get more responsibility, but also more opportunities to be proactive.

Secondly, the story of the reidentification of the EU as a guardian of Human Rights continues.[52] With this judgment the court, similarly as with the "Digital Rights Ireland"[53] and "Google Spain"[54] judgments, adds one more step to shaping substantive data protection law as well as the constitutional legal framework of human rights protection in the EU and beyond. This aspect is also reflected by the initial response of Schrems to the judgment: "I very much welcome the judgement [sic!] of the Court, which will hopefully be a milestone

---

safe-harbor-ist-ungueltig-schluss-mit-der-blauaeugigen-datenuebertragung-in-die-usa/ - accessed on 06.10.2015.

[50] ECJ, Press Release No 117/15, C-362/14, 06.10.2015 via http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf - accessed on 06.10.2015.

[51] ECJ, C-362/14, „Maximilian Schrems v. Data Protection Commissioner", ECLI:EU:C:2015:650, Mn. 67 ff., 104.

[52] *Gstrein,* "The European Union and its reidentification as a guardian of human rights", Saar Blueprints 01 / 2014 EN, p. 10 f. via http://jean-monnet-saar.eu/?page_id=67 – accessed on 06.10.2015.

[53] ECJ, C-293/12 and C-594/12, „Digital Rights Ireland", ECLI:EU:C:2014:238.

[54] ECJ, C-131/12, "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González", ECLI:EU:C:2014:317.

when it comes to online privacy. This judgement [sic!] draws a clear line. It clarifies that mass surveillance violates our fundamental rights. Reasonable legal redress must be possible."[55]

Thirdly, a new transatlantic framework must be established for the processing of personal data.[56] In a reaction to the judgment on the same day it was handed down Commissioners Timmermans and Jourová confirmed that this new framework should include a stronger consideration of art 7 and 8 of the Charter of Fundamental Rights of the EU and that the Commission will try to prevent a fragmentation of the Digital Single Market. It will be interesting to see how the US will react to the concerns of the Europeans. In the meanwhile, the search for alternatives for the time without this new framework had already begun.[57] Such alternatives are for instance the informed consent of an individual to process personal data for a clearly defined purpose and if the processing of personal data is vital to fulfil or prepare the fulfilment of a contract (e.g. booking a hotel room in the US). However, it is clear that a general legal framework would facilitate the conduct of business and improve legal certainty significantly.

It should be added that at the time of writing a similar case is pending in the United States Court of Appeals for the Second Circuit.[58] In "Microsoft Corporation v. United States of America" the technology giant refuses to hand over customer data to US authorities which are being stored on a "Hotmail" server in a data center in Ireland: "The Government applied for and Magistrate Judge Francis issued a warrant [...] to seize the contents of an email account belonging to a customer of Microsoft Corporation."[59] Microsoft appealed arguing that it was not obliged to hand over the data stored on a foreign server simply because it was a company headquartered in the US. Microsoft is supported by several NGOs and other technology companies.[60]

The legal question behind the cases and the problems with the Safe Harbor regime is how to interpret and apply the principle of territoriality in the digital age.[61] In other words it is about

---

[55] *Schrems*, Initial response Press Release via http://www.europe-v-facebook.org/CJEU_IR.pdf - accessed on 06.10.2015.
[56] *Rotenberg*, "On International Privacy: A Path Forward for the US and Europe", Harvard International Review via http://hir.harvard.edu/archives/5815 - accessed on 06.10.2015.
[57] *Bager*, "Nach dem EuGH-Urteil: Alternativen zu Safe Harbor" via http://www.heise.de/newsticker/meldung/Nach-dem-EuGH-Urteil-Alternativen-zu-Safe-Harbor-2837700.html - accessed on 06.10.2015.
[58] *Thielman*, „Microsoft case: DoJ says it can demand every email from any US-based provider" via http://bit.ly/1hZa9Kt - accessed on 29.09.2015.
[59] The US Court of Appeals for the Second Circuit, „Microsoft Corporation v. USA", Brief for Appellant, 14-2985-CV, p. 6 via http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf - accessed on 29.09.2015.
[60] *Thielman*.
[61] Cf. Harvard Law Review, Recent Case : 15 F. Supp. 3d 466 (S.D.N.Y. 2014), "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.", 128 Harv. L. Rev. 1019 – 1026, p. 1019.

how to enforce the rule of law in a space which is not real, but merely virtual and in which, at least in theory, any state can participate and act in the same manner. Russia has recently tried to solve this problem by drafting a new statute which obliges data processors to store personal data of Russian citizens only on servers which are located on Russian territory. The law entered into force on 01.09.2015.[62] Similar discussions are being held in Germany and Europe where some demand the introduction of "national or European routing."[63] But also in Brazil and Canada discussions on "Network Sovereignty" and „Boomerang Routing are currently taking place."[64]

Strengthening the territoriality principle via technical means is certainly attractive from the perspective of conventional law enforcement. It would make it easier to enforce already existing provisions. However, it must also be taken into account that measures like national routing could lead to new monopolies and seriously affect businesses.[65] There is also the danger of fragmentation of the Internet. Furthermore, national routing and similar measures cannot be considered as effective safeguards against surveillance since it has turned out that national intelligence services, which still would be able to monitor traffic, could be willing to share their insights with foreign intelligence services. This has proven especially true in Germany.[66]

Despite being more cumbersome it seems preferable to establish an international regime which guarantees human rights protection (especially the protection of freedom of expression and privacy) and derives its legitimacy from the concept of human dignity of each internet user. This would have to be backed up by better technological protection against interference of any sort. If society truly wants to reap the benefits of the dynamic development of technology it must be acknowledged that the more static field of law has to adapt to the new circumstances. If technology as the dynamic part would be compelled to adapt it is questionable if and how much social advancement there would be at the end of the day. History after all shows that human rights protection and technological development both benefit greatly from leaving national borders and concepts behind and instead relying on sensible and commonly shared principles.

---

[62] *Henni*, „Russlands neuer Datenschutz – Herausforderung für Online-Unternehmen" via http://bit.ly/1QJjDoo - accessed on 29.09.2015.
[63] *Geminn*, "Die Debatte um nationales Routing – eine Scheindebatte?", Multimedia und Recht, 2015, p. 98 – 103, p.99.
[64] Ibidem, p. 99.
[65] Ibid., p. 102.
[66] Ibid., p. 100.

D. Data Retention

For activists against data retention the 08.04.2014 was a great day. The ECJ declared in its judgment in "Digital Rights Ireland" that "[…] Directive 2006/24/EC, […] has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter [of Fundamental Rights of the EU]."[67] Since the judgment struck down the legal foundation of data retention in the European Union it looked as if the battle over civil rights had been won. However, considering events from today's perspective, it must be concluded that data retention has not ceased to exist. It was just transferred back from the common European to the national level.

After a lengthy discussion whether to re-draft the data retention directive following the ECJ judgment the attacks on the French magazine "Charlie Hebdo" in early January 2015 again changed the landscape.[68] Meanwhile countries like France,[69] the United Kingdom (UK),[70] Finland,[71] the Netherlands,[72] Germany[73] and Austria[74] either have changed their surveillance laws or are in the process of doing so. Critics of data retention talk about a vicious circle when it comes to that discussion: First proponents demand that data needs to be retained in order to be able to prevent terrorist attacks and other serious crimes. And if it then turns out such crimes still happen the proponents do not acknowledge that data retention is ineffective wrong or disproportionate, but simply demand that more data needs to be collected and stored in order to make the systems work effectively.

---

[67] ECJ, C-293/12 and C-594/12, „Digital Rights Ireland", ECLI:EU:C:2014:238, Mn. 69.

[68] For a timeline of the events cf. "Charlie Hebdo attack: Three days of terror" via http://www.bbc.com/news/world-europe-30708237 - accessed on 28.09.2015.

[69] La Quadrature du Net, "Lettre ouverte aux députés français sur la proposition de loi relative à la surveillance international" via http://bit.ly/1KFwnuZ - accessed on 28.09.2015; *Kirsten*, "Frankreich führt Überwachungsgesetz für ausländische Kommunikationen ein", Netzpolitik.org 23.09.2015 via https://netzpolitik.org/2015/frankreich-fuehrt-ueberwachungsgesetz-fuer-auslaendische-kommunikationen-ein/ - accessed on 28.09.2015.

[70] *Boffey*, „Theresa May keeps snooper's charter secret", The Guardian 13.06.2015 via http://www.theguardian.com/politics/2015/jun/13/snoopers-charter-theresa-may-refuse-to-share - accessed on 28.09.2015; cf. in this context Press Release from Privacy International, "Human Rights Watch legal challenge to NSA/GCHQ intelligence sharing" via https://www.privacyinternational.org/node/651 - accessed on 29.09.2015.

[71] *Tammisto*, „Suomessa isoveli ei valvo verkossa", Helsingin Yliopisto via https://www.helsinki.fi/fi/uutiset/suomessa-isoveli-ei-valvo-verkossa - accessed on 28.09.2015.

[72] *Moody*, „New Dutch law would allow bulk surveillance, compelled decryption", Ars technica UK via http://arstechnica.co.uk/tech-policy/2015/07/new-dutch-law-would-allow-bulk-surveillance-compelled-decryption/ - accessed on 28.09.2015; cf. The consulation process via http://www.internetconsultatie.nl/wiv - accessed on 28.09.2015.

[73] *Wilkens*, „Bundestagsanhörung: Luft für Vorratsdatenspeicherung ist 'sehr dünn'", heise.de 22.09.2015 via http://www.heise.de/newsticker/meldung/Bundestagsanhoerung-Luft-fuer-Vorratsdatenspeicherung-ist-sehr-duenn-2822964.html - accessed on 28.09.2015.

[74] *Moody*, „Austria plans 10 new spy agencies with vast surveillance powers", Ars technica UK via http://arstechnica.co.uk/tech-policy/2015/09/austria-plans-ten-new-spy-agencies-with-vast-surveillance-powers/ - accessed on 28.09.2015; Opinion of AKVorrat on the draft of the bill which is being introduced in the Austrian parliament by the government: https://akvorrat.at/sites/default/files/AKVorrat_PStSG_Stellungnahme_RV.pdf - accessed on 28.09.2015.

Looking at the development it seems that data retention is just about to have its big comeback at the end of the year 2015 and that the measures law enforcement authorities will have at hand in the next years will be more intrusive than those available before the annulment of Directive 2006/24/EC.

E. Cyber Security & NIS-Directive

On 25.09.2015 the White House released a fact sheet on the future development of "U.S.-China Economic Relations."[75] In the document it is stated that "[t]echnology is one of the pillars of the bilateral economic relationship between the United States and China. Creating the conditions for expanded two-way trade and investment in the technology sector and avoiding measures that restrict it are critical to sustaining positive momentum in the economic relationship between our countries. […] Both countries commit that generally applicable measures to enhance information and communication technology cybersecurity in commercial sectors (ICT cybersecurity regulations) should be consistent with WTO agreements, be narrowly tailored, take into account international norms, be nondiscriminatory, and not impose nationality-based conditions or restrictions, on the purchase, sale, or use of ICT products by commercial enterprises unnecessarily."[76]

A similar agreement has already been concluded in May of 2015 between China and Russia.[77] It is possible that such bilateral agreements will pave the way to an international regime which will establish binding rules in the area of cyberspace when it comes to cyber-espionage, cyber-crime and cyber-warfare.

In the EU the Commission tried to set an initiative with the publication of a cybersecurity strategy on the 07.02.2013.[78] On the same date a proposal for a "Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union" (NIS-Directive) was put forward.[79] On 13.03.2014 the European Parliament had its first reading of the directive and passed it with

[75] White House, "FACT SHEET: U.S.-China Economic Relations", 25.09.2015 via https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-us-china-economic-relations - accessed on 29.09.2015.
[76] Ibidem.
[77] *Razumovskaya*, „Russia and China Pledge Not to Hack Each Other", Wall Street Journal 08.05.2015 via http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/ - accessed on 29.09.2015.
[78] European Commission, „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 07.02.2013, JOIN(2013) 1 final.
[79] European Commission, „Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 07.02.2013, COM(2013) 48 final.

amendments[80] which were commented on by the Commission on 10.06.2014.[81] At the time of writing it remains to be seen how the Council will finally react to the position of the Parliament and what an amended version adopted by it will look like. However, since the activities and approaches of the member states still vary significantly in 2015 the function of this legislation will necessarily be to establish a common European approach to cybersecurity.[82]

F. Cases Pending in the European Court of Human Rights in Strasbourg

Besides the cases already mentioned in this paper which mostly came from the ECJ this section will point out some of the important cases which may be decided by the European Court of Human Rights (ECtHR) in Strasburg in 2015 and 2016.

First, there is "Big Brother Watch and Others v. the United Kingdom,"[83] a case which was communicated to the court on 09.01.2014. The applicants allege that article 8 of the European Convention of Human Rights (ECHR) was infringed by the UK because its surveillance programs (specifically TEMPORA by the Government Communications Headquarters or GCHQ) as revealed by Edward Snowden.[84]

The second case is "Bureau of Investigative Journalism and Alice Ross v the United Kingdom" which was communicated on 05.01.2015.[85] Similarly to the first case the applicants complain about infringements of articles 8 and 10 of the ECHR. They allege that because of their profession they are very likely to have been the subject to surveillance by GCHQ.[86]

The third case is "Mohamed Ben Faiza v France." The application was communicated on 03.02.2015.[87] In this case it is questionable whether the surveillance measures used by the

[80] European Parliament, "Legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)) (Ordinary legislative procedure: first reading)" via http://bit.ly/1JA8fWD - accessed on 29.09.2015.
[81] For the state of play of the procedure see http://bit.ly/1PLvq5C - accessed on 29.09.2015.
[82] Cf. BSA, "EU Cybersecurity Dashboard 2015", p. 4 via http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf – accessed on 29.09.2015.
[83] ECtHR, „BIG BROTHER WATCH and others v the UK", Communicated 09.01.2014, App. No. 58170/13.
[84] Ibidem via http://hudoc.echr.coe.int/eng?i=001-140713 – accessed on 29.09.2015.
[85] ECtHR, „Bureau of Investigative Journalism and Alice Ross v the United Kingdom", Communicated on 05.01.2015, App. No. 62322/14.
[86] Ibidem, via http://hudoc.echr.coe.int/eng?i=001-150946 – accessed on 29.09.2015.
[87] ECtHR, „Mohamed Ben Faiza v France", App. No. 31446/12.

French police during a criminal investigation are compatible with articles 5 and 8 of the ECHR.[88]

The last case which should be mentioned here is "Roman Zakharov v. Russia." [89] It is pending before the Grand Chamber of the court which held on the 24.09.2014 a hearing. The Chamber relinquished jurisdiction in favor of to the Grand Chamber on 11.03.2014.[90] The applicant claims articles 8 and 13 of the ECHR. He is the editor-in-chief of a publishing company and subscriber to several mobile network operators in Russia. The applicant alleges that the operators installed devices which allowed the national intelligence service (the "FSB") to monitor his activities at any time and without prior judicial authorization. After exhausting all legal remedies in Russia which are allegedly not effective the application had been lodged on 20.10.2006.[91]

G. Other Relevant Developments

I. Modernization of Convention 108

The "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108) of the Council of Europe (CoE) is the oldest binding international agreement in the field of data processing.[92] However, even the best agreement needs to be revised at times, especially when it regulates technology and dates from 28.01.1981 which is now more than thirty years ago. Hence, the process of modernization was formally acknowledged by the Council of Ministers in the 1079th meeting on 10.03.2010.[93]

The aims of the revision are to "better address emerging privacy challenges resulting from the increasing use of new information and communication technologies, the globalisation of processings and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism."[94] The modernized version of

[88] Ibidem, via http://hudoc.echr.coe.int/eng?i=001-152665 – accessed on 29.09.2015.
[89] ECtHR, „Roman Zakharov v. Russia", App. No. 47143/06.
[90] ECtHR, „ Grand Chamber hearing concerning the monitoring of telephone communications", Press Release 269 (2014) via http://bit.ly/1h7C4qD - accessed on 29.09.2015.
[91] Ibidem.
[92] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" via http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm - accessed on 30.09.2015.
[93] CoE, CAHDATA, Draft Explanatory Report, version of 23.11.2014, p. 4 via https://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA%282014%2906_Draft%20explanatory%20report.pdf – accessed on 30.09.2015
[94] Ibidem.

Convention 108 was forwarded by the Ad hoc committee on Data Protection (CAHDATA) to the Council of Ministers for examination and adoption on 03.03.2015.[95]

Convention 108 is an interesting example how standard-setting could work in the field of technology regulation on a global scale. The text is being drafted in a setting where not too many players are involved and where it is possible to find a compromise. But due to the fact that the Convention is open to join for other states and International Organizations too (see Art 23(1) of the draft for the modernized convention)[96] it can evolve to a treaty of global relevance. So far to the old version of the Convention states such as Uruguay, Mauritius, Morocco and Senegal formally declared their willingness to sign and ratify the treaty.[97] Others are likely to follow once the modernized version is formally adopted and the members of the CoE invite them to join.

II. United Nations Special Rapporteur for Privacy

The revelations of Edward Snowden lead to consequences not only in Europe. Following an initiative of Brazil and Germany on 01.04.2015 the General Assembly of the United Nations (UN) decided to appoint a "Special Rapporteur for Privacy" for a period of three years.[98] The thematic mandate includes tasks such as to gather relevant information and exchange with UN member states and regional organizations on the perception and promotion of privacy, to study trends and developments in the area, to respond to the challenges of new technology, to contribute new ideas and concepts to the discourse and to report on alleged violations of the right to privacy as laid down in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.[99] The list of tasks is descriptive, not exhaustive. The Special Rapporteur has to present an annual report to the Human Rights Council and the General Assembly of the UN.[100] In July 2015 the Maltese Joseph Cannataci was appointed to the post.[101]

---

[95] CoE, CM(2015)40, 03.03.2015, p. 1 via https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA%203_Report_CM%282015%2940_En.pdf – accessed on 30.09.2015.

[96] Ibidem, p. 12.

[97] CoE, Treaty Office via http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=30/09/2015&CL=ENG – accessed on 30.09.2015.

[98] United Nations, General Assembly, A/HRC/RES/28/16, 01.04.2015 via http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement – accessed on 30.09.2015.

[99] Cf. Ibidem, p. 3 f.

[100] Ibid.

[101] UN, Office of the High Commissioner for Human Rights, http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx - accessed on 30.09.2015.

H. Conclusion

The development of technology and cyber space will continue to pose one of the biggest challenges for lawmakers in the coming years, probably decades. Since more and more technologies are affecting our lives also more aspects of our lives will have to be implemented and considered in technological development processes. This becomes very visible in the field of human rights protection.[102] The concept of privacy needs to be reshaped and other fundamental rights, most notably the right to freedom of expression, will acquire new dimensions, too. What makes this even more challenging is the fact that most of the fundamental rights affected are not absolute rights. That is to say that the development of new aspects of privacy or freedom of expression need to be balanced against each other and further rights at the same time.

But not only the future of human rights is problematic in a digital age. One of the biggest issues still is how internet governance should look like in general. After the US had announced in 2014 its readiness to transfer control over the Internet Corporation for Assigned Names and Numbers (better known as ICANN) to the international community the subsequent negotiation process demonstrated the world's inability to meet this challenge. After the deadline originally set passed in September 2015 it was decided that ICANN will retain its current status and therefore stay under US supervision.[103]

Technology and especially the internet offer great potential for human development. But the development of great potential requires hard work. And only if both factors come together the outcome will be successful.

[102] Cf. UN General Assembly Resolution, „The right to privacy in the digital age", A/RES/68/167 via http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 - accessed on 30.09.2015.
[103] *Elder*, „U.S. Delays Giving Up Oversight of Internet Administrator Icann", The Wall Street Journal, 18.08.2015, http://on.wsj.com/1KKBnyj - accessed on 30.09.2015.

I. References

1. *Alexander*, “Digital surveillance 'worse than Orwell', says new UN privacy chief”, The Guardian 24.08.2015, http://bit.ly/1fBxFvs - accessed on 16.09.2015.
2. *Ausloos*, “CJEU is asked to rule on the ‘Right to be Forgotten’ again” via http://bit.ly/1gx7UNk - accessed on 18.09.2015.
3. *Bager*, “Nach dem EuGH-Urteil: Alternativen zu Safe Harbor“ via http://www.heise.de/newsticker/meldung/Nach-dem-EuGH-Urteil-Alternativen-zu-Safe-Harbor-2837700.html - accessed on 06.10.2015.
4. *Bennediek*, *Berlich*, *Metzger*, „The European Union’s Digital Assertiveness“, SWP Comments 2015/C 43, http://bit.ly/1ivIWzN – accessed on 16.09.2015, September 2015.
5. *Bergemann*, „Datenschutzreform: Deutsche Datenschützer zerpflücken Position der EU-Regierungen“, via http://bit.ly/1SJrGSq - accessed on 18.09.2015.
6. Biselli, “Europäischer Gerichtshof: Safe Harbor ist ungültig! Schluss mit der blauäugigen Datenübertragung in die USA.” via https://netzpolitik.org/2015/europaeischer-gerichtshof-safe-harbor-ist-ungueltig-schluss-mit-der-blauaeugigen-datenuebertragung-in-die-usa/ - accessed on 06.10.2015.
7. *Boffey*, „Theresa May keeps snooper’s charter secret”, The Guardian 13.06.2015 via http://www.theguardian.com/politics/2015/jun/13/snoopers-charter-theresa-may-refuse-to-share - accessed on 28.09.2015.
8. *Elder*, „U.S. Delays Giving Up Oversight of Internet Administrator Icann”, The Wall Street Journal, 18.08.2015, http://on.wsj.com/1KKBnyj - accessed on 30.09.2015.
9. *Funk*, „Merkel: Daten sind der Rohstoff der Zukunft“, Tagesspiegel, 12.09.2015, http://bit.ly/1KhlNqK - accessed on 16.09.2015.
10. *Geminn*, “Die Debatte um nationales Routing – eine Scheindebatte?“, Multimedia und Recht, 2015, p. 98 – 103.
11. *Greenwald*, „No place to hide”, Metropolitan Books, New York, 2014.
12. *Gstrein,* “The European Union and its reidentification as a guardian of human rights”, Saar Blueprints 01 / 2014 EN, p. 10 f. via http://jean-monnet-saar.eu/?page_id=67 – accessed on 06.10.2015.
13. *Henni*, „Russlands neuer Datenschutz – Herausforderung für Online-Unternehmen“ via http://bit.ly/1QJjDoo - accessed on 29.09.2015.
14. *Juncker*, *Timmermanns*, “Letter of Intent to President Martin Schulz and to Prime Minister Xavier Bettel”.

15. *Kirsten*, “Frankreich führt Überwachungsgesetz für ausländische Kommunikationen ein“, Netzpolitik.org 23.09.2015 via https://netzpolitik.org/2015/frankreich-fuehrt-ueberwachungsgesetz-fuer-auslaendische-kommunikationen-ein/ - accessed on 28.09.2015.
16. *Kuner*, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, University of Cambridge Faculty of Law Research Paper No. 49/2015 via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644237 – accessed on 18.09.2015.
17. *McNamee*, “Fifteen years late, Safe Harbor hits the rocks” via https://edri.org/safeharbor-the-end/ - accessed on 06.10.2015.
18. *Moody*, „Austria plans 10 new spy agencies with vast surveillance powers”, Ars technica UK via http://arstechnica.co.uk/tech-policy/2015/09/austria-plans-ten-new-spy-agencies-with-vast-surveillance-powers/ - accessed on 28.09.2015.
19. *Moody*, „New Dutch law would allow bulk surveillance, compelled decryption”, Ars technica UK via http://arstechnica.co.uk/tech-policy/2015/07/new-dutch-law-would-allow-bulk-surveillance-compelled-decryption/ - accessed on 28.09.2015.
20. *Peltz-Steele*, “The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation”, Journal of Internet Law, Volume 19 Number 1, July 2015.
21. *Razumovskaya*, „Russia and China Pledge Not to Hack Each Other”, Wall Street Journal 08.05.2015 via http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/ - accessed on 29.09.2015.
22. *Reding*, “Bridging the Transatlantic Digital Divide”, Project Syndicate via http://bit.ly/1G0jYgW - accessed on 28.09.2015.
23. *Rotenberg*, “On International Privacy: A Path Forward for the US and Europe”, Harvard International Review via http://hir.harvard.edu/archives/5815 - accessed on 06.10.2015.
24. *Rotenberg* et al., „Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015”, via https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf - accessed on 25.09.2015.
25. *Schaar*, „Europäischer Datenschutz: Bitte nicht aufweichen!“, via http://www.eaid-berlin.de/?cat=8 – accessed on 18.09.2015.
26. *Schaar*, „Leaky Umbrella“, via http://www.eaid-berlin.de/?p=779 – accessed on 21.09.2015.
27. *Schneier*, “Data and Goliath”, W.W.Norton & Company, 2015.
28. *Spies*, *Schröder*, „Cloud Computing und EU/US Safe Harbor Principles – US-Handelsministerium bezieht Stellung“, ZD-Aktuell 2013, p. 03566.

29. *Tammisto*, „Suomessa isoveli ei valvo verkossa“, Helsingin Yliopisto via https://www.helsinki.fi/fi/uutiset/suomessa-isoveli-ei-valvo-verkossa - accessed on 28.09.2015.
30. *Thielman*, „Microsoft case: DoJ says it can demand every email from any US-based provider” via http://bit.ly/1hZa9Kt - accessed on 29.09.2015.
31. *Veil*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, p. 347 – 353.
32. *Weichert*, „Europas Datenschutz“, Datenschutz Nachrichten 03/2015, p. 112 – 117 via http://bit.ly/1imQvYR - accessed on 18.09.2015.
33. *Wilkens*, „Bundestagsanhörung: Luft für Vorratsdatenspeicherung ist 'sehr dünn'“, heise.de 22.09.2015 via http://www.heise.de/newsticker/meldung/Bundestagsanhoerung-Luft-fuer-Vorratsdatenspeicherung-ist-sehr-duenn-2822964.html - accessed on 28.09.2015.
34. *Will*, “Schlussrunde bei der Datenschutz-Grundverordnung?”, Zeitschrift für Datenschutz, 08/2015, p. 345 – 346.