www.jusletter-it.eu

Jakub Míšek

Hidden Pitfalls in Personal Data Processing

Collision between Current Data Protection Framework and New Technologies

The article focuses on several principles of personal data protection legal framework and procedures of public bodies responsible for their legal enforcement, which are in a direct collision with new technologies and uses of information, like Big data. Relevant institutes and judicial rulings are analysed and thus is shown, how strict application of personal data protection rules can cause absurd situations disconnected from the needs of people living in the real world. In the third part of the article are offered methods, which could possibly help to solve analysed problems.

Category: Articles
Field of law: Big Data, Open Data & Open Government; Data Protection
Region: Czechia

Citation: Jakub Míšek, Hidden Pitfalls in Personal Data Processing, in: Jusletter IT 21 May 2015

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Contents

1 Introduction

[Rz 1] «Privacy is dead.» This is not a new observation; it has been here for some time now.[1] Many authors argue that it is just a nature of things, because people don't impose a high value to their privacy anyway,[2] so logically there is no need to protect it anymore. But I am not convinced that the statement is true. Privacy is not only a distributive but also a non-distributive right. Distributive rights are those, which serve for good of a person, and the person can directly claim protection of such rights.[3] Distributive right to privacy is meant in the sense that every person has a right to privacy, or as would Warren with Brandeis say, a «right to be let alone»,[4] and every person can claim their right in front of the court or other competent institution, should this right be infringed. Non-distributive rights are rights which serve for public good and cannot be divided into particular rights of specific persons, even though every person benefits from such right. A good example of a non-distributive right are the environmental and nature-protection rights, rights to public security etc. As Polák states: «*Public good is a set of rules, which, indivisibility to particular subjects, leads in the end to an unique opportunity of their exercise by the state. In this case, public good can be therefore understood as a good of a single person, but because of its indivisibility it can be protected only by direct action of a public power.*»[5] The non-distributive aspect of privacy is strongly connected with the personal freedom. We can say that our society has an interest in liberty of people living in it and their freedom of thought. Without right to privacy the people would self-censor themselves. As Solove says: «*A society without privacy protection would be*

1 See e.g. Ustaran, Eduardo. 2013. Yes, Consent Is Dead. Further, Continuing To Give It A Central Role Is Dangerous. *Privacy Association*; Crosley, Stanley. 2014. Old School Privacy is Dead, But Don't Go Privacy Crazy. Privacy Association.

2 Grossklags, Jens, and Alessandro Acquisti. 2007. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In *6th Annual Workshop on the Economics of Information Security, WEIS 2007, The Heinz School and CyLab at Carnegie Mellon University, Pittsburgh, PA, USA, June 7—8, 2007*; Kumpot, Marek, and Václav Matyá. 2009. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU* 20: 13—20.; Acquisti, Alessandro, Leslie John, and George Loewenstein. 2013. What Is Privacy Worth? *Journal of Legal Studies* 42: 249—274 (Acquisti et al. 2013).

3 Polák, Radim. 2012. *Internet a promny práva*. Téma. Praha: Auditorium, 304 (Polák 2012).

4 Warren, Samuel D., and Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* IV: 193—220, 195.

5 Polák 2012, 343.

oppressive.»[6] In another article Solove quotes Richards and his concept of intellectual privacy.[7] Richards claims: «*[...] intellectual privacy contributes to the generation of new ideas and new ways of thinking about the world. Without free thought, the freedom to think for ourselves, to entertain ideas that others might find ridiculous or offensive, we would lack the ability to reason, much less the capacity to develop revolutionary or heretical ideas about (for instance) politics, culture, or religion. Engaging in these processes requires a space, physical and psychological, where we can think for ourselves without others watching or judging.*»[8] The right to think freely without exposing a persons inner thoughts might be endangered, because nowadays there are technologies like big data profiling and content customisation services which can lock their user in an information bubble and thus influence the way of their thinking.[9] This is the reason why privacy is not dead, why it must be protected even though people directly benefiting from that do not think it is important.[10]

[Rz 2] Having said that, it is necessary to face the fact, that the way how the legal regime of privacy and personal data protection works nowadays is far from perfect. The personal data protection concept, which we use up to this day, has its roots in the year 1980, when the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were published,[11] and were designed with a strong technology and legal neutrality principles. Due to this fact the system could have been somehow up and running through dramatic technological development and improvement no one could foresee. The main idea of the concept is that privacy is protected by the means of capability of holding a control over information — personal data[12]. This leads to a situation where personal data is advancing to the foreground of interest. Basic principles of personal data protection, like the definition of personal data, importance of consent, purpose limitation and focus on the data collection and beginning of processing, are not well adjusted with many new technologies and their possibilities. The Big Data phenomenon is a prime example on which this claim can be properly demonstrated.

[Rz 3] This article is divided into four parts. In the first one problems on the legislative level are described. The second part shows — with examples of decision practice — how problems mentioned in the first part are multiplied when the real life situation is not taken into account by competent bodies. The third part is dedicated to profiling and possible abuse of Big Data analysis and the final part tries to offer solutions to those problems.

---

6 Solove, Daniel J. 2013. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven Conn.: Yale University Press, 50 (Solove 2013).

7 Solove, Daniel J. 2012. *Privacy Self-Management and the Consent Dilemma*. SSRN Scholarly Paper ID 2171018. Rochester, NY: Social Science Research Network, 1892 (Solove 2012).

8 Richards, Na. 2008. Intellectual Privacy. *TEXAS LAW REVIEW* 87: 387—445, 425.

9 Jerome, Joseph. 2014. Big Data: Catalyst for a Privacy Conversation. *Indiana Law Review* 48: 213—242, 220 (Jerome 2014).

10 There is a joke going on in the Czech Republic in which the first Czechoslovak president T. G. Masaryk is saying: «*There will be democracy. And we are not going to vote about that.*»

11 Thirty years after, The OECD privacy guidelines. OECD, 2011, online [25 April 2014]. URL http://www.oecd.org/sti/ieconomy/49710223.pdf.

12 See Polák, Radim. 2014. Getting European Data Protection Off the Ground. *International Data Privacy Law*: ipu019. doi:10.1093/idpl/ipu019, 2 (Polák 2014).

2 Collision of the Law with the Reality

[Rz 4] The first problem includes, how personal data is defined, what information are considered as personal data and therefore fall into the scope of the European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data («Data Protection Directive»). Art. 2/a of the Data Protection Directive defines personal data as «*any information relating to an identified or identifiable natural person (data subject)*». The definition continues as follows: «*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*». This is a very broad definition, which can cover almost any information, and its broadness was confirmed by relevant interpretational bodies such as the Article 29 Data Protection Working Party (WP29)[13].

[Rz 5] Once a piece of information can be used by anyone as a means of identification of a natural person, it becomes personal data and the controller processing it must fulfil duties arising from the Data Protection Directive. This can easily happen in cases of massive databases, which aggregate many different types of data such as any which is used for Big Data. Information, which on its own were not in the scope of the Directive, are suddenly personal data (or even worse — sensitive personal data) when they are properly combined together and can be used for identification. There are exemptions in the Data Protection Directive, such as Art. 3 para. 2, which excludes some kinds of personal data processing, such as processing by a natural person in the course of a purely personal or household activity, from the scope of the Directive. But these exemptions do not provide much loose space, since the provision must be interpreted as narrowly as possible. This was stated by the Court of Justice of the European Union for example in the paragraph 29 of ruling in Case No. C-212/13.[14]

2.1 The Anonymisation Problem

[Rz 6] The directive offers another way out of its scope. When data is anonymised, it is no longer capable of identifying a specific natural person. There are two basic problems with this solution. Firstly, some data just cannot be anonymised by its nature. These are for example sensor datasets from personal wearable electronics like GPS, gyroscope motion sensors and other records coming, broadly speaking, from the «Internet of Things».[15] Secondly, the only perfect anonymisation is the one, from which everything is deleted, otherwise there is always a risk of re-identification. Paul Ohm in his influential article persuasively argues that anonymisation as a miraculous tool failed.[16]

[Rz 7] In the world, where huge databases are at reach of a hand, it is naïve to suppose that re-identification is impossible. The only question is, how hard it is, how much effort must be put into the process. But this question is not reflected in the Directive at all. The idea of anonymisa-

[13] See e.g. Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data. WP136. Online [10 April 2015]. URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[14] Court of Justice of the European Union, case No. C-212/13 from 11 December 2014.

[15] Peppet, Scott R. 2014. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review* 93: 85—178, 131(Peppet 2014).

[16] Ohm, Paul. 2009. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57: 1701—1777 (Ohm 2009).

tion was inherent part of the Data Protection Directive, it was supposed to mitigate strictness of rules for personal data processing and enable relatively open, but privacy friendly internet use.[17] Even now WP29 recommends this tool, although with notion about its problems.[18] The failure of anonymisation was not expected and now the problem is, that the decision whether something is or is not personal data, is binary. Does the information lead to an identifiable subject? Then it is personal data and the controller must fulfil all the duties. It is everything or nothing, which leads to absurd consequences, when disobeying the law is the only way how certain data controllers can run their businesses, which are altogether privacy friendly. This, as will be shown, is tolerated by data protection authorities, and the data protection laws are not effectively enforced.

2.2 Czech Example: A Lost Opportunity

[Rz 8] The Czech Act No. 101/2000 Sb. on personal data protection was enacted in the year 2000 and from the very beginning was meant as an implementation of the Data Protection Directive.[19] However, since the Czech Republic is a member state of the EU from 2004, some provisions in the act used to differ from the European model. The basic definition of the personal data was basically the same, but it included following exception: «*Information is not a personal data, if it is for identification of a person necessary to put forth unreasonable amount of time, effort or financial means.*» This provision was removed from the Czech Data protection act by the Act No. 439/2004 Sb.[20] Its explanatory note argues that this step was necessary due to the fact that in the current state of art is too easy and cheap to identify a person and therefore this provision is redundant. In my opinion the history has rounded up another circle, and nowadays it would be a useful provision again, which could increase legal certainty of data controllers, creative and profitable usability of personal data and when properly balanced, it would not harm data subjects. It could help to solve the problem with re-identification since it might serve as a safe haven for data controllers, who in case they would execute a solid anonymisation, would not need to worry about returning into the scope of the Directive. Today, when there is a constant risk of re-identification, all data, even when anonymised,[21] should be treated as personal data. If this is not true, such data controller processes data *contra legem*. Abovementioned provision would solve this problem. To meet this safe haven, the data controller would have to ensure that re-identification is massively time and money consuming, which would ensure a high level of privacy protection of data subjects.

---

17 Ohm 2009, 1738.

18 Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques. WP216. Online [10 April 2015]. URL http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

19 Act No. 101/2000 Sb., on personal data protection.

20 Explanatory note to the act No. 439/2004 Sb., act which amends act No. 101/2000 Sb., on personal data protection.

21 The word is used here in the sense of anonymisation techniques as presented by WP29 and Paul Ohm, that means a situation, when the data are modified in a certain way which disables identification, unless a high level of effort is put into the process of re-identification.

2.3 The Purpose and Consent Problem

[Rz 9] The second problem is connected with another two basic principles of European data protection system — purpose limitation and a strong role of consent. The fundamental idea behind these concepts is that if we are able to ensure that data is collected in a way which is not harmful, and if we are able to ensure that this status will not change until the end of data processing, then everyones privacy is safe. Purpose limitation is a strong principle arising from Art. 6/1/b of the Directive: «*Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.*» The requirement for specificity of the purpose can — on one hand — help data subjects in realising why their data is processed, on the other hand it prevents data controllers to set the purpose broadly and therefore new kinds of processing, which might be completely legitimate, reasonable and beneficial are precluded unless a new purpose is set and a new legitimate reason for data processing is found.

[Rz 10] This is closely joined with the consent of data subject with processing. Consent with processing is regarded as a tool by which data subject can knowingly establish whether it wants its data to be processed. In real life however, this does not properly work in the way the law supposes, because most of the data subject, if not all of it, just cannot deliver an informed consent.[22] Furthermore in case of the «Internet of Things», which is an unparching source of data for Big Data analyses, it is almost impossible to give consent with the processing.[23] The result of these overwhelming real world impediments is that aforementioned fundamental idea is discredited as it possibly might not serve the purpose for which it is present in the data protection legal framework.

3 Collision of the Law Enforcement with the Reality

[Rz 11] Personal data law enforcement bodies such as data protection authorities (DPA) and courts have to base their decisions on valid and enforceable legal rules. These rules have, as was shown, many fundamental problems arising from the times when they were designed. The nature of rules however does not justify situations when DPA and courts decide while neglecting important elements of the real life. An anecdotic example of that is a decision of the Czech Supreme Administrative Court,[24] which addressed to the Czech Office for personal data protection following: «*The explanation of the claimant, why the CCTV camera was aimed at the street and therefore recorded also entrance of the opposing house is wholeheartedly logical: should had been the camera cast down*

[22] See e.g. Solove 2012; Borgesius, Frederik J. Zuiderveen. 2013. *Consent to Behavioural Targeting in European Law — What are the Policy Implications of Insights from Behavioural Economics?*. SSRN Scholarly Paper ID 2300969. Rochester, NY: Social Science Research Network; Míek, Jakub. 2014. Consent to personal data processing — The Panacea or The dead end? *Masaryk University Journal of Law and Technology* 8. Masaryk University: 69—83.

[23] Peppet 2014, 140.

[24] Facts of the case are following: after a series of attack against his house and property claimant, Mr. Rynes, installed a close-circuit CCTV camera under the roof of his house in a way that it recorded public area in front of his house, a street from which the attacks were coming, with the entrance door of the opposing house. For that he was fined by the Office for personal data protection, a defendant in this case. The office reasoned its decision by the fact, that the camera was pointed to the public space and therefore it was infringing privacy of those who were using the street and entrance into the opposing building. (See CJEU Case No. C-212/13)

and was recording for example just a perimeter wall of the claimant's premises, its function would had been void, because it could never record a potential offender. If the defendant [the Office] «advises» the claimant otherwise, it is just a sad proof that it is utterly disconnected from the real life.»[25] Disconnection from reality, or neglecting of its parts is unfortunately a more general problem, which can be found even in the highest judicatory places.

[Rz 12] On May 13th 2015 the Court of Justice of the European Union issued a decision in the Costeja Gonzalez v. Google Spain case.[26] The court stated that the internet search engine is a data controller, in the meaning of the Data Protection Directive, for all personal data it indexes on the Internet and that indexing analysing and displaying data in the form of search results is processing of personal in the meaning of Art. 2/b of the Directive. This evaluation of the search engines nature was necessary for the so called «Right to be Forgotten», which is a concept taken from the proposal of the General Data Protection Regulation (GDPR).[27] It has been much written about the «Right to be Forgotten»[28] and it is not aim of this article to reflect on that. It must be noted, though, that establishing search engines as data controllers for indexed data do bring a whole set of duties hand in hand with rights for data subject. It is my impression that the Court only focussed on the rights[29] and neglected what duties should be fulfilled by law by the search engine operators.

[Rz 13] First, the legal reason for processing is Art. 7/f of the Directive according to the Court (processing is necessary for the purposes of the legitimate interests pursued by the controller). This is however possible only for «normal personal data». The sensitive personal data, which is defined by Art. 8 of the Directive as «*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*», and which is undoubtedly included in the processing carried out by the search engine,[30] cannot be processed on this legal basis. Art. 8 does not furthermore offer a possible legal ground, which could be used by search engine operators for legitimising sensitive data. Therefore the whole indexing and offering of search engine services is — in the view of personal data protection law — illegitimate, unlawful and should be ceased. This statement is valid also for other duties of the controller, which just cannot be fulfilled, like information duty.[31] There is no possible way how the informing of everyone, whose data is published somewhere on the Internet, could be carried out.[32] Unfortunately, there were published no official statements, which would clarify the

---

25 Paragraph 84, Supreme Administrative Court of the Czech Republic, case No. 1 As 113/2012 — 141 from 25th February 2015.

26 Court of Justice of the European Union, case No. C-131/12 from 13 May 2014.

27 It is necessary to note that in the Google Spain Case it is not *stricto sensu* a new right to be forgotten, but a combination of already existing rights of data subject, which are grounded in the Articles 12 and 14 of the Data Protection Directive. The «right to be forgotten» is just a catch phrase in this case.

28 Crowther, Hannah. 2014. Google v Spain: is there now a «right to be forgotten»? Journal of Intellectual Property Law & Practice 9: 892—893. doi:10.1093/jiplp/jpu148; Frantziou, Eleni. 2014. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. Human Rights Law Review 14: 761—777. doi:10.1093/hrlr/ngu033.

29 And on the fact that «privacy must be protected», which is basically the only argument supporting the Decision.

30 It is undeniable that somewhere on the internet are accessible information about racial or ethnic origin, political opinions, religious or philosophical beliefs or information concerning health or sex life. Once the search engine operator's indexing programs reach them, it is processing of sensitive data.

31 Articles 10 and 11 of the Data Protection Directive.

32 Míek, Jakub, and Jakub Harata. 2015. Analýza praktických dopad rozhodnutí Soudního dvora EU ve vci Google Spain. *Bulletin advokacie* 2015. eská advokátní komora: 30—34, 32.

situation, talk about factual problems the decision brought and offer solutions. Contrariwise, the document «*Myth-Busting: The Court of Justice of the EU and the Right to be Forgotten*»[33] was released by the European Commission, which serves as a non-critique glorification of the decision. There is a huge drawback of this approach. Now it is obvious that in certain cases the data protection rules are not enforced. Firstly, this leads to the lowering of the legal certainty of data controllers, who are knowingly breaking the law, because the only way how to not break it would be to stop their otherwise completely legal business, while hoping that the data protection authority will not fine them. Secondly, since enforceability of the law is one of the prerequisites of its effectiveness, this situation practically lowers data protection law effectivity. The CJEU undermined consistency and orderliness of data protection rules in a good intention of improvement of privacy. This naturally directly affects the personal data protection regime of Big Data as well.

4 Profiling, Big Data and Data Protection

[Rz 14] As was stated in the introduction of this article, the privacy protection cannot be completely left out. It is a hazardous idea and, at the end of day, not a solution at all. Without any regulation the situation could be much worse than it is now. Big Data analysis can pose a dangerous threat for an individual, regardless whether it is done by a private or public body. When data mining and big data analysis is done by the state, it can cause serious and irreversible damages for an individual. Furthermore, the individual might not even find out about that. Solove offers in his book «*Nothing to Hide*»[34] a good example of risks caused by the use of Big Data by law enforcement bodies.

[Rz 15] Profiling based on big data analysis can be seen as a good way for crime prevention, but it cannot be used without any checks and balances. The first problem according to Solove is inaccuracy of results,[35] by which is meant the fact that it is almost impossible to create a solid universal profile of a criminal. There are always many varying factors differing from case to case, therefore the profile must be flexible enough to cover the potential risk. This however trigger a large number of «false positives», that means people who fit the profile but who are not criminals and still would be exposed to restrictive measures without doing anything illegal.[36] Furthermore these people might never know that this profiling is going on, so they cannot defend themselves against it. They cannot raise a challenge, get their hearing and possibly correct false data. Solove calls this a problem of due process[37] and compares it to the situation of the main protagonist from Franz Kafka's book «*The Trial*». Solove continues: «*Kafka wrote about a hapless man who was arrested but never told the reason why. The man became obsessed with finding out more, including what was going to happen to him and how he could prove his innocence. Despite his efforts, he could never find out the charges against him, let alone refute them. Data mining can throw people into the same kind of bureaucratic morassthey are deemed suspicious but can't find out why and so can do*

[33] *Myth-Busting: The Court of Justice of the EU and the «Right to be Forgotten»*. European Commission, 18 September 2014. Online [10 April 2015]. URL http://ec.europa.eu/justice/newsroom/data-protection/news/140918_en.htm.

[34] Solove 2013.

[35] Solove 2013, 1186.

[36] Solove 2013, 188.

[37] Solove 2013, 191.

nothing to refute the suspicion.»[38]

[Rz 16] A similar problem can be found in the processing of big data done by a private company. In such cases it can lead to discrimination. Big Data analyses which involve consumers are mostly based on profiling.[39] It is a logical step made by the companies who try to focus on their customers and offer them what they want before they even know that. It is quite problematic not only in the case of profiles based on age, race, sexual orientation and other characteristics generally mentioned by antidiscrimination law, but also other profiling based e.g. on job or loan applications.[40] WP29 draws the attention to this problem in its Opinion 03/2013 on purpose limitation, where it briefly summarises that use of big data analytics may increase the economic imbalance between large corporation and consumers which could lead to unfair price discrimination with regard to the products and services offered.[41] A nice example of such profiling is offered by Jerome in his article: «*Take the example of an Atlanta man who returned from his honeymoon to find his credit limit slashed from $10'800 to $3'800 because he had used his credit card at locations where others were likely to have a poor repayment history. Is this a sensible decision for a credit card company to take, or does it remain somehow fundamentally unfair?*»[42] In this situation the data subject was harmed by a Big Data analysis he did not even know about, which is again very similar to the Kafka example mentioned above with the only difference that this time it is a private body who is making decisions.

[Rz 17] From the few mentioned examples it is quite clear, that the use of these privacy invading techniques must be done in the least harmful way possible. A possibly interesting solution offers Crawford, who tries to mitigate the harm done by big data processing and proposes a procedural data due process, which grants the data subjects certain rights to defend themselves even in the cases of processing done by private companies.[43] The process is constituted by the three following rights. There is the Right of Notice, which creates a duty for the controller to inform the data subject in cases when the data subject's privacy might be damaged by results of big data analysis;[44] the next is the opportunity for a hearing, which is connected with the right to correct wrong data;[45] and finally there is a right to impartial adjudicator and judicial review, which could correct wrongful processing. It is necessary to mention that Crawfords article is situated in American legal environment. These institutes are already incorporated in European data protection law, with the small difference that in Europe every data subject can benefit from these rights and not only those whose privacy might be damaged. WP29 suggests in its opinion in a similar manner that the organisations using big data for profiling and personalising of the services should disclose their decision criteria.[46] Another thing is, of course, how the law is enforced by data protection

---

38 Solove 2013, 193.

39 Murphy, Michael, and John Barton. 2014. From a Sea of Data to Actionable Insights: Big Data and What It Means for Lawyers. *Intellectual Property & Technology Law Journal* 26: 8—17, 14 (Murphy and Barton 2014).

40 Murphy and Barton 2014, 14.

41 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation. WP203. Online [10 April 2015]. URL http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, p. 46.

42 Jerome 2014, 222.

43 Crawford, Kate. 2014. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston College Law Review 55: 93 (Crawford 2014).

44 Crawford 2014, 125.

45 Crawford 2014, 125.

46 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation. WP203. Online [10 April 2015]. URL http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, p. 47.

authorities.

5 Adjusting Data Protection to Everyday Reality

[Rz 18] As was stated in the first parts of this article, the current European data protection legal regime, which is presumably the finest in the world and which sets data protection standards around the Globe, is far from perfect. However its existence helps to prevent harmful effects on certain kinds of data processing, since the companies and states do have to respect and obey it. Nevertheless there is much to improve. During the next few paragraphs, I would like to mention some possible solutions, which could bring nearer the ivory tower of law and the reality of new technologies, which are as easily applicable as possible.

[Rz 19] The first thing, which in my opinion could be improved, is the way how the legal provisions are interpreted by competent institutions and how well this interpretation is reasoned. It is understandable that the institutions want to retain the status of privacy and data protection as a display case of the European law. This can be seen for example in the importance on the right for personal data protection which is being laid by Court of Justice of the European Union. This process is easily visible in several past decisions[47] and their argumentation quality is quite disputable. For example, the Google Spain decision is based on the premise that a high level of protection must be ensured, and the argumentation almost stops right there. There is not included a proportionality test of any kind, nor is there even mentioned the colliding right for freedom of expression. More precise evaluating of the colliding rights and practical effects of decisions would surely help the cause of data protection.

5.1 Data Protection Granularity

[Rz 20] Introducing more detailed granularity of personal data definition, either by a legislative act or by imperative interpretation, is also a possible way which could be helpful. It could be beneficial to draw a distinctive line between «full regime» personal data and «light regime» personal data, which can be used for identification of a data subject only under certain improbable or difficult conditions, that means personal data with a low level of riskiness of abuse. This would lead to a beneficial situation, a creation of a new kind of personal data, with possibly lower legal requirements for their processing. It would unbind the current rigorous regime of data processing a little bit. It would allow processing of data which is now considered personal, but which is not dangerous for its subject. It would also solve the problem with failure of anonymisation. A good example of such data, which is by law personal, but which does not pose a danger to its subjects, is personal data of authors in the datasets of grey literature repositories.[48] The difficult question is how to connect legal certainty with certain necessary uncertainty of legal language?

[Rz 21] The answer could not lie in the altering of personal data status, but in altering of du-

47 E.g. C-293/12 *Digital Rights Ireland*, C-131/12 *Google Spain*, or most recent C-212/13 *Rynes*.

48 Myka, Matj, and Jaromír avelka. 2013. A Model Framework for publishing Grey Literature in Open Access. *Journal of Intellectual Property, Information Technology and E-Commerce Law* 4: 104—115, 109 (Myka and avelka 2013). Grey literature is that, which is produced on all levels of government, academics, business and industry in print and electronic formats, but which is not controlled by commercial publishers, i.e., where publishing is not the primary activity of the producing body (Myka and avelka 2013, 105).

ties of data controllers. Introducing new exemptions into the law, which would reflect the real demands of technical and practical possibilities, is also a possibility. After all, as can be seen on the example of the Google Spain case, the creation of new kinds of data controllers, which do not have to fulfil all legal duties prescribed by the law, is already happening. It has not just been codified yet. But it should be, the sooner, the better. These new exemptions can cover new legal reasons for data processing (e.g. the controller can process personal data, which can hardly be used for identification of a data subject), exceptions from information duty of controllers (e.g. when it is unreasonably difficult to inform the data subject about the otherwise legal processing) or exceptions from purpose limitation.

[Rz 22] An interesting solution might be to impose different duties on different data controllers based on their motive for data processing, as was suggested by Ohm. His article[49] is concerned primarily with anonymisation and de-anonymisation, but his approach can be used more generally to get granularity of duties. He writes: «*Rules governing what academic researchers can do with data should reflect the fact that academic researchers rarely desire to reidentify people in their datasets. A law that strictly limits information sharing for the general public [...] might be relaxed to allow researchers to analyze the data with fewer constraints. Of course, regulators should draw conclusions about motive carefully, because it is hard to predict who the adversary is likely to be, much less divine his or her motive.*»[50] An example of such lighter restrictions could be for example allowing to process personal data for different purposes than for which it was collected, or to provide such data to third parties, which would also be academic researchers. That however does not mean that other duties of data controllers and principles of data protection, like data security or data minimisation, should be abolished as well. On contrary, in the mentioned cases the principles of privacy by design and privacy by default should be strongly applied. This approach could serve well for the granularity of data protection duties, but it must be ensured that the lighter data protection regime would not be abused. This kind of granularity in data protection duties would be beneficial when properly balanced, because it would enable more free transfer of data and its use for new purposes which were not known at the time the data was collected, and from which the society can profit.

5.2 Consumer Protection as a Good Inspiration?

[Rz 23] As was mentioned before, the problem with the current data protection regime lays partly in the enforcement of data protection rules. Data protection authorities often cannot enforce offences just because of their workload and possible capacities. Individuals, whose privacy were damaged however, do not claim their rights at court quite often.[51] That can be understood as a sign that people generally don't want to take care of their data personally. As Solove puts it, what people want for their data, is «*to be collected, used, and disclosed in ways that benefit them or that benefit society without harming them individually. If people have an objection to certain uses of data, they want a right to say no. [...] They want to know that someone is looking out for their privacy*

[49] Ohm 2009.

[50] Ohm 2009, 1767.

[51] Munz, Martin, and Sylvia Lorenz. 2015. German Government Proposes New Law Entitling Consumer Protection Organizations to Enforce Data Protection Law. *White&Case*. February 16 (Munz and Lorenz 2015).

and that they will be protected from harmful uses.»[52] This concept is very similar to the consumer protection law, where the state guarantees that products which are sold and services which are offered to people are safe and fair. This is the direction that a German federal bill, presented in February 2015, took.[53] It is a proposal for an amendment of the German Act on Injunctive Relief, which, if it should be accepted by the German Parliament, would allow consumer protection associations and market protection associations to claim and enforce data protection law breaches with regard to the processing of consumer personal data. It is very probable that this step will lead to a growth of personal data protection claims at courts, and therefore a wider enforcement of data protection duties of data controllers which would cause a general improvement in the field of personal data protection and privacy as a whole.

6 Conclusion

[Rz 24] The aim of this article was to draw attention to some of the basic concepts, which serve as the roots of the current data protection legal framework, and which can cause a collision with the needs and possibilities of new technologies. It is necessary to find again a once lost balance between different interests of public and private parties, to find a balance between privacy and personal data protection and facilitation of technological development. The way how this balance can be reached might be a brand new system of privacy protection, but in my opinion the current situation can be improved within the now existing and functioning system. Amendments like increasing argumentation quality of the decisions issued by competent data protection authorities, introducing more granularity in data protection system — both granularity of personal data status and controller duties —and introducing principles of consumer protection into personal data protection legal area, can seem small at the first glance, but in fact, they can be quite effective due to the fact that they can be fairly easily implemented.

Jakub Míšek is a Ph.D. student at the Institute of Law and Technology, Masaryk University, Brno, Czech Republic. His main field of research is privacy and personal data protection.

[52] Solove 2012, 1901.

[53] Munz and Lorenz 2015.