Getting European data protection off the ground

Radim Polčák*

Summary

- No matter how hard one works designing an airliner and developing an excellent airframe, great avionics, and a beautiful cabin, the resulting outcome might not be able difficult to serve its purpose if it is built on a suspension of a car.
- In that sense, there is reason to believe that we have not just created such a machine by constructing the enormous regulatory and institutional structure of European data protection, but that we have also launched its mass production in the Member States. Now, we seriously speak about an upgraded model designed entirely in the same manner (ie the proposed Regulation).
- This paper tries to identify and discuss two general issues that fundamentally undermine the overall possibility of European data protective regulatory framework to actually get off the ground. First and the most important is the overall focus of legal regulation; second is the problem of the on-line applicability of European law.

Personal data is not 'it'

Even complex problems in law may have relatively simple causes. The existing data protection legal regulatory framework related to the protection of personal data as well as the draft Regulation generate countless particular problematic issues that can be analysed and discussed from a number of perspectives. However, I think one fundamental philosophical mismatch can be identified where most of particular problems of present and proposed data protection laws originate. In particular, I see the fundamental problem in the general contradiction between the phenomenological nature of information and the regulatory concept of personal data.

Information forms neither a tangible object of law nor it can be the subject of property of any sort.[1] Moreover, information cannot be objectivised by the law even in an intangible form; therefore, it does not have any relevant static existence.[2]

Information is a natural phenomenon whose existence can be determined only in relation to time. If information exists, the level of entropy of a system into which information is implemented tends to stay the same (irrespective of time) or even to decrease. Such an observation cannot be made for one given moment in time, because there is always a need to compare at least two situations distinct by time.[3] Information as such (in Kantian language *an sich*[4]) is thus a dynamic natural phenomenon. In the same way as we cannot objectivise and legally commoditise the 'sparkle of the water' or the 'freshness of the air',[5] it is naturally impossible to do the same to information.

* Doc. JUDr. Radim Polčák, Ph.D., is the head of the Institute of Law and Technology at Faculty of Law, Masaryk University, Brno, Czech Republic – radim.polcak@law.muni.cz.

1 The basis for a proper understanding of information as a natural phenomenon that is inevitably associated with the nature of life was laid down in the work of Erwin Schrödinger. Although Schrödinger did not explicitly name it, he pointed to information as the key differentiating factor in distinguishing between the 'physics' of living and non-living organisms—see E Schrödinger, *What Is Life* (Cambridge University Press, Cambridge 1992), freely available at <www.home.att.net/~p.caimi/Life.doc>.

2 Schrödinger's findings were further elaborated by the founder of cybernetics, Norbert Wiener. His works are based on three main assumptions, ie that information is the opposite of entropy, that life as a natural phenomenon is equipped with greater than a critical mass of information in order to keep organised, and that it is able to react to the course of time (and to subsequent changes of the environment) by producing sufficient amount of information—see N Wiener, *Cybernetics: Or the Control and Communication in the Animal and the Machine* (MIT Press, Cambridge 1961) 11.

3 One of most substantial empirical proofs of the fact that information is to be understood not as a static variable but as a procedure that can be determined only in relation to time was presented by Charles Darwin in his study about the timely development of living organisms—see Ch Darwin, On the Origin of Species By Means of Natural Selection, or, the Preservation of Favoured Races in the Struggle for Life, Project Gutenberg, 1998. Later, it turned out that the organising information is in this case is objectively expressed in the form of DNA.

4 Kant used the term 'Ding and sich' to indicate objective and absolute existence of things. 'An sich' in this case means existence per se that is not dependent on anything related to human perception. See I Kant, The Critique of Pure Reason (transl. Meiklejohn), Project Gutenberg, 2013, sec I. On Space, <http://www.gutenberg.org/files/4280/4280-h/4280-h.htm>. The term 'Ding and sich' is translated here as 'object without us'.

5 These terms were reportedly used by Chief Seattle when responding to proposed sale of the land of his tribe and aimed to demonstrate logical

Apart from the fact that one cannot determine or delimit the existence of information in a given moment in time, legal commoditisation of information is also made impossible by the fact that inevitable part of information is formed by its communication, meaning its potential availability or even the actual presence of information in some systems.[6] Consequently, information *an sich* is nothing more than statically undeterminable potential organisational effect that is made actual in the course of time depending on a number of criteria (while its mere quality is neither the only nor the most important of them).

It is, for example, absolutely impossible to determine what organisational value a DNA profile of a particular person has unless it is given a certain form of use or availability. As a result, one's DNA might be extremely valuable (in case it helps to save lives of other people) or totally useless or even harmful (in case its processing does not bring any other effect than burdening the processing facilities or harming the personal reputation of its holder)—all absolutely depending on the time and overall circumstances of its objective existence. Thus, while it does make sense to legally commoditise other forms of property due to the fact that there is always a possibility to determine or at least anticipate their factual static value,[7] it is absolutely useless to try the same approach with regards to information.

It obviously does not mean that it is impossible for the law to objectivise information at all—if it would be so, the law would not make sense, because there is no more important task for it than to promote and protect the ability of the mankind to produce information.[8] Although information cannot be legally approached *an sich*, it is still possible for the law to serve its primary purpose through objectivising the effects of information[9]; in particular, information that directly or indirectly affect individuals. It is, for example, possible to legally tackle the particular effects of the existence of personal data through factors like individual reputation, renown, attitudes, etc.

In this regard, there is a fundamental difference between the protection of privacy and the protection of personal data. Privacy is a concept that evidently has its determinable static existence—it is of an informational nature, but where privacy is concerned, the law does not try to focus on the mere information but rather on the effect of its appearance or availability on one's private life.[10]

It is also important that central focal point of a protective regulatory framework for privacy is a human and that the law is concerned only with the (negative) effects of information on the private life of a particular person.[11] Consequently, laws protecting privacy are not burdened by the aforementioned fundamental defect and, if designed and applied wisely as to their particular content, they might actually serve their purpose.

On the contrary, the protection of personal data is based on the commoditisation of information (into the concept of personal data) and consequently on the centrality of that data. In other words, the law in this case is not primarily about the rights of a person, but rather about rights associated with data (some of which are attributed to a person or a 'data subject'). The focus of the legal regulatory framework, namely the processing of personal data, regards only the effects of the processing of information as secondary or subsequent criteria.[12]

contradiction between the concept of property and the factual nature of the land—see PS Wilson, 'What Chief Seattle Said' (1992) 22 Environmental Law 1451.

6 Wiener gives mathematical explanation of the relation between time and communication of information in Wiener, *Cybernetics* at 60–94 (n 2).

7 See for example J Locke, Second Treatise of Government, Project Gutenberg, 2010, chapter V. <http://www.gutenberg.org/files/7370/7370-h/7370-h.htm>. One might argue that if Chief Seattle had known about Locke's work, he would have probably spoken in his statement against land as property a bit differently.

8 Despite, as Schrödinger explains in his aforementioned *What Is Life* (n 2), entropy is the second law of thermodynamics, and just as the primary concern should be in general heat (or energy), the primary concern of mankind has always been more specifically about information. Instead of taking any of sophisticated examples commonly used by sciences, we (lawyers) might simply argue in favour of that statement by hypothetic example of an intelligent and a stupid person. The intelligent one (i.e. the one able to create information) should regularly be able to obtain energy to survive.

9 This is why intellectual property does not commoditise information as such but rather its tangible and/or economic effects. Whenever the law tended to commoditise information *an sich*, it always resulted in paradoxes or inefficiencies as in the case of our contemporary understanding of copyright—see for example T Gillespie, *Wired Shut – Copyright and the Shape of Digital Culture* (MIT Press, Cambridge 2007) 242.

10 In that sense, understanding privacy as the 'right to be let alone' in its original sense seems very appropriate. Although this approach to privacy is popularly attributed to Warren and Brandeis, the term and the concept were not invented by them, but by justice Cotterell and referred to in second edition of Cooley on Torts. See L Brandeis and S Warren, 'The Right to Privacy', (1890) 4 Harvard Law Review 195.

11 The centrality of a person is a typical feature of Euro-Atlantic legal cultures. The fact that we call the rights of a person 'fundamental' and that we base our legal systems on them makes our legal cultures distinct from the rest of the world—see for example P Glenn, *Legal Traditions of the World* (Oxford University Press, Oxford 2004) 143.

12 There is a good reason to consider this situation a general conflict between the mere concept of data protection laws and the principles of internal morality of the legal system and to add this to the list of particular immoralities of data protection law that was earlier discussed with regard to Fuller's eight tests by Christopher Kuner in C Kuner, 'The "Internal Morality" of European Data Protection Law', November 24, 2008. <http://ssrn.com/abstract=1443797>. In that respect, it does not help much if the proposed Regulation mentions protection of individuals in its name or that it explicitly stipulates individual interests as core teleology of processing of personal data, while focusing in its content primarily on personal data and rights or obligations related to them (whereas a person and personal data

Consequently, there are very limited opportunities to remove the substantial functional defects that can be observed in the existing or proposed regulatory framework, unless the protection of personal data is primarily based on a procedural understanding of the effects of information on individual private life or on social interests,[13] rather than on statically protecting information *an sich*.

These all might seem difficult to achieve, as personal data are already being statically commoditised and traded, so reshaped laws would then seem to go against settled business practices. However, what are (and can be) bought and sold are not the mere data, but rather rights to process and utilise them in a specific manner in the course of time.[14] This would also mean that the physical existence of personal data *an sich* should not be problematic, as the primary concern would then be about forms of their use, or better said, rights to use them.[15]

For example, the protection software is also not in the first place about code being physically (statically) present on a machine, but rather about rights to use it. Despite the fact that the Court of Justice of the EU tends to think that the right business model is to sell or buy software similarly to sales of eggrolls,[16] the industry has already moved in a more natural way by promoting software as a service. Various protective externalities like digital rights management (DRM) do not focus on the mere existence of the code or on the number of its copies, but rather on forms in which the code can be used.[17] Similarly, privacy by design should be primarily about technical limitations on the use of data (not on their physical presence).

Death penalty for data: good and bad information

One of the particular implications of the aforementioned fundamental flaw concerns the right to erasure,[18] originally called the 'right to be forgotten and to erasure'. The general idea of forgiving through forgetting and forgetting through deletion[19] is based on the assumption that it is objectively possible to statically (or instantly) assess the quality of information and to even regulate its mere (physical) existence.

The proposed regulatory regime as well as recent case law of the Court of Justice of the EU is based on the proportionate balancing between reasons for deletion and reasons for existence of information.[20] While the reason for deletion is based entirely on individual factors (ie the will of the respective person a.k.a. the 'data subject'[21]), reasons for the existence of personal data are related to general considerations such as the necessity of data processing for historical purposes, freedom of information, or data processing in the area of public health.

It would be easy to criticise in this respect overly general nature of aforementioned terms. Yet, it is impossible to predict their scope and particular content, the indeterminate nature of which makes the entire regulatory framework anything but certain or predictable.

are obviously two different concepts). It is simply not possible to make direct implication in the sense that whenever one protects personal data, it always means protection of individual rights (the absence of this logical implication became obvious even in one of landmark data protection cases at ECJ, namely the 2003 Lindqvist judgment, C-101/01).

13 Definition of such interests can be based on the assumption that a use of personal data might lead not just to individual harm but also to significant unwanted societal effects—see for example D Hirsch, 'Is Privacy Regulation the Environmental Law of the Information Age?' in K Strandburg and D Raicu, *Privacy and Technologies of Identity* (Springer, Berlin 2006) 239–53. This aspect of data protection, ie protecting the social environment against possible or actual abuse of certain kinds of knowledge, for example, in the form of social engineering (similar to the case of protecting markets against the abuse of dominant market power) is, however, still neglected in the European law. See also J E Cohen, 'Examined Lives: Information Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373.

14 At the moment, data can be commoditised also thanks to the fact that consent can be understood statically, ie like 'giving data away'—see for example J Misek, 'Consent to Personal Data Processing – the Panacea or the Dead End?', (2014) 8 Masaryk University Journal of Law and Technology 69.

15 It is to be noted here that mere existence of personal data is never capable of causing any harm to the 'data subject'—it is always about some form of use of the data.

16 See the Case C-128/11 *UsedSoft GmbH v. Oracle International Corp.*, 2012.

17 For critical debate about DRM protecting copyrights, see for example J Cohen, 'DRM and Privacy' (2003) 18 Berkeley Technology Law Journal 575, and L Sobel, 'DRM as Enabler of Business Models: ISPs as Digital Retailers' (2003) 18 Berkeley Technology Law Journal 667.

18 See namely para 47, 48, 53, 54, 59, 83, and 129 of the recital, Articles 10a and 17 of the amended draft.

19 It is doubtful what in fact philosophically stands behind this right as to its fundamental teleology. The Christian right to be forgiven is one possible options, while there are a number of other ones, from property-like concepts of personal data to theories based on information self-determination or tautological self-evident theories. See for example J Ausloos, 'The "Right to Be Forgotten" – Worth Remembering?' (2012) 28 Computer Law & Security Review 143–52.

20 There is not much case law on this right, but in the landmark Case C-131/12, Google Spain SL, *Google Inc. v Agencia Española de Protección de Datos*, 2014, the CJEU clearly states in para 74 that there '[ap]plication of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter'.

21 The use of citation marks, whenever a 'data subject' is referred to, is meant to point out the strange situation that the legislative language seems for some reason to intentionally avoiding speaking about individuals, persons, or simply humans. The fact that we avoid speaking about people and rather invent a new formal term that by its definition cannot refer (sic!) to anything else but humans illustrates well the above-criticised fact that the processing of personal data is in fact not primarily about people but about their data. It might even induce thoughts about objectivising the data subject in the form that is picturesquely explained in Kafka's *Trial*—see F Kafka, The Trial, Project Gutenberg, 2012 <http://www.gutenberg.org/cache/epub/7849/pg7849.html>.

I think their use was inevitable in this case, as they aim to describe nothing less complex than the objective informational nature of personal data.

As claimed by the early cybernetics, 'information' can be defined as the opposite of entropy.[22] In regular language, we use the term 'information' mostly to indicate all sorts of instructions or data that are created, stored, or communicated in an objectively viewable form. However, only a very small part of those can be regarded as 'the' actual information at issue, as it in fact does not bring any decrease of entropy, but it rather increases chaos in respective systems (disinformation) or burdens their processing capacities (noise).

In that regard, it is extremely difficult to outline any criteria of how to actually determine whether the level of organisation of some system has increased or decreased. It is also extremely difficult to even find any logical or empirical method to distinguish in general between information and the rest (chaos or noise).

I used to think that although it is utterly impossible to determine informational nature of rules, it should be relatively simple to do the same with regards to statements. The reason was that with rules, we just speak about their validity, whereas the fact that a rule is valid does not tell much about whether it is actually good (ie organising). On the contrary, we assess statements as to their truthfulness and, following the ancient philosophers, we might think that true information simply must be good (ie organising).

Truth, however, does not seem to me to imply the informational character of statements. Apart from the fact that a substantial amount of statements cannot even be determined to be clearly true or false (take, for example, a statement like: 'I really like my mother-in-law' or 'a mole cannot fly'[23]), it is even possible to find a number of examples of perfectly truthful information causing chaotic consequences, particularly when people process information on an emotional rather than a rational basis. When it comes to one's health, beauty, love, or money, truth can actually do terrible harm.

In that situation, it is simply impossible to absolutely state that truthful information is good and a lie[24] is bad. Moreover, the inevitability of information is formed by its communication or availability in given circumstances. Consequently, a statement (true or false) can be organised if communicated to certain target audience at certain time, while it might be harmful elsewhere or at another time.[25]

When the law tries to strike a balance between the individual interest in the non-existence of information on the one hand and the public interest in the availability of organising information on the other hand, the use of extremely general terms is inevitable. In any case, neither the most beautiful or appealing names for the organisational nature of information nor herculean efforts to make them more particular and certain as to their meanings can provide for any useful substantial guidance as to the determination of whether some information should prevail over one's will to have it deleted.

This implies that the fundamental problem of the right to be forgotten or right to erasure is not in the fact that it is wrongly formulated, but that it is again based on wrong fundamental assumptions. Apart from the aforementioned faulty assumption as to the possibility to objectivise information, there is also the wrong assumption as to our ability to objectively determine the quality of data at a given moment of time and to immediately assess the proportionality of reasons to delete it versus the reasons to retain it.[26]

The jurisdictional game

Nothing in last two thousand years has brought more fun to international law than the introduction of the Internet. There are countless entertaining legal situations arising of the fact that information can move across jurisdictions with no costs, efforts, or even without anybody really noticing[27]—not to mention the fact that

22 See Wiener, *Cybernetics* at 11 (n 2).

23 This might seem *prima facie* to be a didactical illustrative example of a logically true statement. However, any golf green-keeper will confirm that if a mole enters her field, it will fly (and we can strongly believe that if it does, it will).

24 Let us call it in English deceit, deception, dishonesty, disinformation, distortion, evasion, fabrication, falsehood, fiction, forgery, inaccuracy, misrepresentation, myth, perjury, slander, tale, aspersion, backbiting, calumniation, detraction, fable, falsification, fib, fraudulence, guile, hyperbole, invention, libel, mendacity, misstatement, prevarication, revilement, reviling, subterfuge, vilification, whopper, or tall story.

25 This is perfectly illustrated by Giovanni Sartor and others in P Korenhof and others, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data' (13 May 2014), <http://ssrn.com/abstract=2436436>.

26 We have entirely omitted here another problematic assumption, ie that information can in fact be deleted pursuant to an authoritative decision. The fact that putting information on the Internet practically prevents its efficient removal was also noted by the ruling on an injunction in *Max Mosley v. News Group Newspapers* [2008] EWHC 1777 (QB). The court concluded that 'although this material is intrusive and demeaning, and despite the fact that there is no legitimate public interest in its further publication, the granting of an order against this respondent at the present juncture would merely be a futile gesture'—see J Oates, 'Max Mosley loses battle to get sex video off web', *The Register*, 9 April 2008, <http://www.theregister.co.uk/2008/04/09/formula_one_boss/>.

27 See for example U Kohl, *Jurisdiction and the Internet* (Cambridge University Press, Cambridge 2007) or D Svantesson, *Private International Law and the Internet* (Kluwer Law International, The Netherlands 2007).

with latest cloud technologies, it is becoming impossible to physically locate or localise information at all.[28]

Moreover, sovereign states have only very limited technical capacities to directly and, in particular, to control information networks, which means that it is hardly possible for them to exercise their jurisdiction over information traffic even when it is possible to localise information within their borders. Compared with the situation in the off-line space, states have neither the technical means nor the skills and competence to directly act on-line through their official bodies.[29]

If a state wants to exercise its sovereign powers, for example, over a driver of a car, it might directly do so through policemen who are technically able and legally empowered to stop the car, take out the driver, and do to her whatever corresponds to the official normative will. On the contrary, there is no such option for the case where a state would like to exercise its sovereign powers over a driver of a car, a dragon, Pegasus, or whatever is being regularly driven in the Second Life or the World of Warcraft. In those cases, there is simply no state official legally entitled and technically capable of doing so.

One might argue that states can still exercise their ultimate powers and forcefully implement their sovereign will also in the information networks, as everything what happens on-line always depends on something present in the off-line world. In other words, every line can be cut and every server can be blown out. That option, ie to physically enforce the normative will of the sovereign through off line violent means, would, however, always means such a brutal distortion of the network traffic that no state with one major exception[30] is really willing to regularly undertake it unless it might be of critical importance.

Given the nature of the Internet where everything happens through some service, it becomes obvious that the only efficient way of particular everyday enforcement[31] of sovereign will of a state on-line is through a service provider.[32] Consequently, only states that are in any way able to make service providers obey their sovereign orders can consider themselves factually sovereign in these territories (meaning not areas delimited by some official borders, but rather logically defined places controlled by respective providers).[33]

In my last book, I compared the factual regulatory regime of the Internet to the divine governance of ancient Greece.[34] Ancient Greeks believed that almost every piece of their physical world is governed by some kind of gods whose powers were limited to their respective vicinities. These gods always controlled specific areas or phenomena. Their powers differed greatly among one another and they even regularly overlapped. Yet while the gods had more or less extraordinary powers and abilities, their characters were rather human—thus, they often acted randomly, irrationally, or emotionally.

Poseidon, one of the most important of them, controlled the seas. If some states, of course purely hypothetically, would be able to exercise its jurisdiction over him, it would actually mean that it would be practically able to factually apply its sovereign powers not just within its borders but on the whole territory of the seas (including territorial waters of all other states).

The physical presence (the domicile) of the gods of the Internet was the original basis for the jurisdictional arrangements of the E-Commerce Directive[35] and the same jurisdictional model is partly used also in the draft Regulation.[36] On the contrary, it is also possible to understand the jurisdictional criteria in a way that theoretically provides for jurisdictional coverage of information society services by laws of all countries where such data originate or where they are physically present based on the criterion of the forum of the 'data subject'.[37]

28 In his Declaration of the Independence of Cyberspace, John Barlow wrote, addressing sovereign states on behalf of the on-line community: 'These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts'. The full text of the Declaration is available at <https://projects.eff.org/~barlow/Declaration-Final.html>. The jurisdictional challenge of 'spreading' information 'across the Planet' is obvious.

29 See for example R Weber, *Shaping Internet Governance: Regulatory Challenges* (Springer, Heidelberg 2009).

30 There is only one sovereign country able today to economically and socially exist without having to tolerate the existence and (at least some) use of the Internet within its sovereign borders; however, there is a reason to think that only a very few people, apart its own government, Dennis Rodman and the contemporary CEO of the Czech Railways (who has just been pictured with its flag-badge on his jacket), would actually like to live there.

31 It is to be noted that it is this everyday particular enforcement what probably makes law to actually exist in the modern Euro-Atlantic world. As long as the law cannot depend as to its existence on historically continuous and religiously established grounds of the sovereign power, it can rely (only) on everyday backing of its rules by some form of institutionalised enforcement—see for example N MacCormick, *Institutions of Law* (Oxford University Press, Oxford 2008).

32 See for example N Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 California Law Review 395.

33 See M Price and S Verhulst, *Self-regulation and the Internet* (Kluwer Law International, The Netherlands 2005).

34 See R Polcak, Internet a promeny prava (Auditorium 2012).

35 See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

36 See namely para 116, Articles 4(13) and 54a of the amended draft Regulation or Article 51(2) of the original Proposal.

37 This criterion is, similarly to the regulatory framework for distance consumer contracting, partly implemented in the amended draft Regulation when it comes to direct actions of 'data subjects'.

In data protection, the first approach based on the place-of-establishment principle makes operations of ISPs much more certain as to their legal regulatory regime and it also seems more efficient as to potential jurisdictional conflicts.[38] The latter approach seems to provide for a higher level of certainty to people (data subjects), as they can rely on 'their own' laws and procedures[39] despite what physically happens to their data. This approach also helps to prevent the emergence of safe harbours where data protection authorities tend to protect foreign investments over foreign personal data,[40] and also to prevent a situation when a state is factually (technically) deprived of its sovereign powers to regulate personal data that are being gathered or processed on its territory.

There are obviously many more reasons in favour and against both the aforementioned approaches. It is even theoretically possible to split the jurisdictional question according to the nature of the respective service or to its provider—one might then speak about, for example, a domicile-based approach for independent service providers, while controllers and processors of personal data can be under the regime of the country of origin of the data. In any case, the question of finding the jurisdictional silver bullet for the protection of personal data is extremely difficult and every new data-processing technology makes it even more problematic.

Having said that, I believe that the core of this particular problematic issue is, just as in the previous two cases, of a much more general nature. Not just transborder protection of personal data but a number of other generically similar problems like on-line betting, cross-border political propaganda, cyber-attacks, or even procedural issues related to e-discovery and the handling of electronic evidence show that there might be some common ground for all jurisdictional issues arising from the emergence of the Internet, and that it is related to the (non-factual) concept of information sovereignty.[41]

As noted above, the traditional concept of territorial sovereignty for various reasons simply does not work on the Internet. This obviously does not mean that there is inevitably a need to develop something entirely different to alter the territorial understanding of sovereignty. However, it does demonstrate that we need to think about sovereignty as an already virtualised[42] concept and to adapt our legal understanding accordingly. It means that there is a need to identify the core of the concept of sovereignty to analyse its non-essential formal aspects and to find out how they are changed when switching from off-line to on-line.

The resulting position with regard to the information sovereignty of a state can either be based on one of the two approaches. One is a bottom-up approach, ie on the implication that a state has sovereign power over information that it is physically and particularly able to get under its efficient control. This approach would be primarily based on the aforementioned theory of efficient off-line jurisdiction over the gods of the Internet and would practically end up in a search for legal justification of the existing factuality. Consequently, it would mean that, for example, Facebook would be regarded as US sovereign informational territory, with all the implied consequences that brings (such as an obligation not to meddle on the one hand and due diligence requirements on the other hand).

On the contrary, the top-down approach to the information sovereignty would be based on a traditional territorial understanding of sovereignty and would aim creating legal regulatory environment and factual arrangements that would let states efficiently exercise their jurisdiction over information that is in some manner linked to their territory, their citizens, or their general interests[43].

In any case, unless there is at least some general guidance as to the fundamental understanding of the concept of information sovereignty in the EU, it is impossible to find solid solutions for particular on-line jurisdictional issues including those arising from processing of personal data. In that respect, strong European pressure on extraterritorial application of its protective provisions

38 It also reflects the natural problém of clouds, ie the impossibility of determination of actual place of the data—see for example W Hon, C Millard and I Walden, 'The Problem of 'Personal Data' in Cloud Computing - What Information Is Regulated? The Cloud of Unknowing, Part 1' (2011) 4 International Data Privacy Law 211; Queen Mary School of Law Legal Studies Research Paper No. 75/2011, available at SSRN: <http://ssrn.com/abstract=1783577>.

39 It is to be noted that, despite the existing harmonisation, the substance of the protection of personal data still differs greatly among the Member States, not mentioning administrative or court procedures. See for example the Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments, Working Paper No. 2: Data protection laws in the EU, <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf>.

40 The reasons to believe that an example of this kind of case is the situation over Facebook's investment in Ireland can be found on the website <http://europe-v-facebook.org/>—the related case at the High Court of Ireland, ref. 2013 No. 765JR, has just been referred to the CJEU (the referring decision is available on-line at <http://www.europe-v-facebook.org/hcj.pdf>).

41 For the definition of the problem, see for example A Addis, 'Thin State in Thick Globalism: Sovereignty in the Information Age' (2004) 37 Vanderbilt Journal of Transnational Law 1.

42 By virtualisation, I mean here not the popular meaning of that word but rather the process that Piere Lévy explains in his book P Lévy, *Becoming Virtual – Reality in the Digital Age* (Plenum Trade 2002).

43 This approach is explained in the introductory part of the article by Wenxiang Gong. See W Gong, 'Information Sovereignty Reviewed' (2005) 14 Intercultural Communication Studies 119.

with regard to personal data that has led to legislative and even political developments at various parts of the world has already raised a number of general questions of international sovereignty.[44] Consequently, there is a reason to believe that data protection, despite (or maybe even thanks to) its substantive defects and contradictions, might represent a useful ground for further development of universally applicable concepts of information sovereignty that can be further used in order to resolve not just jurisdictional issues of data protection, but also those present in other fields of cyber law.

A pragmatic approach to jurisdiction

The game of virtualised sovereignty and Internet jurisdiction does not have to represent only a hardship or obstacle. Careful understanding of its rules might help not just in making the law to (finally) work on the Internet, but even to tackle some of complicated problems arising of cultural, political, and economic differences around the world.

At the moment, one of the most problematic issues of European data protection arises from the fact that it sets requirements that go far beyond standards and even technical and economic possibilities in other parts of the world. In result, nations outside the EU are not willing or are in a number of cases even not able to stick to these European standards. Even Europe, despite its economic and political strength, cannot then afford to impose any strict restrictions as to the intercontinental flow of personal data, so it leads into the situation where offshore governments pretend that the European standards are met and the EU pretends that it all works perfectly fine.[45]

The existence and efficiency of personal data protective instruments can be indicated by other factors such as by the number of enforcement cases and by the regular practice of the respective institutions.[46] One might think that if the same rules and enforcement standards apply, there should be a similar number of enforcement cases in any part of the world. Of course, there might be different causes for a lack of significant numbers of personal data protection investigation or enforcement proceedings. I tend to believe that the cause in this case is not that everybody is perfectly obedient to the rules and that no significant problems actually exist in offshore jurisdictions that would call for extensive penalties or draconic countermeasures.[47]

In this situation, ie when European law tolerates the existence of de facto double or multiple standards of protection,[48] it is difficult to argue towards controllers and processors who for some reason (still) keep their data in Europe that the obligations placed on them represents just a necessary minimum in social, political, and economic terms. If what European processors or controllers are required to do truly is a necessary minimum to protect fundamental rights of EU citizens, then it would seem that the EU should require that the same minimum standard should be obeyed also in the offshore processing of European personal data. If, on the contrary, what we have in Europe is not really the necessary minimum, then one might ask why the European controllers and processors are being so burdened.

In my very personal opinion, the situation in this case might be similar to the treatment of Russian tourists in fancy restaurants.[49] There are, on the one hand, standards of etiquette for expensive restaurants that to a large extent define these places and make them special. On the other hand, Russians have the reputation of being not entirely etiquette-obedient guests but excellent customers when it comes to spending money for extraordinary treatment. Consequently, there should be no place for noisy or improperly dressed guests in fancy restaurants, but having from time to time a bucolic party can be good for business. That, of course, applies as long as such events do not seriously harm or ruin the reputation of the restaurant—in that case, it would lose its regular etiquette-obedient guests, and I believe even its Russian clients as well.

With regards to European protection of personal data, the problematic question is how to enable certain

44 See for example C Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)', (2010) 18 International Journal of Law and Information Technology 176.

45 Compare for example the decisions on US safe harbour programme taken by the Commission upon Article 25(6) of directive 95/46/EC—<http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>—with the basis for possible claims under 18 U.S. Code § 1001 (also referred to as the False Statements Act).

46 See for example P Schwarz, 'The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harvard Law Review 1966.

47 For a typical example of the enforcement of the US safe harbour regime, see the recent settlement proposal made in a case of American Apparel, Inc. (file No. 142 3036), <http://www.ftc.gov/system/files/documents/cases/140507americanapparelagree.pdf>.

48 This is despite the fact that the Commission has had for a while a more than comprehensive analyses of the factual situation in a number of jurisdictions including the US. See for example the Communication Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf> (this analysis is, however, still very modest with regard to comparison of the EU and the US regimes or as to the analysis of compliance with them).

49 What I mean here by 'Russians' is beautifully explained in a column by Alina Rudya in the Kyiv Post—see A Rudya, 'Why Do 'Russian' Tourists Behave so Badly Abroad?', *Kyiv Post*, 11 February 2011, <http://www.kyivpost.com/opinion/op-ed/why-do-russian-tourists-behave-so-badly-abroad-35354.html>.

amount of not-so-obedient bucolic bacchanalia that are good for business, while still being able to argue to the majority of responsible guests that the haute etiquette represents in fact a minimum required standard.

In this respect, I think that issues of information sovereignty and jurisdiction may step in. When Dan Svantesson introduced his jurisdictional lasagne (originally called the 'layered approach'[50]), it was probably intended primarily to resolve a number of operational defects[51] in particular cases of extraterritorial application of European data protection laws. In my view, it can also be used as an example of wise legislative approach to tackling the aforementioned strategic political issues.

At the moment, we can choose between two explanatory statements regarding standards for offshore processing of European personal data, ie

1) European personal data are protected anywhere in the world to the same extent as in the EU.
2) European personal data are protected differently in the EU and abroad depending on the level of willingness and factual capabilities of offshore governments.

While the first statement is difficult to believe, the latter is difficult to swallow—in particular, for an EU-domiciled data processor or controller that is permanently subject to administrative duties, investigative procedures, or sanctions. In that sense, the proposed Regulation neither removes the fictive nature of the first, nor the political incorrectness of the latter.

I believe the adoption of Svantesson's approach might add a third version of an explanatory statement of offshore processing of personal data that might sound like the following:

3) European personal data are protected differently in the EU and abroad depending on the jurisdictional reach of the European law.

Instead of pretending that there is one European standard and it is (should be) applied worldwide or acknowledging the factual discrimination of EU-domiciled processors and controllers, the jurisdictional approach might provide for a pragmatic and fair solution. Pragmatic it would be namely because it would provide for a possibility of offshore data transfers that are, simply speaking, good for business. Fair it would be not just with regards to EU-domiciled data controllers and data processors who might finally feel privileged by being officially acknowledged under a regulatory regime with high standards (at the moment their official position is the same as of those domiciled elsewhere), but also to people (data subjects) who would have an official reason to finally stop believing that their personal data are protected offshore in the same manner as in the EU.

Conclusions

The aim of this paper was to point to two generally problematic issues behind the European protection of personal data that in my opinion represent the core of most of particular defects of both the existing regulatory framework and the proposed Regulation. The first issue relates to the general teleology of European data protection that is primarily focused on data and their processing, while data itself are understood as a static, property-like category. In that respect, I tried to argue that very primary focus of the law should not be data or their processing but a person (a.k.a. 'data subject'), and that fundamental rights should not be protected through the protection of personal data but otherwise. In connection with that, I tried to argue that rather than focusing on a static understanding of data and their processing, we should focus on a procedural understanding of the effects that the processing of personal data actually has on individual and social interests.

As to the operational mode of the European data protection regulatory framework, I discussed the problem of cross-border transfers of personal data and the fact that there are multiple standards of protection. This issue could be resolved in a number of ways, but I argued for at least an attempt to try to find first some general guiding concept of information or on-line sovereignty grounded in public international law and to adopt the subsequent cooperative or harmonising efforts accordingly, whether for personal data, on-line gambling, cybercrime, or anything else. Consequently, I expressed an opinion that a jurisdictionally centred approach might work well in order to pragmatically enable the international flow of personal data, while providing for fair and reasonably arguable rules for their protection.

doi:10.1093/idpl/ipu019
Advance Access Publication 12 September 2014

50 See D Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3 International Data Privacy Law 278.

51 For an explanation of the operational mode of law and its distinction from other modes, see for example A Schmidt, 'Radbruch in Cyberspace: About Law-System Quality and ICT Innovation' (2009) 3:2 Masaryk University Journal of Law and Technology 132.