Gizem Gültekin-Várkonyi[1]

Life after the GDPR: Dreaming of a Uniform Application

Like the oil-rich countries, the data-rich countries or companies, even individuals who invest in technologies that could collect and manage data are the most powerful today, and they certainly will be in the future. If we look at some of the largest and most valuable companies in the world[2], we will easily realize that first they are either American or Chinese tech companies, and then they are the ones who have sufficient tools and technologies to collect and manage data. Their continuous investment in such tools as Artificial Intelligence has been a real game changer for them. Examples of such companies could be Facebook, Alibaba, Amazon or Google.

People voluntarily and freely contribute to the world of personal data through their social media accounts, web browser, the transactions they make electronically shopping online. They leave their digital fingerprints in every corner of the virtual world where it does not matter who they are but what data they are represented by. They post wherever they are, whatever they eat, their taste in movies, political views, health-related issues, or they even post their pictures showing all biometric features, videos disclosing their voice, and so on.

As a result of such constant contributions, all that needs to be done by action-ready entities is to analyze that data to offer more personalized

1 Information Management BA and International Relations MA. PhD student, University of Szeged, Faculty of Law and Political Sciences.

2 https://www.forbes.com/powerful-brands/list/#tab:rank Last accessed: 16 December 2018

services fitting people's preferences the most. Be it companies or governments, these entities have already realized the power of the data to predict, to profile, and to manage people's behavior. The most interesting in this story is that people do not really know about the existence of these practices or about the consequences of this fact, the fact that is called "datafication"[3].

What might be the consequences of such datafication? Certainly, people would like to enhance their life by receiving personalized healthcare services which must be uniquely offered in accordance with their own health status. People surely would like to get tips for their financial arrangements or would like to express their political opinions, because we are still humans, and we live in environments where we communicate with humans.

Freedom of speech, freedom of thought, our right to access to medical assistance and many such fundamental principles are basic values of our democratic societies. However, unfortunately in practice, we are faced with some issues that affect our life to the core, and I must stress that there are issues that we are not yet aware of. Some, of course, we are already aware of like the Snowden revelations or the Facebook-Cambridge Analytica scandal (the Wylie revelations, as we prefer) but these only prove how far surveillance could extend through manipulating people's political choices, collecting and transferring their data somewhere out of their knowledge, or refusing their credit application just because they live in a poor area of the city. All these issues clearly reflect that there are cases in which people are decided about by processing their data outside of the scope of legally specified purposes, and without their knowledge, in a way that could do harm to both the individual and the society.

To battle all of these still dangerous trends and issues, data protection was one of the fundamental rights that was first recognized in

3 Mayer Schönberger, V., Cukier, K. (2013), Big data: A revolution that will transform how we live, work and think. London: John Murray.

Europe in the 1970s. Sweden was the first country adopting a national law on protecting personal data in 1973. Council of Europe's Convention 108[4] (on the protection of personal data against computerized processing of personal data) was signed and ratified in 1981 by most of its Members, and today, its scope has become wider since countries such as Argentina, Mexico, Tunisia, Senegal also signed it. These countries voluntarily choose European data protection rules for their citizens although they are far from Europe geographically. Although most of the EU Member States already adopted data protection rules similar to the Swedish Data Protection Act and/or Convention 108, the adoption of the Directive 95/46/EC[5] (as an "updated version" of Convention 108), created the basis for the European Union way of data protection. Strong data protection rules have been developed since then and today, Europe and the EU is in such a position where its legislation has been taken as a guidance not only by most of the European countries, but also globally.

The EU especially tried to construct one of the strongest data protection laws in the world. However, there is still a need for balanced protection, especially in light of such well-referred exceptions as national security, where the EU sometimes lifts its own legal instruments whenever a controversy between the right to data protection and some compelling Member State objectives arise.[6] The invalidation of the so-called Data Retention Directive in 2014 could be one of the most significant

4 ETS No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981. Convention 108 has been updated on 18 May 2018. The updated text reveals many similarities with the GDPR such as, requirements for obtaining consent, right to not to be subject to a purely automated decision, references to the Data Protection by Design rules, etc.

5 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

6 Ojanen, T. (2014). Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, 10 EuConst 528.

examples to this. In that case, the Court of Justice of the European Union did not fear to decide in favor of data protection rights of individuals even if it amounted to invalidating an agreement between the EU and the US, two strategic, political, and trade partners. As it is referred in many papers within this book, the Schrems case invalidating the Safe Harbor agreement between the EU and the US enabling legal flows of personal data between the two, could be another example.

All these issues caught the EU lawmakers' attention and they decided to comprehensively update EU data protection rules. Since the GDPR was drafted in 2016 and entered into force on 25 May 2018 they are "market leaders" in this field. Targeting uniform application in all twenty-seven Member States is a commendable vision but since every Member State has its own approach to interpret the privileges of the GDPR, it might prove harder than it seems. In this paper, we would like to shortly highlight some of the novelties of the GDPR, then introduce the meaning of the Regulation in the EU legal sphere. Finally, I will discuss the chances of the uniform application of the Regulation by using Sweden as an example. The Swedish case is particularly worth examining further because of the country's well-known American-type liberal approach to data-based market and economy which is, if not fully, contradictory to the EU's rights-based approach. In the view of such an approach, we could easily realize how the GDPR could be circumvented by some Member States interpreting the exemptions in a broad sense.

The Nature of Regulations in the EU and the Novelties of the GDPR

First of all, better protection for individuals by broadening interpretation of already existing principles and the introduction of new rights for them to tackle the problems raised by technological developments are certainly key novelties of the Regulation. The right to be forgotten

or right to erasure, strengthened consent rules and the right to request a copy of personal data processed are just some further examples of the improvements brought about by the GDPR. All of these stronger rights for data subjects and the obligations imposed on data controllers could be called as "GDPR direct effects on individuals", which also shape the specific legal nature of the Regulation as part of the EU legal order.

The EU is a unique supranational entity both from the aspect of its construction and its procedures. One of the reasons for its uniqueness admittedly is its legal construction and its effects on the Member States. The EU operates based on the founding treaties, which provide the general framework of its scope of action and where the Member States are bound to implement and apply EU legal acts.

The founding treaties and their amendments are the primary sources of EU law. Secondary sources consist of several other legal instruments based on the founding treaties and on the top of their hierarchy, regulations are those legal acts that are directly applicable, i.e. they do not have to be transposed into national law, but enforced as national law.

Article 288 of the TFEU confirmed former Article 189 of the EEC indicating and states that *"[a] regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States*." In interpreting the treaties, the CJEU created a case law, based on which where MS failed to apply regulations it was said that Member States do not have a room for maneuver to apply them partially or apply as they wish. In a preliminary ruling case referred on 14 December 1971 by *Politi s.a.s. v Ministry for Finance of the Italian Republic*, the *Tribunale civile e penale di Torino* referred a question to the Court of Justice whether particular articles in Regulation no 121/67/EEC of the Council of 13 June 1967 on the Common Organization of the Market in Pigmeat[7] *"are immediately applicable within the national legal system*

7 Regulation No 121/67/EEC of the Council of 13 June 1967 on the common organisation of the market in pigmeat

and, as such, create individual rights which national courts must protect".[8] The Court answered by referring to the Article 189 of the EEC and indicated that *"by reason of their nature and their function in the system of the sources of Community Law, Regulations have direct effect and are as such, capable of creating individual rights which national courts must protect. Court further referred to the effect of a Regulation which "prevents the implementation of any legislative measure, even if it is enacted subsequently, which is incompatible with its provisions"*. In another case, *Commission of the European Communities v Italian Republic*, the Court of Justice drew the attention of the Italian authorities to the fact that a Member State cannot opt out of Regulation provisions and Regulations are effective from the date they were published in the Official Journal[9]. This is a particularly important case since it highlights that obedience to regulations is important from the date of their publication[10].

Prior to the GDPR, the EU's data protection legislation was guided by a "softer form" of an EU legal act, Directive 95/46/EC. Unlike Regulations, Directives are "softer" due to their importance in securing the uniformity of the EU law, giving a certain margin of appreciation to the Member States to implement the regulatory objectives specified by the Directive. Its initial purpose is harmonization of EU law, not unification, being the ultimate aim of Regulations. Article 288 of the TFEU states that *"[a] directive shall be binding, as to the result to be achieved,*

8 61971CJ0043, Judgment of the Court of 14 December 1971. - Politi s.a.s. v Ministry for Finance of the Italian Republic, ECLI:EU:C:1971:122

9 61972J0039 Judgment of the Court, 7 February 1973. - Commission of the European Communities v Italian Republic. Premiums for slaughtering cows. - Case 39-72.

10 Indeed, the Commission could monitor the Regulation's application status in case the Member State is fully ready to implement, but first, the Commission needs a well-founded suspicion before referring the case to the Court. Finally, we think that it is practically impossible to check every Member State on a daily basis whenever a Regulation or any other legal instrument is adopted.

upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"[11].

This distinction is very important in the legal force of data protection rules as well. Practically, under a directive, we would find 28 different ways of implementation, but topics subject to a Regulation are applied "as is". Regulations are strong legal acts and increasing the force of privacy protections and personal data protection was undoubtedly one of the reasons why Directive 95 was switched to a Regulation. It was important to take this step, especially since China and US data protection challenges the EU's approach from several points.

Before the GDPR, some Member States had stricter data protection rules than others. Traditionally, Germany and Austria are known of their stricter data protection regimes than those of Ireland, Italy and Romania. Indeed, it is not a surprise that the European headquarters of some of the tech giants (Facebook, Google) were all settled in Ireland. Most of the Member States were not taking the right to data protection into account in their political discussions, awareness regarding data protection issues was low.[12]

Hoping the GDPR would open a new blank page in the European way of unifying data protection rules, I still think that a completely uniform application of the GDPR practically will not be possible, at least in the near future.

Switching from a Directive with twenty-three years of practice (with low general awareness standards) to a Regulation in two years' time is not an easy task for the Member States. In the practices that developed in implementing Directive 95/46/EC exceptions and solutions unique to the Member States have been created, and now a global change of mindset is required. I would like to illustrate this with the Swedish example.

11 Becker 1982 Tobler C., Beglinger, J. Essential EU Law in Text, Lap- és Könyv Kiadó, Budapest, 2010. p.43 Van Duyn case; Judgment of the Court of 4 December 1974. Yvonne van Duyn v Home Office. ECLI:EU:C:1974:133.

12 Custers, B., Dechesne, F., Sears, A.M., Tani, T., van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, Computer Law & Security Review 34, 234–243.

The Origins of Data Protection Law in Sweden and the Swedish Path to the GDPR

Sweden is the first country in the world that adopted a national personal data protection law, the Data Protection Act, in 1973.[13] There were huge differences between today's data protection legislation and the laws of that time. Today's technology is completely different than the technology in the 70s. Computerized processing of personal data only became an issue underlying Convention 108 (as we have seen above) in the 1980s. In the Sweden of the 1970s, data could be processed only if the Swedish Data Protection Board (*Datainspektionen*) would give permission to the data controller[14]. The Swedish Data Protection Act was updated from time to time with minor changes, but a comprehensive revision occurred when Sweden became an EU member in 1995. Until the adoption of the GDPR the amendments continued, but it certainly has brought the biggest change in Swedish data protection legislation.

The Swedish Data Protection Act – although the oldest – was very general in its scope which was made whole through sector-specific legislation on data processing. As a result, there were different data protection laws in different fields such as healthcare,[15] crediting,[16] electronic

13 Technically, historical record shows that the German Land of Hessen has indeed put in place a „national" data protection law in 1970, but due to the federal structure of the German State it is not considered hereby as a „national data protection law". The German federal Datenschutzgesetz (which now qualifies as a Member State regulation) was finally adopted, based on the Hessen example in 1978, thereby became only the second „national data protection law" to be adopted for the purposes of the above historical description.

14 Öman, S. (2004) . Implementing Data Protection in Law, in IT Law, Wahlgren, P. ed., Scandinavian Studies in Law, The Stockholm University Law Faculty, 47, pp.390-403, p400.

15 Patientdatalagen (2008:355) (Patient's Data Act).

16 Kreditupplysningslag (1973:1173) (Credit Information Act).

communications,[17] camera surveillance[18] and so on, making up a "complex system".[19]

Although Sweden was the first to have legal protection for data protection rights of individuals, its approach to the subject was criticized several times. A report published by the Human Rights Committee comprising representatives from Privacy International, Civil Rights Defenders and DFRI (*Digital Freedom and Rights Association or Föreningen för Digitala Frioch Rättigheter*)[20] states that the Swedish Act on Signals Intelligence in Defence Intelligence Operations[21] gives power to the Swedish National Defense Radio Establishment to collect data from transnational communications through analyzing search terms of groups of people from different nationalities. However, practice shows that only a small percentage of collected data is relevant to the targeted aim (national defense). Furthermore, it was reported that the Act was unclear on the parties that were legally authorized to collect data, and both the State Inspection for Defence Intelligence (i.e. the oversight mechanism for intelligence-related data protection) and the Defence Intelligence Court which authorizes data collection for intelligence, were found lacking independence and transparency. This example is important to understand how legal exemptions could sometimes cause conflicts.

The following example presents how some of the Swedish actors in the data protection field may mistakenly interpret the essence of the regulation which may cause the misapplication of the GDPR. In a report discussing protection of personal health related data, it was referred that health data is being collected and stored in medical devices

17 Lag (2003:389) om elektronisk kommunikation (Electronic Communications Act)
18 Kameraövervakningslag (2013:460) (Camera Surveillance Act)
19 Öman, p.400.
20 https://privacyinternational.org/sites/default/files/2017-12/HRC_Sweden_0.pdf Last accessed 25 November 2018
21 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet

in Sweden by the Swedish Management Network for Biomedical Engineering[22] within the framework of the Swedish Patient Data Act, the Patient Safety Act and the Medical Devices Act. However, since these acts did not use a uniform definition of "medical device data" which is almost any data about a patient collected by devices, Swedish people's data protection right was not fully protected.

Also, the above-mentioned Acts had different approaches and sometimes very narrowly tailored (legal and other security) measures to protect such data. As a result, besides security- and technology-related recommendations, the Swedish Management Network for Biomedical Engineering proposes to harmonize the examined Acts with EU personal data protection legislation. As indicated in the report, *Datainspektionen* was the only opposing party to this statement, and I think that it is most probably because the wording "harmonization" was used instead of uniform application.

Now I will try to explain how the GDPR may be a challenge for Swedish courts regarding to the country's traditions of a differently balanced data protection culture.

The Swedish Data Protection Act was updated based upon the GDPR and the new legal text was prepared on 19 April 2018, and following adoption, it entered into force on 25 May 2018. Sweden is one of the countries that did not miss the GDPR's *de jure* enforcement deadline. In her article, Jonason (2018)[23] comprehensively explains Swedish path to the GDPR. About two months after the GDPR was officially announced

22 The Swedish Management Network for Biomedical Engineering, The Swedish Patient Data Act in the clinical everyday- What demands are made on medical devices? Condensed Report Part 2: Application of information security in medical devices and systems 30 September 2016 English version 23 October 2017 http://www.lfmt.se/Filer/SI-forum/uppladdade%20dokument/LfMT%20-%20The%20Swedish%20Patient%20Data%20Act%20in%20the%20clinical%20everyday%20-%20Condensed%20Report%20Part%202%20-%20171023.pdf

23 Jonason, P. (2018). The Swedish Measures Accompanying the GDPR, in Mc Cullagh K., Tambou O., Bourton S. (Eds.), National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg February 2019, 130 pages. Available at: https://wp.me/p6OBGR-3dPp.6.

in the EU's Official Journal, two groups were assigned by the Swedish Government to prepare Swedish legislation for GDPR: Data Protection Inquiry (DPI) for preparing the legal provisions and a Data Protection Committee (DPC) for discussing the questions related only to institutional construction. DPI comprehensively examined the GDPR and drafted the first version of the new Act in May 2017. After the ordinary consultations and revisions, the Swedish Parliament adopted the new Data Protection Act. Jonason[24] notes an important point from the DPI's report that they did not have enough time to examine all the aspects in a deeper manner which may have amounted to better differentiations in the Act.

Jonason's further analysis points to Sweden's unique approach to the GDPR in cases where the right to data protection and freedom of expression need to be balanced.[25] Processing of personal data based on solely journalistic purposes which was an exemption under Article 9 of Directive 95/45/EC, which still is under GDPR Article 85, is interpreted in Sweden in the broadest sense. The Swedish Constitutional Court decided in one of its judgments[26] in favor of the petitioner who published some bank employees' personal data on a website to prove malpractices in the Swedish banking system, and stated that this act was based on a journalistic purpose, i.e. to inform the public. The Swedish Supreme Court (Högsta domstolen) interpreted the case based on the ECHR and the case law of the ECtHR. Although *Datainspektionen* criticizes the Court's decision, no further steps were taken.

From the point of view of the Court of Justice, Sweden's data protection approach that is more expression- and press-centric may not be acceptable. In *Dennekamp v European Parliament* where Dennekamp (a Dutch journalist) asked for MEPs' pension scheme documents, the

24 Ibid., p.43

25 The first Freedom of Press Act dates back to 1776 in Sweden.

26 Case B 293-00, judgment of 12 June 2001, Referred from, Bygrave, L. (2002). Data Protection Law —Sweden: Balancing Data Protection and Freedom of Expression in the Context of Website Publishing — Recent Swedish Case Law, Computer Law & Security Report, 18 (1).

CJEU rejected any claims to providing the documents stating that the MEP's personal data cannot be transferred without a clear expression of necessity. Based on the very clear logic of the existence of public interest information, the applicant claimed that those documents are important *"for European citizens to know which MEPs had a personal interest in the additional pension scheme when called upon to take decisions regarding its management"*[27], and accessing personal data in the documents is necessary in line with the right to information and the right to freedom of expression which could serve for European citizens to see *"how public money was being spent, on the possible impact of private interests on the voting behavior of the MEPs and on the functioning of control mechanisms"*, but the Court still did not annul the decision of the EP which found applicant's statements unconvincing in their examination of necessity.

Finland, EDPS, and as expected, Sweden (intervening) were in favor of the applicant, reporting that the documents could serve transparency of the EP and MEPs. The case shows how the CJEU and Sweden reflect divergent positions about interpreting the right to information and the right to freedom of expression, and transparency of public institutions.

Obviously, the Swedish legislator updated the Data Protection Act in a way that the GDPR still cannot precede the Freedom of the Press Act and the Fundamental Law on Freedom of Expression. Although Swedish *Datainspektionen* warned the Swedish Government (*Regeringskansliet*) about the fact that Regulation is one of the legal instruments of the EU which shall be directly implemented, it was not taken into consideration. However, and evidently, Swedish lawmakers were already aware of this situation since an explanation was delivered regarding the judgment stating that *"previous provision of the Personal Data Act with a similar content had not been the subject of legal challenges nor*

27 Case T-115/13, Judgment of the Court of 15 July 2015, Gert-Jan Dennekamp EU:T:2015:497

had it been questioned by the European Commission during its 20 years of application"[28].

If these statements remain same for the next couple of years, and if Sweden will not be referred to the CJEU for breach of EU law by the Commission, then we should not even wait for robots to come alive to question the uniform application of GDPR in practice. Some countries like Sweden already interpret the Regulation in their own way.

Another example could help to illustrate the situation further[29]. In Sweden, the owner of a publicly available database may get a publisher's license which then will enable them to protect and control the content they publish. With this license, they can import personal data such as phone numbers without consent. Since Swedish law puts the GDPR in a weaker position in case of a conflict with freedom of expression, database owners take this opportunity to build their own databases full of personal data collected without data subjects' knowledge.

One more point in the assessment of the above-cited Jonason shows how the Swedish point of view of the GDPR is different from the spirit of the law itself. As she argues, the Swedish legislator shaped the Data Protection Act in such a way that it is not "abuse-centric" but opts for a "regulatory model" which means that some of the data breaches may be tried to be repaired through retrospective inspection. Government's notification taking into account that deciding on the violation should "not [be] based on the release itself but after the release" is evident[30], pointing its opinion as a later on response to the breaches of rights of data subjects. However, once data is made available out of data subject's consent or knowledge, even though it happens accidentally, it is almost impossible to take an ex post action to remove the negative effects. Such

28 Jonason, p.6.

29 Meyer, D., Sweden's open society is clashing with EU privacy law, and regulators are frustrated, 22 May 2018, IAPP. Available: https://iapp.org/news/a/swedens-open-society-is-clashing-with-eu-privacy-law-and-regulators-are-frustrated/

30 Swedish Government Official Report SOU 2017:52. Referred from, Storr, C., Storr, P. (2018). Sweden: Quantitative (but Qualitative) Changes in Privacy Legislation, 4 Eur. Data Prot. L. Rev. 97

statement also goes against the much-desired logic of Data Protection by Design which requires proactive or ex ante action rather than retrospective measures in protecting privacy.

Storr and Storr[31] refer to the previous Swedish Data Protection Act and argue that it seems stricter than the updated one since the Swedish legislator (*Riksdag*) chose to apply loosened rules of consent, data minimization and purpose limitation for personal data[32]. Finally, the Swedish legislator's opposition to *Datainspektionen* contains some messages reflecting on the future Swedish application of the GDPR. For example, when *Datainspektionen* raised its voice several times on several topics, from lowering the age limit for a child's consent from fifteen to thirteen[33], and warned the lawmaker regarding the way they try to interpret the GDPR, it was not taken seriously by the legislator.[34] This approach shows how authority of a National Supervisory Authority whose competences increased in the GDPR could be shaken even more drastically in the future.

Based on the above statements, Sweden had some problems with interpreting Directive 95/46/EC, and has some obstacles with understanding the GDPR, and finally, the sector-based practices where the Swedish Data Protection Act was excluded could sufficiently and comprehensively cover the issues.

31 Ibid., p102.

32 Ibid. 97. Authors call such data processing "unstructured" which is a term derivable from Article 4 (6) of the GDPR giving the definition of 'filing system': *"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."* It seems that the Swedish legislator thought that if there was a structured set of data, then there must be unstructured data too, so such data should be exempted from the scope of the GDPR.

33 Ibid. p,100

34 Jonason, p.7

Conclusion

The GDPR is the most up-to-date legal document on data protection introducing new rights for data subjects, as well as introducing new rules and obligations to data controllers. Member States of the European Union have a duty to ensure GDPR's full application, but first, they must adopt it in accordance with the spirit of the Regulation.

Unlike Directive 95/46/EC, the GDPR does not leave room for so many different interpretations and implementations. As the Swedish example reflected above, Member States' specific traditions and implementations hedge off the demanded uniform application of the GDPR, although it offers **Good Data Protection Rules** for the data controllers and **Good Data Protection Rights** for EU citizens.