Balkan Journal of Social Sciences

BJSS

Derginin ana sayfası: https://dergipark.org.tr/bsbd

Araştırma Makalesi ● Research Article

General Data Protection Regulation: A Transformative Law

Genel Veri Koruma Düzenlemesi: Dönüştürücü Bir Yasa

Hassan SYED [a], Sema YILMAZ GENÇ[b]

[a] Dr., BPP University, Islamic Finance Law, London, UK, h.syed2@my.bpp.com, Orcid:0000-0003-2114-2473
[b] Assoc. Prof. Dr. Kocaeli University, Marketing and Advertising, Kocaeli, Turkey. semayilmazgenc@gmail.com, Orcid: 0000-0002-3138-1622

MAKALE BİLGİSİ

Makale Geçmişi:
Başvuru tarihi: 28 Şubat 2020
Düzeltme tarihi: 30 Mart 2020
Kabul tarihi: 15 Nisan 2020

Anahtar Kelimeler:
Veri
Kişisel Veriler
Veri Hakları
Kimlik
GVKD

ÖZ

Bireylerin kişisel verileri, 1940 Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi'nden bu yana uluslararası hukukun merkezinde yer almıştır. Bu haklar, İnsan Hakları Evrensel Bildirgesi'nde vurgulanan diğer kişisel haklarla iç içe geçmiştir. Avrupa Birliği (AB), bütün bir kıtanın bir topluluk oluşturmak üzere bir araya gelmesinin eşsiz bir sosyal örneğidir. AB Hukuku, AB Üye Devletleri'nin yerel yasaları üzerinde üstünlüğe sahip uluslarüstü bir hukuktur. AB, insan onuru ve hakları ile ilgili yasaları yapma konusunda hep ön planda yer almıştır. AB Haklar Şartı, Madde 8'de kişisel verileri bir temel insan hakkı olarak tanımlamaktadır. Avrupa İnsan Hakları Sözleşmesi ise, kişisel veri hakkını kişisel özgürlüklerin bir parçası olarak tanımaktadır. AB Genel Veri Koruma Düzenlemesi, Mayıs 2018'de yürürlüğe girmiştir. Yürürlüğe girdiğinden bu yana dönüştürücü olmuştur. Bu çalışma, Avrupa Mahkemelerinin İçtihatları çerçevesinde Genel Veri Koruma Düzenlemesi'nin dönüştürücü niteliğini vurgulamaktadır. Çalışma ayrıca, kimlik ve vatandaşlığın veri koruma haklarını daha geniş kavramlar altında ele almaktadır.

ARTICLE INFO

Article history:
Received February 28, 2020
Received in revised form March 30, 2020
Accepted April 15, 2020

Keywords:
Data
Personel Data
Data Rights
Identity
GDPR

ABSTRACT

From the beginning people seeking fundamental rights which they have from existing, had to face struggle with tyranny. End of the long process in the idea of human rights, people reached very fundamentally right those still continued to evolve. The personal data of individuals has been at the centre of international law since the 1940's Universal Declaration of Human Rights (UDHR) by the United Nations (UN). Those rights were intertwined with other personal rights asserted in the UDHR. The European Union (EU) is a unique social example of an entire Continent coming together to form a community. The EU Law is a supranational law that has supremacy over the municipal laws of the EU Member States. EU has been at the forefront of legislating laws that concern human dignity and rights. The Charter of Rights (CFR) of the EU under Article 8, defines personal data as a fundamental human right. The European Convention ECHR recognizes personal data right as part of personal freedoms.EU General Data Protection Regulation (GDPR) came into force in May 2018. It has been transformative since it's coming into force. This paper highlights the transformative nature of the GDPR under the Case Law of the European Courts. The paper also considers data protection rights under the broader concepts of identity and citizenship.

1. Introduction

The EU Law GDPR has given new meanings to the human rights pertaining to data under Article 8 CFR. GDPR has also placed new emphasis on the terms such as personal *information* in its broadest within the scope of international law (Goddard, 2017). Personal information has the socio-political dimension of *identity*. The economic dimension of personal information carries the scope of *privacy*. The law

* Sorumlu yazar/Corresponding author.
e-posta: semayilmazgenc@gmail.com

enforcement and the added aims of national security concerning information on the world wide web have added the dimension of using the information to fight crime in the realm of *cyber warfare* (Reidenberg, 1996).

Within its narrowest definition, the personal data offers *monetary value* that has the potential to generate economic gains based on the data subject's valuation of the '*price*' attached to their privacy (Schwartz, 2003). Policymakers for socio-economic policies and the lawmakers are grappling with the ever-increasing reliance of all measures of economic activity that places personal data as its focal point (Doyle, 2018).

The *Purpose Limitation* is recognized as the guiding principle for most of the existing international legal instruments for data protection (Forgó & et. al, 2017). There is consensus within the Academy that any analysis of international law on data protection rights must be viewed under the *Purpose Limitation Principle*. It is also agreed that under the Purpose limitation, the legitimacy of collecting, storing and accessing a person's personal data or information must be for specific purposes that are guided under transparent laws on how that data should be collected, stored and accessed (Von Grafenstein, 2018).

The principle of the *Purpose Limitation* still does not answer the fundamental question of *why* identity, information and specifical data should be protected as a fundamental right. It also follows up with the question of the necessity for laws that must guarantee the right to privacy of such information.

It was perhaps these question that the European Union's much-celebrated *Supranational* data protection legislation General Data Protection Regulation (GDPR) EU 2016/679 emerged. This paper examines the above questions with the view to examine if GDPR aims to transform the existing regimes of data protection and if GDPR may prove to transformative across the narrowly defined objectives of this new EU data protection law. It will examine the global impact of General Data Protection Regulations and the interaction process between changing information age and regulations. Furthermore, it will review the position of regulations for globalization and its effect on public opinion and human rights violations.

2. End of Globalization

The emergence of nationalist politics in North America under the US President Trump and the epic loss of Labour Party to the EU-loathing Conservative in the UK marks the end of globalization in western politics (Virdee & McGeever, 2018). The hype of globalization that gained momentum during the 1980s has died an unnatural death due to *protectionist* and *ultra-nationalist* policies becoming the popular socio-political rhetoric of western leaders.

Scholars have criticized the US and its western allies for waging Middle East *Wars for Oil* (Jones, 2012). A type of conflict has merged in the global economic space. This conflict is about controlling the *personal data* of billions of worldwide web users using various web-enabled devices. The US, UK, EU, China, Russia and India are all players in this war to get an upper hand in who controls the global flow of personal data that drives the massive global data markets (Wu & et. al, 2013). The massive role of personal data in driving the global economy has been recognized as the biggest disruptor of the 21st century (Tattersall & Grant, 2016).

The US and EU including European nations that are not part of the EU have been trying to find a *legal* way to share global data of persons collected by their security agencies. The data collected by the US and its allies in Europe also consists of persons who are neither US citizens nor Europeans, rather they reside in Asia, Africa and Australia etc. (Yoo, 2014). The United States Transportation Security Agency (TSA) requires data of all foreign nationals prior to them boarding any flights either transiting or flying to the US (Gubitz, 2004). Such arrangements of overt and covert collection of personal data of individuals were not the subject of general public debate. The US Security Contractor Edward Snowden drew global attention to the United States '*Prism*' program of secret collection of personal data from around the globe. The UK was running its own covert collection of mass personal data without any legal oversight under its *Tempora* program (Lyon, 2014).

Post Snowden revelations, the European Union Data Security Supervisors were pushed into action and EU Data Protection laws were brought under review by the EU Parliament (Wright & Kreissl, 2014). The Court of Justice of the European Union (CJEU), Luxembourg and the European Court of Human Rights (ECtHR), Strasbourg started to take a fresh look at the handling of mass data collection, storage and access by technology giants such as Google, Facebook and Microsoft. The foremost concerns of the two Courts followed the political demands of holding the tech-giants responsible for any violations of data protection rights (Nesterova, 2017).

It seems that the GDPR is a direct and accumulative consequence of the demands by the civil society, liberal politicians, human rights and legal activists who took a serious view of the intrusion in their privacy by the State agencies through tech-giants willing to share individual data without any legal oversight. The US government, the conservative government in the UK including the tech-giants like Google, Microsoft, Amazon, Facebook and Apple are all against any proposed restrictions such as those imposed by the GDPR to limit their ability to collect, store and access personal data without impunity (Ciriani, 2015).

3. Data Versus Identity

Personal data, in general, revolves around the intrinsic core concept of identity. Identity also helps to lend the element of something personal when any data that is classified as personal data is used in the context of information. Information is in itself a neutral concept if there is no *specific* identity assigned to the information. The description of the information once assigned to the general activities concerning any unique and specific physical body then raises the question of certain rights (Floridi, 2011). Michel Foucault's ideas about the non-fixated notion of identity concern a legal person. Identity in Foucault's view is

contingent, provisional, achieved not given (de Leeuw & Bergstra, 2007).

In social literature, not only is *identity* a difficult concept to be formally defined, even the *individual* is a problematic definition to reconcile. In the milieu of the problematic definitions of *identity* and *individual*, the resultant argument is further complicated by the diachronic nature of an individual's identity within the community. The diachronic identity means that the individual's identity is established through continuously *emerging* or *reappearing* in various events within the community. Thus, the diachronic identification is not concerned with establishing *separate identities* between individuals in the society; rather it concerns the same individual's identity with reference to different events. This argument is based on the correlation between 'identity and person' linked to events that take place within a community. The significant factor to consider in this argument in case of identity is the *object* of identity which is the person. Identity, therefore, can be a hollow concept in the absence of its object, the person. Also, the person's identity can only be recognized if the community events are determined as a frame of reference for the purposes of the person's identity. What has emerged from our discussion is the establishment of a theoretical framework for how significant is the *identity* once it is linked to the events within a community. The person's identity, therefore, remains critical to identify that person as long as the community exists.

The idea of *identity management* is by corollary intrinsically linked with the concepts of *community management*. The management of this *contingent* and *achieved identity* gives rise to questioning the purpose of *identity management*. It seems that the 'management' of identity is a label and not the purpose. We assert this as the use of the word *management* in the context of *personal identity* or *personal data* lends it a meaning for *securing* the identity. One can argue that identity management is, therefore, an advertisement to create the notion of *security* for the *data subjects*. The actual security of the data would be an altogether different mechanism that has been labeled as a system for identity management. So, we are not really sure what exactly is a settled meaning of personal identity and personal data. It is for this reason that socioeconomic studies refer to the legal domain for these definitions through Statutes and Case Law.

The GDPR Article 4(1) defines 'personal data' within the limitation of four intrinsic interconnected elements. It states that personal data is any information relating to an identified or identifiable natural person. Interestingly the four elements that constitute *personal data* within the definition of GDPR speak to the earlier discussion on the identity connected to resurfacing and emerging of a person in various events.

The personal identity is then always in a perpetual state of development and is not a static idea. The sciences of data management, therefore, convey the idea that perhaps once identity becomes data, there exists a system that can secure that data through a process of *management*, thereby giving the data subject a *secure identity*. The State has a positive obligation to operate under laws such as GDPR to ensure that the aims defined at the core of prescribing such laws are upheld (de Than, 2003).

4. Development of Data Rights

There are two distinct and independent law-making bodies that prescribe laws within Continental Europe. The first is the Council of Europe (COE), Strasbourg France and the second is the European Union (EU) Brussels. Both owe their genesis moments to the events and atrocities committed by European against each other and other nations during the Second World War. The Council of Europe is linked with the *United States of Europe* concept under the Truman Doctrine (Merrill, 2006). The so-called Truman Declaration to the US Senate by US President H.S. Truman in March 1947 called for immediate aid to Greece and Turkey to prevent both the countries from falling under the influence of the Soviet Union. The doctrine evolved from Great Britain's inability to offer any economic assistance to both the countries that were crucial to secure the Mediterranean gate-way to Europe. Following President Truman's announcement of delivering US$ 4 Billion aid package to secure the European sea routes from the Soviets, the British Prime Minister W. Churchill in his September 1946 speech at Zurich University floated the idea of the *United States of Europe* (Lénárt, 2003).

The UK was struggling with the impact of losing its colonies around the world during the 1940s. Thus, the UK accepted a subservient role to the new leading power of the world, United States. The US conceived Europe to be the ally that would protect the interests of the United States for times to come. The precipitation of the UK's power in the late 1940s forced the UK to save its economic interests globally by aligning itself with the American socioeconomic agendas for Europe. Churchill subsequently chaired the Hauge meeting of the *Congress of Europe* that laid the foundation for a European Assembly and Court of Human Rights. The UK's supportive role resulted in the London signing of the *Statute of the Council of Europe* on May 5, 1949. The statute came into force on August 3, 1949 (Marston, 1993).

The Council of Europe's most famous legislation is the European Convention on Human Rights (ECHR). ECHR was adopted by its 10 original members on November 4, 1950. The signatory states to the ECHR are called *High Contracting Parties*. Presently 27-member states of EU along with other nations comprise the 47-member states today. The ECHR is enforced through its own judicial body, the European Court of Human Rights (ECtHR), Strasbourg. ECHR protects fundamental human rights. There is no separate right within ECHR for personal data protection. The ECHR determined and interpreted the data protection right as, *the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the European Convention on Human Rights* (Kokott & Sobotta, 2013).

The European Union (EU) is a distinct and unique legislative body of Institutions in the world. It has been described as a

unique social experiment by social scholars. In that, it gave rise to a body of law that is enforceable across the continent of Europe and takes precedence over national laws of the member states in areas provided under its law. The EU's genesis can perhaps be attributed to the signing of the *Customs Convention* in September 1944 (Bantaș & Beldiman, 2017). The purpose of this treaty was to remove trade barriers between the BeNeLux nations (Belgium ,Netherlands, and Luxembourg).

The European Coal and Steel Community (ECSC) followed in April 1951. Originally only envisaged between France and West Germany, the final signatories were France, West Germany, Italy and the BeNeLux nations. The aim of the treaty was to remove the control of steel and coal by the wartime industries and divert the steel and coal resources to the rebuilding of Europe. ECSC's framework provided for the establishment of a *High Authority* comprising a *Council of Ministers* representing the member states. It also provided for an *Assembly* and a *Court of Justice* to deal with all matters arising from the *Acts* of the Council of Ministers. This legally unique and independent organization was the creation of a truly *internationally enforceable* agreement. The agreement allowed for the transfer of sovereignty for the matters covered under the agreement from the member states to the institutions of ECSC. This is the legal foundation that led to the later creation of the European Economic Community (EEC) signed in a treaty by the same six signatory nationals of ECSC in 1958 (Dedman, 2006).

The signing of the Brussels Treaty in 1965 and the Single European Act (SEA) in 1986 paved the way for the 1993 Maastricht Treaty. Maastricht Treaty is also known as The Treaty of European Union (TEU). TEU laid down the broad European intergovernmental cooperation through the so-called *Three Pillars* established through the TEU. The first pillar was the unification of all previous bodies such as EEC, ECSC etc. The second pillar speaks to intergovernmental cooperation for security and foreign affairs. The third pillar concerns justice and home affairs (Wessels, 1994).

The Treaty of Lisbon signed in December 2007 and enforced in December 2009, retained the TEU and renamed the EC Treaty as Treaty on the Functioning of the European Union (TFEU). Both TEU and TFEU are the basis of the primary sources of the EU Law. TFEU also proposed the European Charter of Fundamental Rights (CFR). Article 8(1) to 8(3) guarantees the protection of personal data under Title II of Freedoms. This is not an absolute right under the CFR. The EU member state's interference with this right is permissible under certain exceptions. It must also be noted the later development of EU Data Protection laws through TEU and TFEU is an expansion of this right.

The EU data protection laws distinctively uphold the principles of protecting fundamental human rights and the rule of law. The EU data protection law ensures broader and much deeper cooperation for socioeconomic freedoms as the principal aims of the 27-member states union. The cornerstone of EU law is to guarantee the so-called four freedoms, the free movement of *people*, g*oods*, *services* and *capital* within the EU under Article 26(2) TFEU. Both the Council of Europe and the EU share the same *fundamental values* that guarantee fundamental rights for data protection under the principle of the rule of law (Mantelero, 2017).

5. European Identity & Data Rights

The Council of Europe's Convention 108 is the first *European* internationally enforceable legal instrument for data protection (Rodotà, 2009). The EU's first supranational data protection law came as a *Data Protection Directive* in 1995 (Simitis, 1994). Article 16 TFEU affirms the distinct data protection right under Article 8 of the EU Charter for Fundamental Rights (Cate & et. al, 2018). GDPR and Article 16 TFEU is an interplay between the EU's primary and secondary law that comprehensively addresses the protection of personal data under the EU Law.

At the heart of all EU lawmaking for the protection of data is the idea of the *European* identity (Cate, 1994). It is a separate debate, and beyond the scope of this paper, how the *European identity* operates within the scope of various *national* identities amongst the EU member states.

The question of what defines the European identity within the scope of data rights is an important one. A clear understanding of the European identity within the context of data rights can further facilitate the importance of data protection under the GDPR regime. Such an understanding should be able to clarify that the GDPR proposes to *protec*t the *freedom*s attached to the personal identity of the EU citizens de (Andrade, 2010).

Within the context of EU Law, the identity of EU citizens has been reconciled as the *political* identity of the EU citizens. This concept of political identity is further attached to the concept of *European Citizenship* (Fossum, 2001). EU Citizenship emerged as a concept within the 1993 Maastricht Treaty. Article 8 TEU, which is now Article 20 TFEU conferred European citizenship to all individuals who are nationals of the EU Member States. The EU citizenship concept with the underlying political identity is aimed to strengthen the shared economic prosperity concept across the EU (Van den Brink, 2012).

This discussion allows for a few conclusions. The political identity of the EU citizens aims to further the proposed goals of ensuring shared prosperity through EU citizenship as a legal identity. To fully understand this point within the context of *identity* and the supranational nature of EU Citizenship, the national identity is subsumed within these political and legal concepts of identity within the EU Law.

If the EU law for data protection, which is a supranational legal regime, protects the data rights of a person at the levels of municipal law, then the supranational nature of EU data protection law must ensure the same level of protection at the EU citizenship level. All these protections are linked with the identity of the individual.

The EU law also allows for interference with the individual rights of data protection conferred by Article 8 of EU CFR and a right as an extension of ECHR's Article 8 right for respect of personal family. The State's right to interference with data rights under the EU Law is covered under the Official Authority. Article 51 TFEU describes what

constitutes the exercise of Official Authority (De Hert & Papakonstantinou, 2016):

"The provisions of this Chapter shall not apply, so far as any given Member State is concerned, to activities which in that State are connected, even occasionally, with the exercise of official authority. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may rule that the provisions of this Chapter shall not apply to certain activities".

A cursory reading of Article 51 suggests a very broad definition of the exercise of the official authority. Also, the wording *certain activities* do not clearly define the exact nature of how to exercise the official authority to interfere with the data protection right.

In the seminal CJEU case of Rayner's v the Belgian State[1], the Court defined the Official Authority as, "Official authority is that which arises from the sovereignty and majesty of the state; for him who exercises it, it implies the power of enjoying the prerogatives outside the general law, privileges of official power and powers of coercion over citizens."

The definition of Official Authority in the case of Re Rayner's links the concept to the Sovereignty of the State, which in itself is an abstract concept. The concept of sovereignty is further diminished due to the rising powers of the international law (Lewis, 1982). CJEU has narrowly defined the use of official authority to *process* or *manage* any personal the case of Commission v Italy (Data Processing).[2] The Court held that the exception of *Official Authority* did not extend to the design and operation of data-processing systems for public authorities.

In the seminal joint cases of Volker und Markus Schecke GbR[3] concerning the protection of natural persons with regard to the processing of personal data, the CJEU held (Para 52-54):

"The right to respect for private life with regard to the processing of personal data, recognized by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, concerns any information relating to an identified or identifiable individual. Legal persons can thus claim the protection of Articles 7 and 8 of the Charter only in so far as the official title of the legal person identifies one or more natural persons. That is the case where the official title of a partnership directly identifies natural persons who are its partners."

The CJEU clearly stated that data protection concerns the identity of the legal person. Further clarification by the Court that a legal person is a natural person is perhaps for drawing a distinction between the company law definition of a corporation being a legal person as well. In this instance, the legal person referred to a human or a natural person. The word *officially* lays emphasis on the *political* construct attached to the meaning defining the identity of the natural person. The CJEU in the same case laid down the guidelines about the situations in which the data rights could be interfered with by the State (Para 52-65):

"Article 52(1) of the Charter of Fundamental Rights of the European Union accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms, and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others. The limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the European Convention on Human Rights."

The EU Directive 2006/24/EC came to strengthen the post 9/11 EU Directive 2002/58/EC. The purpose of both the directives was to allow law enforcement agencies to access information about the personal identities related to ICT communications of the subscribers within the EU. The Directives allowed for storage and access of such information to be held by law enforcement agencies between six months and up to two years.

The mass data collection and storage of such ICT identities were challenged in the seminal CJEU case of Re: Digital Rights Ireland.[4] The Court declared the EU Directive 2006/24/EC to be invalid while giving a joint judgment of two such cases in the same instance.[5] The Court held that the EU Directive was in direct violation of the Article 8 Charter Rights for Data Protection. The Court also stated guidelines for what would constitute lawful interference with the data protection rights under Article 8. The Court held that any interference with the data protection rights required a *proper legal basis*, for the purposes of *fighting serious organized crime including terrorism* and should not go *beyond strictly necessary*. The Court finally held that the data must be retained within the EU and must comply with the *strict limits* of the prescribed retention period of between six months and not beyond two years.

The Court finally addressed the issue of identity within the scope of elements of communication (Para 32):

"This is defined as a subset of communications data that identifies the sender or recipient of a communication; the time or duration of a communication; the type, method, pattern, or fact of communication; the system from, to, or through which a communication is transmitted; or the location of any such system."

Article 48 GDPR reads:

"No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State."

Article 48 GDPR prevents any data disclosures of any data subject of EU to any third country without the presence of an

[1] CJEU: Reyners v The Belgian State (Case 2/74) (1974) ECR 63.
[2] CJEU: Commission v Italy (Data Processing) (Case C-3/88) (1989) ECR 4035
[3] CJEU: Joined Cases C-92/09 and C-93/09
[4] CJEU: Digital Rights Ireland C-293/12
[5] CJEU: Joined Cases C-293/12 and C-594/12, Judgment April 8th, 2014.

internationally binding agreement between the EU and that country. This is a powerful clause that would prevent any of the EU Member States from violating the data protection rights of an EU Citizen if any emergency orders are made by an official agency without a treaty in place.

The UK was the first country to opt-out of this clause of the GDPR. The UK took the opt-out of Article 48 GDPR under Protocol No. 21 of TFEU that allows UK and Ireland to opt-out of any EU laws that UK and Ireland do not want to adopt in the areas of Freedom, Justice and Security. This does not mean that any actions by the UK or Ireland that violate Article 48 of GDPR in violation of any data protection rights cannot be challenged in the Courts of law. The option of a *Judicial Review* within the UK and Ireland and also the possibility to approach the CJEU remains open for the enforcement of Article 48 GDPR.

GDPR is a law that is transformative in nature. Mr. Jan-Philipp Albrecht, the German Member of EU Parliament and German representative for the consultative committee for GDPR attributed the delay in the implementation of GDPR to the resistance by state covert intelligence agencies. He stressed that the reasons delay is due to increased *covert* access to European data by US and UK intelligence agencies. The implementation of the GDPR will not only transform data rights, but it will transform the rights within the context of the security and defense of the EU (Fleming, 2015).

6. Economic Transformation

The GDPR has come into force in May 2018. It is far too early to critically examine any of its tangible impacts on the economies of the EU. However, the EU leadership is acutely aware of the economic significance of the personal data of its citizens (Reding, 2014). The GDPR aims to balance the monetary benefits of personal data with the need to protect the privacy and all afforded data rights of the EU citizens.

The European Economic Association (EEA) through its European Free Trade Association (EFTA) Agreements formed the single largest economic market in the world in 2016.[6] Pursuant to Article 7(a) of the EEA, all member states are obligated to adopt GDPR nationally. Article 288 TFEU makes GDPR *applicable* to all EU Member States in all matters including the economy. Article 288 TFEU refers to the *binding* nature of the EU's secondary source of law that is the EU Regulations, of which GDPR is one such Regulation. Article 288 (2) makes GDPR binding on all, *"a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."*

The EEA Agreement Articles 102(1) through 102(6) prescribe *five-stages* to comply with EC Regulation No.2894/94 concerning enforcement of any EU law such as GDPR across the Member States, that are signatory to the EEA. So far the Stage-1 has been decided. The Stage-1 Agreement of EEA compliance makes GDPR mandatory of all economic activities defined under the EEA agreement. The subsequent stages will involve participation by the representatives of the EEA Member States to provide consultative advice to the EU Commission. The proposal would then go through the EU legislative process for any necessary adjustments if required in the GDPR.

The purpose of the EU Legislative process concerning GDPR within the EEA is to ensure that the process would result in the most transparent and predictable application of GDPR within the EEA zone. GDPR has a huge impact *within* the European markets through its adoption for the purposes of the European Economic Association (EEA) under Articles 217 and 288 of TFEU.

7. GDPR International Impact

The international scope of GDPR makes it a complex problem within the international treaty law. The Vienna Convention for Treaty Law 1969 (VCTL 1969) is an inter-state legal regime. GDPR requires inter-state as well as international organization treaties. Vienna Convention for Treaty Law- International Organization 1986 (VCTL-IO 1986) is still not enforced. Thus, GDPR has to be resolved under international law regimes that make it difficult to enforce outside of the EU.

The US is the largest trade partner of the EU along with Japan, China and Russia. The US Constitution does not provide any specific data protection rights. The Constitution of Japan also does not provide any such protections. Both the USA and Japan, have adopted the *Market-Based* strategy to apply minimum restraints through legislative and regulatory interventions in the area of data protection. In the market-based regime, the ICT Industry leads the way in advising the legislature on policies that balance the data privacy and protection rights verses the economic interest of the market. In short, the legal regime follows the rules of the self-regulated market.

China and Russia use state-control to strictly regulate the ICT industry. Such controls also impact the economic activities connected with the flow of data and privacy rights. In China and Russia, cybersecurity is treated as an exclusive policy-making domain of the national security institutions for all matters concerning storage and excess of mass data.

Canada and Australia follow the interventionist strategy to deal with data usage. The *interventionist* approach aims to seek comprehensive coverage of all aspects of data and information services regardless of its application. It includes data used for purposes such as economic, social or cybersecurity.

The GDPR falls under the interventionist approach. GDPR is supranational legislation that does not concern itself with the existing national legislation on data protection and privacy in any of its Member states. Due to its supranational nature, GDPR has direct an effect both vertically and horizontally all across Europe. While the legal discussion of the *Vertical and Horizontal Effects* of EU legislation is beyond the scope of this paper. It would suffice for the general understating that *Vertical Effect* concerns State Institutions that must comply with the legislations while the *Horizontal Effect* can include persons and organizations that are not part of the State.

[6]Agreement on The European Economic Area (OJ No L 1, 3.1.1994, p. 3; and EFTA States' official gazette.

It is this doctrine of *Horizontal Effect* of the GDPR that binds states, companies and individuals to comply with GDPR. The GDPR legal regime of enforcement through CJEU prescribes strict financial penalties for any violations under the GDPR. These penalties are directly enforceable within the EU. CJEU cases such as Google v Spain[7] are based on this doctrine of *direct-effect* and *vertical and horizontal* effect.

Article 45(2) of the GDPR concerns the assessment of the level of protection afforded to the data of EU citizens by a third-party or a third-country. The EU Commission decides the adequacy of such measures. One of the elements to be assessed by the EU Commission under Article 45(2) is the matter of international commitments of the EU related to personal data protection. The adequacy assessment is complex when it concerns vast internetworks carrying massive amounts of personal data across various time-zones in nanoseconds. This complexity of the *physical infrastructure* of global ICT communications networks poses real challenges to determine adequacy of protection since the data may or may not be *permanent* in one geographical location at a given time. Such assessments can not only delay the process of the adequacy but it may also pose issues of international obligation concerning bilateral trade agreements affected by Article 45(2) compliance.

EU Commission's position for the purposes of adequacy requirements pertaining to data pursuant to Article 45 GDPR creates a preference for those countries outside the EU that fall in the list of countries that are already considered satisfying the adequacy requirement under Article 45 GDPR. The international obligations of the EU under the World Trade Organization's (WTO) GATS[8] MNF[9] structure may create potential violations under GATS Article XVII[10] due to non-compliance with the adequacy requirement under GDPR Article 45.

8. Conclusion

GDPR is in its formative years. Case law is emerging from the CJEU that points to the seriousness of the Court to address any violations of GDPR without impunity. The resulting effect of GDPR has also created friction between the EU and the US concerning the operation of the US technology giants like Google, Microsoft and Apple within the EU. The US President Donald Trump has threatened the EU with economic sanctions over any proposed limits on the operation of the US tech giants in the EU.

It is a unique legal instrument that gives a new lease to data protection rights which became obscure post 9/11 in the western countries. GDPR also has the potential to give rise to a new generation of international rights order concerning personal data. To confine the scope of GDPR to its economic impacts would mean denying the disruptive role of information technologies to human life in the contemporary age. GDPR has drawn the attention of the world to the importance of personal data protection in the heightened environment of human rights violations across the globe. GDPR is the step in the right direction seeing how data is continuing to transform the face of human interactions in all spheres of life.

[7] Google v Spain (Right to be Forgotten). Decided 13 May 2014. Case No. number C-131/1

[8] GATS:WTO's General Agreement on Trade and Services (GATS). The creation of the GATS was one of the landmark achievements of the Uruguay Round, whose results entered into force in January 1995. https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm

[9] MNF: WTO's Most Favoured Nation concept allows for equal trade advantages by the recipient country. https://www.wto.org/english/tratop_e/region_e/regatt_e.htm

[10] GATS Article XVII: Provides for obligations on Members in respect of the activities of the state trading enterprises referred to in paragraph 1 of Article XVII, which are required to be consistent with the general principles of non-discriminatory treatment prescribed in GATT 1994 for governmental measures affecting imports or exports by private traders.

References

Bantaş, D. A., & Beldiman, E. (2017). Postwar international organizations predecessor of the European Union. *Challenges of the Knowledge Society*, 374-383.

Cate, F. H. (1994). The EU data protection directive, information privacy, and the public interest. *Iowa L. Rev.*, *80*, 431.

Cate, F. H., Kuner, C., Lynskey, O., Millard, C., Ni Loideain, N., & Svantesson, D. J. B. (2018). An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security.

Ciriani, S. (2015). The economic impact of the European reform of data protection. *Communications & Strategies*, (97), 41-58.

de Andrade, N. N. G. (2010). Data protection, privacy and identity: distinguishing concepts and articulating rights. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp. 90-107). Springer, Berlin, Heidelberg.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer law & security review*, *32*(2), 179-194.

de Leeuw, K. M. M., & Bergstra, J. (Eds.). (2007). *The history of information security: a comprehensive handbook*. Elsevier.

de Than, C. (2003). Positive obligations under the European Convention on Human Rights: towards the human rights of victims and vulnerable witnesses?. *The Journal of Criminal Law*, *67*(2), 165-182.

Dedman, M. (2006). *The origins and development of the European Union 1945-1995: a history of European integration*. Routledge.

Doyle, J. (2018). *Unreal objects: Digital materialities, technoscientific projects and political realities*, Kate O'Riordan, SAGE Publications, England.

Fleming, J. (2015). EU Lawmaker Warns of Data Protection Rules Delay till 2016, (Accessed on: 20.01.2020), https://www.euractiv.com/section/digital/news/eu-lawmaker-warns-of-data-protection-rules-delay-till-2016/.

Floridi, L. (2011). The informational nature of personal identity. *Minds and machines*, *21*(4), 549.

Forgó, N., Hänold, S., & Schütze, B. (2017). The principle of purpose limitation and big data. In *New technology, big data and the law* (pp. 17-42). Springer, Singapore.

Fossum, J. E. (2001). Identity-politics in the European Union. *Journal of European Integration*, *23*(4), 373-406.

Gubitz, A. S. (2004). The US Aviation and Transportation Security Act of 2001 in Conflict With the EU Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism. *New Eng. L. Rev.*, *39*, 431.

Jones, T. C. (2012). America, oil, and war in the Middle East. *The Journal of American History*, *99*(1), 208-218.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, *3*(4), 222-228.

Lénárt, L. (2003). Sir Winston Spencer Churchill and the Movement of the Unification of Europe. *European Integration Studies*, *2*(2), 17-28.

Lewis Jr, H. S. (1982). Three Deaths of State Sovereignty and the Curse of Abstraction in the Jurisprudence of Personal Jurisdiction. Notre Dame L. Rev., 58, 699.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, *1*(2).

Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer law & security review*, *33*(5), 584-602.

Marston, G. (1993). The United Kingdom part in the preparation of the european convention on human rights, 1950. *International & Comparative Law Quarterly*, *42*(4), 796-826.

Merrill, D. (2006). The Truman doctrine: containing communism and modernity. *Presidential Studies Quarterly*, *36*(1), 27-37.

Nesterova, I. (2017). Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards. In *European Society of International Law (ESIL) 2016 Annual Conference (Riga)*.

Reding, V. (2014). A data protection compact for Europe. European Commission, (Accessed on: 04.01.2020), https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_14_62.

Rodotà, S. (2009). Data protection as a fundamental right. In *Reinventing Data Protection?* (pp. 77-82). Springer, Dordrecht.

Schwartz, P. M. (2003). Property, privacy, and personal data. *Harv. L. Rev.*, *117*, 2056.

Simitis, S. (1994). From the market to the polis: The EU directive on the protection of personal data. *Iowa L. Rev.*, *80*, 445.

Tattersall, A., & Grant, M. J. (2016). Big Data–What is it and why it matters. *Health Information & Libraries Journal*, *33*(2), 89-91.

Van den Brink, M. J. (2012). EU citizenship and EU fundamental rights: taking EU citizenship rights seriously?. *Legal Issues of Economic Integration*, *39*(2), 273-289.

Virdee, S., & McGeever, B. (2018). Racism, crisis, brexit. *Ethnic and racial studies*, *41*(10), 1802-1819.

Von Grafenstein, M. (2018). *Principle of Purpose Limitation in Data Protection Laws*. Nomos Verlagsgesellschaft mbH & Company KG.

Wessels, W. (1994). Rationalizing Maastricht: the search for an optimal strategy of the new Europe. *International Affairs*, *70*(3), 445-457.

Wright, D., & Kreissl, R. (2014). European responses to the Snowden revelations. In *Surveillance in Europe* (pp. 20-64). Routledge.

Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2013). Data mining with big data. *IEEE transactions on knowledge and data engineering*, *26*(1), 97-107.

Yoo, J. (2014). The Legality of the National Security Agency's Bulk Data Surveillance Programs. *Harv. JL & Pub. Pol'y*, *37*, 901.