JOEEP

Journal Homepage: http://dergipark.org.tr/joeep

Araştırma Makalesi ● Research Article

Transformation of Europe Socio-Economics In The Wake of General Data Protection Regulation (GDPR)

Genel Veri Koruma Düzenlemesi (GDPR) Sonrası Avrupa'nın Sosyoekonomik Dönüşümü

Hassan SYED[a], Rui Alexandre Castanho[b] & Sema Yılmaz Genç[c*]

[a] BPP House, Aldine Place, 142-144 Uxbridge Road, London.
ORCID: 0000-0003-2114-2473
[b] Assoc.Prof.Dr., WSB University, 41-300 Dabrowa Górnicza, Poland;: Dabrowa Górnicza, Poland
ORCID: 0000-0003-1882-4801
[c] Assoc.Prof.Dr., Kocaeli University, Marketing and Advertising Kocaeli Üniversitesi Umuttepe Yerleşkesi 41001, Kocaeli, Türkiye.
ORCID: 0000-0002-3138-1622

MAKALE BİLGİSİ

Makale Geçmişi:
Başvuru tarihi: 14 Mart 2020
Düzeltme tarihi: 16 Nisan 2020
Kabul tarihi: 16 Nisan 2020

Anahtar Kelimeler:
Genel Veri Koruma Düzenlemesi
Veri Koruma ve Güvenlik
AB Hukuku
Sosyoekonomi

ÖZ

Avrupa'nın sosyoekonomik durumu 1919 ile 2019 yılları arasında köklü bir dönüşüm geçirmiştir. Avrupa kıtasının son yüz yıl içinde geçirdiği bu dönüşümün bir paraleli yoktur. Avrupa'nın 1919, 1949 ve 2019 yılları arasında değerlendirmesi yapıldığında sosyo-ekonomik durumu etkileyen ortak noktanın zamanın hükümetleri tarafından ilan edilen güvenlikle ilgili hükümler olduğu bulunmuştur. Bu makale yeni Avrupa kapsamlı güvenlik yasası olan GDPR'nin yayınlanmasının ardından Avrupa'nın dönüşümünü incelemektedir. AB yasa koyucuları yasanın Avrupa vatandaşlarının (veri) güvenlik taleplerini karşıladığını ilan etmektedir. Birinci olarak, tarihin ve AB'deki temel haklar kuralları içinde yapılan veri tanımının ışığında GDPR'nin sosyoekonomik etkisini ve Avrupa Birliği Adalet Divanı'nın (CJEU) içtihatlarının bu yasanın üzerinde oynadığı rolü inceleyecek. İkinci olarak, GDPR bağlamında Türkiye'nin sosyoekonomik önemini ayrıntılarıyla ele alınacaktır.

ARTICLE INFO

Article history:
Received: Marth 14, 2020
Received in revised form: April 16, 2020
Accepted: April 16, 2020

Keywords:
General Data Protection Regulation
Data Protection and Security
EU Law
Socio-Economic

ABSTRACT

The socio-economic landscape of Europe has seen a dramatic transformation between 1919 and 2019. As a continent, Europe has no parallel for such a transformation within the last hundred years. An analysis of Europe between 1919, 1949 and 2019, would find one common factor influencing the socio-economic; the security imperatives proclaimed by the respective governments at the time. This paper examines the transformation of Europe in the wake of its latest pan-European security law, the GDPR. The EU policy makers proclaim that the law satisfies the (data) security demands of the European citizens. First, we will examine the socio-economic impact of GDPR in the light of the history and the definition of data within the precepts of fundamental rights in the EU and the role of the jurisprudence of the Court of Justice European Union (CJEU) in influencing this law. Second, we will further explore the socio-economic significance of Turkey within the context of GDPR.

1. Introduction

In this finite world the information in its broad terms and data in specific terms have infinite uses and dimensions. There is the socio-political dimension of identity and then there is the socioeconomic dimension of privacy cost and yet another dimension is the legal dimension of using

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

Atıf/Cite as: SYED, H., Castanho, R.A., YILMAZ GENÇ S.. (2020). Transformation of Europe Socio-Economics In The Wake of General Data Protection Regulation (GDPR). *Journal of Emerging Economies and Policy*, 5(1), 5-16.
e-ISSN: 2651-5318.

information or data to fight crime or in the realm of cyber warfare. In its rather narrow confines one can examine data for its monetary value that derives economic gains based on the individual data subject's valuation of the price attached to their privacy. There is enough literature out there to fill a library on the topic of the economic value of privacy within the meaning of personal data in the present advanced age of Information and Communications Technology (ICT) and its milieus of web marketing strategies for Internet of Things (IOT) etc. Surely any further analysis of such economic implications of data won't add much to the debate.

The Purpose Limitation is recognized as the guiding principle for most of the existing international legal instruments for data protection. We also agree with the position taken by most of the academics that any analysis of international law on data protection rights would highlight the Purpose Principle. After all, the purpose of collecting, storing and accessing a person's personal data or information must be for the legitimate and specific purposes that should guide the law for how that data should be collected, stored and accessed. The principle of the Purpose Limitation still does not answer the fundamental question of why identity, information and specifically data should be protected, and necessary laws should guarantee the right to privacy of such information.

To this end, we have chosen to take a much broader approach to examine if the European Unions much celebrated Supranational data protection legislation General Data Protection Regulation (GDPR) EU 2016/679 is transformative in nature. To answer this question, we will be looking at the transformative nature of the GDPR from the perspective of the historical development of Europe and its body of laws, the European identity, the European Security identity and last but not the least if there exists any transformative impact of the GDPR outside the legislative boundaries of the EU law.

The European Union (EU) is the result of socio-political and socioeconomic transformation of the European continent post Second World-War. The devastations of the war not only shook the sensibilities of the European population, it also resulted in a transformed map of the world with new nation-states emerging at the end of the predominantly European imperial rule.

The period of European history post Second World War is what defines Europe today. Afterall, both the First and Second World wars that results in casualties (Nash, 1976) in the range of 21 million dead and 85 million dead worldwide respectively were started by Europeans and for reasons internal to the politic of Europe at the time. Such colossal loss of lives is not an easy burden to bear. We are not too sure if lessons of history from the times of the great Wars are still ringing in the ears of the present-day European leadership. There is historical relevance to our topic of discussion. The relevance is of the European Identity ideas which are woven in the fabric that forms the basis leading to the formation of EU and factors that are pertinent to the laws of the EU.

We will be carrying out our analysis for the purposes of asserting our theory that the General Data Protection Law (European Union Regulation, 2016) of the EU that came into force on 25th May 2018 is transformative in nature. We further propose that it is the EU laws such as GDPR that will cause the resultant transformation to alter the socioeconomic and socio-political land scape of Europe in the future. We believe that the present state of divisive politics within Europe that has led to Brexit is closely linked to the formulation of EU legislations such as GDPR. In a short span of 75 years since the end of the Second World War in 1944, the world has come full-circle in terms of raging socio-political divides based on ethnic and cultural grounds. The League of Nations formed in the 1940s is now the United Nations. It purpose was to resolve conflict through dialogue. Yet it only serves the purposes of the permanent members of its Security Council as a rubber stamp. The UN has now been reduced to a global bureaucracy.

The hype of globalization that gained momentum during the 1980s slowly died down in the mid 2000s and the slide towards protectionist and ultra-nationalist polices became the popular socio-political rhetoric of global leaders. Donald Trumps politics and policies are the epitome of such rhetoric behind his calls for America First. The post 9/11 world has become bitterly polarized due to the so-called War on Terrorism. Fundamental human rights can now conveniently be engaged and breached under the opaque laws of national security. Collection of enemy data through any means possible can be then fed to advanced war machines and people can be executed without a fair trial through drone strikes. There is line in the sand when it comes to state-sanctioned extra-judicial killings using personal data. No cases exists in any international courts on these breaches. This War-on-Terror has resulted in perpetual wars in Afghanistan (started October 2001- 18 years) and Iraq (started in March 2003- 15 years). Both these wars resulted in further armed conflicts in Syria (started March 2011- 8 years) and Yemen (started March 2015-4 years).

While the wars waged in the Middle East which some researchers terms as War for Oil, a different war started in the realm of personal data. United States and Europe were trying to reconcile a legal way to share global mass data[1] of persons ("Data Subjects"), in particular the European citizens for the so-called reasons of national security (European Union, 2016). The United States Transportation Security Agency (TSA) required the data under the US Home Land Security Act (Department of Homeland Security, 2002). The mechanism to deal with the mass data that was being collected was not a subject of general public debate. The US Security Contractor Edward Snowden[2] drew global attention to the United States Prism program of secret collection of personal data from around the globe

(Lee, 2013). UK was running its own covert collection of mass personal data without any legal oversight under its Tempora program.

Post Snowden revelations, the European Union Data Security Supervisors[3] jolted into action and EU Data Protection laws of 1990s were brought under review on war-footing (European Union, 2018). The Court of Justice of the European Union (CJEU), Luxembourg (European Union Anti-Fraud Office, 2016)[4] followed the lead of The European Court of Human Rights (ECtHR), Strasbourg in taking to task Big data[5] (Council of Europe, 2018) violations by technology giants such as Google[6] with Microsoft following suit (Bing, 2016) for personal data right so-called, Right to be forgotten.

It seems that the GDPR is a continuation in this series of evolutionary legislations that claim to satisfy the demands of the EU citizens to know the exact nature of how their personal data is being collected, stored and accessed. However, there are also theories about the protectionist policies within the EUs policy making that have given give rise to laws such as GDPR. The possibility of the GDPR influencing law making of similar laws in countries that are major socioeconomic partners of EU also demands some attention. We will therefore shed some light on the corresponding recent legislations pertaining to data in Turkey and China. The socioeconomic cost of such legislation is not easily measurable. Also, the transformative nature of such legislation is also not easily understood with a cursory analysis.

Our position remains neutral in terms of drawing our conclusions for the purpose of our theory about the transformative nature of GDPR. We neither support nor oppose the legislation as that is not our aim. Our aim is to simply analyse of the above-mentioned factors to better understand the transformative nature of GDPR on the economies of Europe.

2. Understanding Personal Data, Persons Identity and Information Management

Data in general and personal data in particular concerns the intrinsic core concept of identity. In short, identity is perhaps the underlying aim behind the concept of personal in data or information. We will be using data and information interchangeably throughout this paper. Information is the neutral element that is generic for the general description of activities concerning any physical body. We have based our argument for identity on Michel Foucaults revolutionary ideas about non-fixated notion of identity that concerns a legal person. Identity in Foucaults view is contingent, provisional, achieved not given (Leeuw and Jan 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 (Leeuw and Jan Bergstra, 2007) nature of an individuals identity within the community. The diachronic identity means that the individuals 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 individuals 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 frame-work 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 labelled as 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 our 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 then prescribes laws such as GDPR to enforce whatever aims at the core of prescribing such laws. We can therefore conclude that neither the idea of identity nor the management of identity is a settled concept. The plethora of literature on the subject is a testimony to our statement.

We will rely on this discussion for our later arguments on the definition of identity and data concerning a person within the EU data protection laws.

3. Historical Transformation of Europe & Data Protection Laws

There are two distinct and independent law-making bodies that prescribe laws that are enforceable across 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 end of the Second World War. We shall first deal with the Council of Europe. The idea for a United States of Europe is closely linked to the Truman Doctrine (McCullough, 1992). 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 Britains inability to offer any economic assistance to both the countries that were crucial to secure the Mediterranean gate-way to Europe. Following President Trumans 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. UK was forced to play a supportive role to the new leading power of the world, United States. Europe was to protect the interests of the United States for times to come. The collapse of the British Empire in late 1940s had forced Britain 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 UKs supportive role resulted in the London signing of the Statute of the Council of Europe (Council of Europe, 1949) on 5th May 1949. The statute came into force on the 3rd August 1949.

The Council of Europes most famous legislation is the European Convention of Human Rights ("ECHR"). ECHR was adopted by its 10 original members[7] on the 4th of November 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 provides for the European Court of Human Rights (ECtHR), Strasbourg. While ECHR protects fundamental human rights, there is no separate right within ECHR for personal data protection. The ECtHR 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 Right" (European Court Of Human Right, 2019).

Under ECHR data protection is not an absolute right. There are exceptions that can allow a High Contracting Party to the ECHR to interfere with this right of an individual under Article 8 ECHR. All legislations of the Council of Europe are called Conventions. The body of laws under Council of Europe remain distinct from EU law. The enforceability of ECHR extends beyond Europe due to its membership of non-EU countries such as Turkey.

The European Union (EU) is a distinct and unique legislative body of Institutions in the world. It is described as a unique social experiment by social scholars across the globe. In that it gave rise to a body of law that is enforceable across the continent of Europe and takes precedent over national laws of the member states in areas provided under its law. The EUs genesis can perhaps be attributed to the signing of the Customs Convention[8] in September 1944 (CVCE, 2018). The purpose of this treaty was to remove trade barriers between the Benelux nations[9]. The European Coal and Steel Community[10] (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 rebuilding of Europe. ECSCs 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 a 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.

The signing of the Brussels Treaty in 1965 and the Single European Act (SEA) in 1986 that paved the way for the 1993 Maastricht Treaty known as The Treaty on 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 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. Our interest for the purpose of this paper is in the development and implication of security and justice.

TEU also proposed the European Central Bank and the European Currency Euro. It also proposed a social chapter. Interestingly the UK while being an architect of the TEU negotiated an Opt-Out for both the proposal under the TEU. 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 (1-3) guarantee protection of personal data under Title II of Freedoms. This is not an absolute right under the CFR. The EU member states 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.

While Council of Europes laws concern distinctively with the principles that uphold democracy, protection of fundamental rights, and the rule of law. The EU law ensures broader and much deeper cooperation for socioeconomic freedoms as the principle aims of the 27-member state Union. The cornerstone of EU is to guarantee the so-called four freedoms, the free movement of people, goods, services and capital within the EU under Article 26(2)[11] TFEU. Both Council of Europe and the EU share the same fundamental values that guarantee fundamental rights, democracy and the rule of law (Council of Europe, 2018).

4. GDPRs Transformative Effect on European Identity

The Council of Europe's Convention 108 is the first European internationally enforceable and legally instrument on Data Protection. The European Unions first supranational data protection law came as a Data Protection Directive in 1995[12]. Article 16 TFEU affirms the distinct data protection right under Article 8 of the EU Charter for Fundamental Rights. GDPR enforced since May 2018, is according to the EU, an answer to protect personal data due to the raid advancements in information and communication technologies.

At the heart of all this European law making for the protection of data connected with the EU citizens is the idea of the European identity. It is a separate debate, and beyond the scope of this paper, how the European identity operates within the realm of various national identities amongst the EUs member states. The question before us for the purposes of data protection laws, is not of a commonly defined European identity that forms the various elements of the personal data, but it is to define what forms the frame of reference for the concept of identity in Europe. If we are able to understand this frame of reference, we argue, then it will be easier to understand the thought process that has led to data protection laws such as GDPR that propose to protect the freedoms connected with the identity of the citizens of Europe.

We have already established in our earlier discussion in the paper about that the definitions of identity, individual and personal data as not settled definitions. The reason for this discussion and our earlier analysis of identity on the basis of social-political theories is that the European Legislators have defined identity and its related data in the one-dimensional area of politics. We argue that it is easier to express identity politically as it then consequently easier to exploit for the purposes of creating a common political platform to advocate any or all issues concerning the national or supranational. Therefore, we assert that all aspects of data that the GDPR proposes to protect are political identity based when it comes to the individuals personal data protection rights.

Since we have established that within the context of EU, the identity issue has been reconciled as the political identity of the Europeans and its further translation in the concept of European Citizenship. EU Citizenship[13] concept was first described within the 1993 Maastricht Treaty. Article 8 TEU, which is now Article 20 TFEU conferred the European citizenship to all individuals who are nationals of the EU Member States. To understand this fully within the context of identity the supranational nature of EU Citizenship is intrinsically linked with the national identity of the person. Also, if the national identity confers a right to protect the person identity or data, by default the supranational identity or data must also be protected. In both the cases, data protection remains a right regardless of any national laws within the EU Member States that may or may not afford the same protection as legislated by the supranational EU laws such as GDPR. EU further issued Directive 2004/38 so-called Citizenship Directive to provide detailed legislation ensuring free movement of Union citizens.

There is an elaborate body of Case Law of the Court of Justice of EU that pertains to breaches of data protection rights of the EU citizens by their host states or their states of origin. The detailed discussion of such cases is beyond the scope of this paper. We would however make a concluding remark about the repeated emphasis of the Court to ensure free movement by expounding on the principle of freedom of movement and non-discrimination on any grounds as laid down in the Charter of Rights. While data protection is a separate right in the European Union as explained earlier in our discussion, the management of data to enforce the principle of freedom of movement is not very clear either in the EU legislation nor in the Case Law. We refer to Article 21(1) TFEU that makes it obvious that the right conferred by the freedom of movement is subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect.

The scope of the limitations that allow interference with the distinct right of data protection conferred by Article 8 of EUs CFR and an extension of ECHRs Article 8 right for respect of personal family includes the States right of interference under official duties. Article 51 TFEU describes what constitutes the exercise of Official Authority:

"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 this law suggests a very broad definition of the exercise authority. The certain activities are not clearly defined that restricts the exercise of official authority that may result in interference with the data protection right.

The landmark European Court of Justice case of Reyners v The Belgian State[14] defined the official authority:

"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."

This definition of official authority confirms our thesis on the political nature of identities and rights under the EU law. However, the use of official authority to processing or managing of personal data has been defined narrowly by the CJEU in the case of Commission v Italy (Data Processing)[15]. The Court held that the exception of Official Authority did not extend to the design and operation of data-processing systems for public authorities.

Let us summarize our discussion on the topic of the role of the supranational nature European identity and the national identities for the purpose of data protection. The EU laws related to data do not seem to extend beyond the political identity of the citizens of Europe. The nature of the data that forms part of the personal data is based on the political identity principles surrounding events that are defined under the data subjects life within the political identity of national and European citizenship. Also, the exclusive right conferred by Article 8 of the European Charter of Fundamental Rights for data protection seems to suggest that this right is assured within limitations for the purposes of the EU citizenship.

The use of the word identity specifically within the language of the seminal Case Law of CJEU suggests that identity remains the core defining word when it comes to any data that pertains to a legal person and for the purposes of such data protection.

In the seminal joint cases of Volker und Markus Schecke GbR[16] concerning 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, recognised 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 case referred above clearly indicates that data protection concerns the identity of legal person conferred through the Charter under the definition of a legal person who is officially entitled to be identified as a natural person. The word officially lays emphasis on the political construct for the meaning attached to the identity of the person. The CJEU in the same case laid down the guidelines when the data rights could be interfered with by the EU or Member State Authorities (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 recognised 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 limitations on the right of data protection are limited by lawful tolerance in relation to the rights. The lawful right of the state to interfere flows from the political rights of the State under the EU or the Member States laws. The legal guidance therefore again points to the protection of data rights being political identity rights with regards to the scope of those rights even within the social implications of family and personal freedoms.

The EU Directive 2006/24/EC was formulated 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 and communication identities of the subscribers within EU. The blanket storage and access could be between six months and up to two years. The mass data collection and storage of such ICT identities was challenged in the famous Digital Rights Ireland[17] case. The ECJ declared EU Directive 2006/24/EC to be invalid[18] and in violation of the Article 8 Charter Rights of Data Protection. The Court also laid carefully selected guidelines for how the interference could be justified. The criteria for allowing interference with data protection rights require a proper legal basis, for the purpose of fighting serious organized crime including terrorism and should not go beyond strictly necessary and data must be retained within the EU and within strict limits of retention period.

The wordings of the case elaborate and strengthens our earlier constructs of identity linked to an individuals resurfacing in multiple events in a community to form the basis of any identity specific data to be generated for the purposes of personal data. The Court held (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."

CJEUs cases of Watson[19] and Schrems[20] are powerful and assertive judgments of the Court of Justice on the matters of indiscriminate retention and invalidity of the Safe Harbour Decision[21] concerning data protection rights guaranteed under Article 8 of the Charter (Court of Justice of European Union, 2015).

In Watson the Court held that the retention of a person's ICT data providing exact location would provide precise conclusions for the purposes of the data concerning the private lives that includes every day habits. This reference to the important issue of protecting the identity of the data subject with relation to their resurfacing in various community events again strengthens our theory that not only is the identity politically defined, the establishment of that identity as being unique to other members of the society is intrinsically linked to the resurfacing of the individual in various community events. The questions of the data retention were raised because of the powers conferred for data retention and access by the Law Enforcement agencies in the UKs Investigatory Powers Act 2016.

In Schrems, the Court has declared the Safe Harbour Agreement between United States and EU for retention and access of EU Citizens data by US agencies for the purposes of law enforcement. The Court not only declared the self-certified safe status of US data storage and access facilities, it also raised the matter of mass surveillance being inherently a possible means to interfere and breach the data protection rights regardless of the safeguards in place to prevent any abuse.

The GDPR came on the heels of the CJEUs decision to declare the US-EU Safe Harbour Agreement invalid. We are in no way suggesting any link between the Schrems judgment and the rapid approach adopted by the EU to come with a supranational instrument for data protection, one that would be comprehensive and allow no national legislations to be enacted by the Member States. There are, however, some clues that suggest a remote linkage between the two.

The European Data Protection Supervisor added trust[22] as an essential condition for evolution of ICT products based on the EU laws protecting the data rights of its citizens. Essentially EU law makers were advocating an ethical framework for developing ICT services that could satisfy the data protection rights conferred by Article 8 of the Charter. This brings us full-circle to our earlier discussions on the reasons for the implementation of GDPR.

Since EUs legal instrument for protecting the data rights was declared invalid by the Court of Justice, the EU law makers took the opportunity to bring another dimension to the one-dimensional political definition of identity by adding the social dimension of trust to the definition. The reaction of the US Attorney General to the addition of this social dimension to the identity data treatment by the EU law makers is very strong in its opposition. The U.S. Attorney General Loretta Lynch raised the so-called War on Terror agenda to oppose the ethical inclusion for the purposes of data by warning of possible inability to prevent future terrorist attacks if personal data was ethically protected. While this subtle connecting of dots is not the major theme of our paper, we offer this as a point-to-ponder to our readers. Remember we elaborately explained the US Truman Doctrine and Marshall Plan in our introduction and the US international relations doctrines involving Europe post Second World War.

The inclusion of Anti-FISA[23] clause in the GDPR was the result of US Security Contractor Edward Snowdens revelations about the covert global data collection under the US PRISM[24] program (Braun et al, 2013). The draft clause of GDPR Article 43(a) which is now 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."

The clause allowed for preventing of any data disclosures of any data subject of EU to any 3rd country regardless of the legal orders without the presence of an internationally binding agreement between the EU and that country. This is a powerful clause that would prevent any of the EU Member State from violating the data protection rights of any EU Citizen. UK was the first country to opt-out of this clause being a close ally of the US in collecting mass data for the purposes of covert intelligence accessed jointly by the US and UK intelligence agencies (MacAskill et al. 2013). UKs 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 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 Judicial Review within the UK and Ireland and also the possibility to approach the Court of Justice remains open for the enforcement of Article 48 GDPR.

For the purposes of our theory that GDPR is a law that is transformative in nature, we have laid-out a plausible argument that the post 9/11 so-called War on Terror has some influence in the EU law making leading to GDPR. The period between the declaration of the invalidity of the US-EU Safe Harbour mass data retention and access and the run-up to the reforms that led to the legislation of

GDPR, another identity of Europe emerged due to this transformation. The European Security and Defence Identity (ESDI) is the result of 1994 NATO Ministerial meeting in Brussels. The analysis of the defence implications of this defence & security identity of Europe is beyond the scope of this paper. What is relevant for the purposes of this paper is the transformation of Europe due to legislations that led to the formulation of GDPR and GDPR itself. North Atlantic Treaty Organization (NATO) in a publically declared document revealed the aims Development of the European Security and Defence Identity (ESDI) within NATO (NATO, 1999). Interestingly one of the seven areas of focus for the development of the ESDI within NATO is:

"Arrangements for the effective sharing of information, including intelligence, that NATO and the WEU (Western Europe Union) would require in the context of WEU-led operations."

The wording of this aim is similar to the wordings that are existing in the US-EU Safe Harbour mass data retention and access agreement that was declared invalid by the Court of Justice of the European Union. For the purpose of our paper it is sufficient to assert that GDPR is not a narrowly defined data protection law rather it covers the identity data for the citizens of the EU that includes their political as well as social identity that is trust based. We also argue that the security and defence identity of European Union itself that provided for effective information sharing for the purposes of intelligence with its defence partner NATO is also transformed by the GDPR. By analogy we can happily conclude that the security and defence of the EU and by its definition Europe would see transformation due to GDPR. The European defence identity ESDI came with its own set of problems and strategic policy issues which is beyond the scope of this paper. We will conclude our discussion with these thought-provoking words by Dr. F. Stephen Larrabee of RAND (Larrabee, 2000), USA which he spoke before the United States Senates Committee on Foreign Relations:

"We should be striving for a new Transatlantic Bargaining which we remain engaged in Europe while encouraging our allies to assume more responsibility for security in Europe -- but also outside of it. ESDI could contribute to such a new Transatlantic Bargain."

These words resonate of the Truman Doctrine and Marshall Plan of 1940s for Europe continuing to the present times. The idea of Western Europe Union (WEU) (European Union, 2016) combined defence emerged from the 1948 Treaty of Brussels signed by the UK, France and the Benelux countries. The ESDI is a creature of the 1948 Treaty of Brussels (NATO, 2009). The European Identity for the purposes of its defence are enshrined in ESDI. This identity is linked to other supranational of laws of the EU for security that include the GDPR for Data Sharing and Data Protection for the purposes of battle-field intelligence and cyber security. The framing of GDPR and its transformative nature concerning Europe's defence and security benefits from the European legal experience arising from program such as PRISM, TEMPORA and Safe Harbour as explained earlier.

Mr. Jan-Philipp Albrecht (Fleming,2015) the German Member of EU Parliament and German representative for the consultative committee for GDPR attributed the delay in the implementation of GDPR due to the duel reasons of increased covert access of European data by intelligence agencies and national self-interests of Germany, France and UK to delay GDPRs implementation. The implementation of the GDPR, we assert is not only transformative for the security and defence of the EU, at the same time it has far reaching consequences for any future covert interference with the data of European Union population.

5. GDPR and the Socioeconomic Transformation of Europe

The GDPR has come into force recently, since May 2018. It is far too early to critically examine if it has any tangible impact on the economies of EU or for its economic transformative nature. What is clear is the thoughts of the EU leadership (Reding, 2014) concerning the economic significance of personal data of its citizens. The emphasis on the element of trust in the development of the ICT based use of personal data of the Eu citizens started to echo more clearly. The large corporation's view of data protection legislations as stumbling block to the development of new ICTs was not accepted as a relevant consideration by the EU leadership. Balance was rather titled towards assigning top priority a more robust legal framework for data protection in its use for economic benefits. It must be remembered that such reflective thought on part of the EU law makers follows in the foot-steps of Edward Snowdens revelations for covert mass data retention and access by US and UK intelligence agencies. It seems that the EU law makers did not discard the economic espionage element of the same data retained by the intelligence community.

UK remained and still remains an opponent of the GDPR since the landmark decisions of Watson[25], Digital Rights Ireland[26] and Schrems[27] by the Court of Justice declaring mass data retention and access to be unlawful. A UK based economic survey[28] of 504 businesses of all sizes published its finding that over 80% of the surveyed businesses could neither quantify the compliance cost of GDPR nor could they quantify their existing cost of any data protection measures (London Economics, 2013). The survey was the result of UKs Information Commissioners office.

The economic relevance of the GDPR within the EU flows from Article 217 TFEU (Treaty for the Functioning of the European Union) that requires all Member States of the EU to abide by the law that states,

"The Union may conclude with one or more third countries or international organisations agreements establishing an

association involving reciprocal rights and obligations, common action and special procedure."

The European Economic Association (EEA)[29] through its European Free Trade Association (EFTA) Agreements formed the single largest economic market in the world (EFTA, 2018). 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 economy. Article 288 TFEU refers to the binding nature of EUs 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 pursuant to its Article 102(1) through 102(6) prescribes five-stages in compliance with EC Regulation No.2894/94 concerning enforcement of EU secondary law such as GDPR across the Member States signatory to the EEA. So far the Stage-1 has decided that GDPR is EEA relevant. The subsequent phases involve participation by the representatives of the EEA Member States to provide consultative advice to the EU Commission that would then through the EU legislative process make the final proposal to the EU Parliament for necessary adjustments if required in the GDPR. It must be noted that GDPR is fully adopted and enforced since May 2018. The purpose of this EU Legislative process concerning Europes Economic Assocation (EEA) is to ensure that the process would result in the most transparent and predictable application of GDPR within the EEA. This process will also ensure the continued stability and working of the European Economic and Information Markets. Our above brief yet focused legal analysis of the GDPR as a supranational law concludes that GDPR has a huge impact within the European markets through its adoption for the purposes of European Economic Assocation (EEA) under Articles 217 and 288 of TFEU will result in the transformation of the European economic landscape.

The last part of our analysis of the economic transformative nature of GDPR concerns its impact outside the legislative boundaries of EU law. In the international arena of law concerning data, identity and information, the issue concerns balancing the economic interests and innovation liberalization with the competing laws for fundamental freedom for privacy and data protection rights. This is a complex problems to solve for those entrusted with making global laws as there is no agreed upon global framework for regulating data flow across jurisdictional maze of often diametrically opposing regulatory regimes.

The latest literature on the topic of legal strategies to deal with these diametrically opposing jurisdictional complexity of legislation related to data handling and its flow for the purposes of economic and trade internationally suggests three solutions (Mitchell and Mishra, 2018). For the purpose of this paper we aim to look at the three leading strategies and compare it with EUs GDPR. United States Constitution does not provide any specific data protection rights. The Constitution of Japan also does not provide any such protections. Both USA and Japan, who are leading trade partners of EU adopted the Market-Based strategy to apply minimum restraints through legislative and regulatory interventions in the area of data protection. The ICT Industry leads the way in advising the legislature on polices that balance the data privacy and protection rights verses the economic interest of the market.

China, Russia, France and the UK, all major trade partners of EU have a Cautious strategy towards data protection and privacy concerning economic policies and regulations. Excluding France and UK, China and Russia also use State-Censorship to strictly regulate the ICTs which resultantly also impacts the economic activities connected with flow of data and privacy rights. Cyber Security is treated as an exclusive policy making domain of the national security institutions for all matters concerning storage and excess of mass data.

The third strategy is the Interventionist in nature that aims to seek comprehensive coverage of all aspects of data and information regardless of its application such as economic, social or cyber security. Canada, Australia are leading counties that apply such legislations across the entire domain of data-based applications.

The GDPR also falls under the Interventionist strategy as it is a supranational legislation that does not concern itself with the existing legislation on data protection and privacy in any of its Member States. Due to its supranational nature, GDPR has direct 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. It is this doctrine of Horizontal Effect of the GDPR that companies and individuals who are in violation of GDPR can be subjected to the remedies prescribed under the GDPR and all provisions of GDPR are directly enforceable against such entities. Cases such as Google v Spain[30] brought before the Court of Justice 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 by the EU Commission, which 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. This is not a straight forward element that can easily assessed for the

purposes of assessing the level of protection that will be afforded to the data of the EU citizens. The complexity of the physical infrastructure of global ICT communications networks where data jumps multiple-jurisdictions within a Nano second leaving data impressions that may or may not be permanent within the narrow definitions of storage adequacy of protection etc poses a huge complexities for assessments. It would be relevant to this discussion that such assessments may not only delay the process of assessments entrusted to EU Commission, it may also pose some international obligation issues concerning bilateral trade agreements affected by Article 45(2) compliance.

Also, EU Commission position for the purposes of adequacy requirements pertaining to data pursuant to Article 45 GDPR creates a preference for those countries outside EU that fall in the list of countries that are already considered satisfying the adequacy requirement under Article 45 GDPR. The international obligations of EU under World Trade Organizations (WTO) GATS[31] (WTO, 2018) MNF[32] (WTO, 2018) structure may create potential violations under GATS Article XVII[33] due non-comply with adequacy requirements under GDPR Article 45. There is no provision for derogation from GATS Article XVII for EUs positive obligation to give access to its national markets under GATS that concern services using data. We are avoiding a detailed legal discussion on this point and would only elucidate that fact that GDPR compliance may create possible violations of GATS by EU in the foreseeable future as there is no existing Case Law to help navigate such potential violations due to divergent legal obligations under GDPR and WTOs GATS.

We had intentionally left the discussion on the GDPRs possible transformative impact on EUs one of the largest trade partners Turkey. In our introduction we had established that post World War II, the USA emerged as the new global power replacing the British Empire. US placed significant importance on Turkey being a gate-way nation through the Mediterranean Sea and Aegean Sea. Our discussion indicated the reasons through our references to the Truman Doctrine and the Marshall Plan. For reasons beyond the scope of this paper, EU has always treated Turkey at-an-arms-distance. Turkey has been denied membership of EU due to stiff opposition from Greece based on the Cyprus issue[34]. Turkey is one of the High Contracting Parties to Council of Europes fundamental rights instrument ECHR. While ECHR does not have any specific right for data protection, the Article 8 right to privacy and family includes the right to data protection as also discussed earlier. Turkey has recently legislated its data protection law that is based on the broad principles of the EU Directive 95/46/EC that has been replaced by the GDPR. Turkeys data protection legislation followed Turkeys ratification of ECHRs Convention 108 for the protection of personal data. The new Turkish legislation for data protection has differentiated itself from EUs GDPR for the purposes of consent. While GDPR does not stipulate consent with any degree of severity, the Turkish legislation calls for strict consent in cases of sensitive data and change in the scope of data for the purposes of data protection. Both GDPR and Turkish data protection legislation give the data subject exclusive powers through the requirement of consent. The exceptions in both the cases remain exclusively in the areas of law enforcement, fighting serious crime, terrorism and national security. It seems that the Turkish data protection law is following the transformation of laws in Europe and it would consequently transform the socioeconomic landscape of Turkey. It remains to be seen if these legislative efforts by Turkey would suffice the law makers in EU to continue to positively consider Turkey for EUs membership and further cooperation in economics and trade.

Conclusion

The EU is a unique experiment of a supranational nature that created the largest single economic market with its unique set of laws. The ensuing chaos that followed World War II created a new world order that shaped what we know as Europe of today. The supranational nature of the EU laws is a new legal order of international laws. GDPR is a continuation of that legal order of international laws. GDPR is not a law that stands merged within the wide body of the European Jurisprudence. It is a unique legal instrument that is transformative in nature and has yet unknown and perhaps infinite repercussions for not only the EU but the entire world. The European Convention of Human Rights and the EU Charter for Fundamental Rights set the stage for various Constitutional provisions for rights protection around the world. GDPR also has the potential for such transformative impression to give rise to a new generation of international rights concerning data. To confine GDPR to the narrow scope of global economy would be confining the scope of the technology that it aims to regulate. The lessons of World War II that shaped Europe must remain in our sight of we are to fully understand the nature of the laws that we legislate today.

Notes

1) "The European Commission and the U.S. Department of Commerce reached on 2 February 2016 a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (IP/16/216). This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses."

2) A classified PowerPoint presentation leaked by Edward Snowden states that PRISM enables "collection directly from the servers" of Microsoft, Yahoo, Google, Facebook and other online companies.

3) As of 25 May 2018, the Article 29 Working Party will be replaced by the European Data Protection Board (EDPB). The EDPB has the status of an EU body with legal personality and is provided with an independent secretariat.

4) Case Law Data Protection, CJEU.

5) Case Law Data Protection, ECtHR.

6) Google v Spain (Right to be Forgotten). Decided 13 May 2014. Case No. number C-131/1. Held:' that an Internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties, upholding a right of erasure'.

7) 10 original signatory states to ECHR are: Kingdom of Belgium, the Kingdom of Denmark, the French Republic, the Irish Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Kingdom of Norway, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland.

8) The Netherlands–Belgium–Luxembourg Customs Convention.

9) Belgium, Netherlands, and Luxembourg, Benelux is from using first alphabets of signatory nations, (BeNeLux).

10) Schuman Plan 1951 was proposed by French economist Jean Monnet and tabled by the French Foreign Minister Robert Schuman

11) Article 26(2) TFEU: The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.

12) Directive 95/46/EC. Directive for protection of personal data and free movement of such data

13) Treaty of Maastricht in 1992: Article 20(1) TFEU, Citizenship of the Union is hereby established. Every person holding the nationality of a Member State shall be a citizen of the Union. Citizenship of the Union shall be additional to and not replace national citizenship.

14) CJEU: Reyners v The Belgian State (Case 2/74) [1974] ECR 63

15) CJEU: Commission v Italy (Data Processing) (Case C-3/88) [1989] ECR 4035

16) CJEU: Joined Cases C-92/09 and C-93/09

17) CJEU: Digital Rights Ireland C-293/12

18) CJEU: Joined Cases C-293/12 and C-594/12, Judgment April 8th, 2014

19) CJEU: Joined cases C-203/15 and C-698/15.Tele2 Sverige AB v. Post- och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others

20) CJEU: C-362/14. Maximilian Schrems v. Data Protection Commissioner

21) The US systems to store EU Citizens data allowed under the jointly agreed scheme between USA and EU was declared inadequate and in violation of the protection afforded to EU Citizens for the purposes of their data protection rights.

22) Update Opinion 03/2015 on GDPR: 9 October 2015 statement by European Data Protection Supervisor Giovanni Butarelli

23) FISA is United States Foreign Intelligence Surveillance Act that allows collection of foreign intelligence by US agencies

24) Secret to PRISM Program: Even Bigger Data Seizures

25) CJEU: Watson & Other Joined Cases C-203/15 and C-698/15

26) Digital Rights Ireland C- 293/12

27) CJEU: Schrems C- 362/14

28) Analysis of the potential impact of GDPR, implications of the ICO's Draft Guidelines on consent.

29) EEA: "The Agreement on the European Economic Area, which entered into force on 1 January 1994, brings together the EU Member States and the three EEA EFTA States — Iceland, Liechtenstein and Norway — in a single market, referred to as the "Internal Market"

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

31) 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.

32) MNF: WTO's 'Most Favoured Nation' concept allows for equal trade advantages by the recipient country.

33) 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'.

34) On-going dispute between Turkey and Greece since 1974, the dispute started with British occupation of the Islands from Ottoman's in 1925.

REFERENCES

KNOMAD (2015). Return Migration and Re-Integration into Croatia and Kosovo. Croatian Heritage Foundation, May 11-12, Zagreb.

BING (2016). Bing to Use Location for RTBF. (Accessed: 02.01.2017), https://blogs.bing.com/search/august-2016/bing-to-use-location-for-rtbf.

Council of Europe (2018). Case Law of the European Court Human Rights. (Accessed: 13.12.2018), https://www.coe.int/en/web/data-protection/echr-case-law.

Council of Europe (1949). Statue of the Council of Europe https://rm.coe.int/1680306052Council of Europe (2018).

Court of Justice of the European Union (2015). Press Release No 117/ 15. (Accessed: 25.02.2018), https://curia.europa.eu/ jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

CVCE (2018). Historical Events: The Netherlands–Belgium–Luxembourg Customs Convention. (Accessed: 05.06.2018), https://www.cvce.eu/en/epublications/eisc/historical-events.

EFTA (2018). EEA Agreement. (Accessed: 21.11.2018), https://www.efta.int/eea/eea-agreement.

European Comission (2016). Fact Sheet. (Accessed: 07.03.2018), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

Council of Europe (2018). The Council of Europe and the European Union. (Accessed: 08.07.2018), https://www.coe.int/en/web/ portal/european-union.

European Comission (2018). 2018 Reform of EU Data Protection Rules. (Accessed: 15.09.2018), https://ec.europa.eu /commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

European Court of Human Rights (2019). Personel Data Prtotection. (Accessed: 10.01.2019). https://www.echr.coe.int/Documents/ FS_Data_ ENG.pdf.

European Union Anti-Fraud Office (2016), Summaries of EU Court Decisions Relating to Data Protection 2000-2015. (Accessed: 17.05.2018).https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf.

European Union (2016). Shaping of a Common Security and Defense Policy http://eeas.europa.eu/csdp/about-csdp/weu/index_en.htm. Accessed 2 July 2018.

European Union (2018). European Data Protection Board News. (Accessed: 09.01.2019), https://edpb.europa.eu/

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications. The Guardian, 21, 2013.

Fleming, J. (2015). EU Law Maker Warns Of Data Protection Rules Detay Till 2016. (Accessed: 20.01.2019). http://www.euractiv.com/ sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100.

Homeland Security (2018). US Home Land Security Act 2002. (Accessed: 25.12.2018).https://www.dhs.gov/homeland-security-act-2002.

Larrabee, F. S. (2000). RAND The European Security and Defence Identity and American Interests Washington, D.C.. (Accessed: 23.01.2019), https://www.rand.org/content/dam/rand/pubs/testimonies/2005/CT168.pdf.

Lee, Ti. B (2013). Heres Everything We Know about PRISM to Date. (Accessed: 05.12.2018).https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?noredirect=on&utm_term=.da53c139509b.

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

London Economics (2013). Implications of the European Comissions Proposal for A General Data Protection Regulation For Business. (Accessed: 18.01.2019). https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf.

McCullough, D. (1992). Truman. New York: Simon & Schuster.

Nash, J. R. (1976). Darkest Hours. Rowman & Littlefield, London.

Mitchell, A. D. & Mishra, N. (2018). Data at the Docks: Modernizing International Trade Law for the Digital Economy. (Accessed: 16.02.2019), https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm.

NATO (1999). Development of the European Security and Defence Identity within NATO. (Accessed: 02.02.2019), https://www.nato.int/docu/comm/1999/9904-wsh/pres-eng/05esdi.pdf.

NATO (1948) The Brussel Treaty. (Accessed: 05.02.2019), http://www.nato.int/cps/en/natohq/official_texts_17072.htm.

Reding, V.(2014). A Data Protection Compact for Europe. (Accessed: 02.09.2018), http://europa.eu/rapid/press-release_SPEECH-14-62_de.htm.

WTO (2018). The Basic Rules for Goods. (Accessed: 26.12.2018), https://www.wto.org/english/tratop_e/region_e/regatt_e.htm.