THE RIGHT TO PRIVACY IN THE AGE OF PANDEMICS "A STUDY IN GERMAN AND EUROPEAN LAW"

Dr. Mohamed Aboubakr Abdelhadi
Public Law Assistant Professor
Faculty of Law
Mansoura University &
Sultan Qaboos University

Abstract

The right to protection of personal data arises where personal data requires processing, usage ad storage. It is therefore a process requiring extracting of personal data from an individual and processing it without infringing on the person's rights to protection of data as well as privacy. Contact tracing technology is used at the time of epidemics, and it is a technique by which people can be monitored to find out their interactions with a person who has tested positive for a specific infectious disease. This process was previously done as a means of managing infectious diseases so as to shorten the response time. Specifically, for the Covid-19 pandemic, the process has been digitized across the globe. In dealing with covid-19, the state should take into consideration the need to balance between the right of individuals to good health and the right to protection of data as contact tracing and following up on infections is paramount in managing the corona virus pandemic. This can be through setting out legislation that limits the use of information collected for the purposes of corona-virus for that limited purpose in the required institutions. Since Coronavirus is an emerging problem, more needs to be done in terms of research to understand how to deal with it effectively and in balance while protecting the rights and freedoms of individuals.

The Paper discuss the legal principles on the right to personal privacy in both Germany and the European Union, through a comparative study between European Union General Data Protection Regulation (GDPR) which came into force on 25th May 2018, and German Federal Data Protection Act (BDSG) of 30 June 2017, amended by Article 12 of the Act of November 20, 2019. it will delve deeper on the relationship between the protection of personal data and other fundamental rights and freedoms. Lastly it studies the balancing between measures that could help track and contain the virus while safeguarding the privacy of individuals.

Key Words: Fundamental Rights - Personal Data - Proportionality - Technology Surveillance.

الملخص

ينشأ الحق في حماية البيانات الشخصية عندما تتطلب البيانات الشخصية معالجة واستخدام تخزين، لذلك فهي عملية تتطلب استخراج البيانات الشخصية من الفرد ومعالجتها دون التعدي على حقوق الشخص في حماية البيانات وكذلك الخصوصية. تُستخدم تقنية تتبع الاتصال في وقت انتشار الأوبئة، وهي تقنية يمكن من خلالها مراقبة الأشخاص لمعرفة تفاعلاتهم مع شخص ثبتت إصابته بمرض معدي معين. تمت هذه العملية في السابق كوسيلة لإدارة الأمراض المعدية وذلك لتقصير مدة احتواء الوباء، وتحديدًا، بالنسبة لوباء **Covid-19**، حيث تمت رقمنة العملية في جميع أنحاء العالم في التعامل مع هذا الوباء. يجب على الدولة أن تأخذ بعين الاعتبار ضرورة الموازنة بين حق الأفراد في التمتع بصحة جيدة والحق في حماية البيانات، حيث إن تتبع المخالطين ومتابعة الإصابات أمر بالغ الأهمية في إدارة هذه الجائحة. يمكن أن يكون ذلك من خلال وضع تشريعات تحد من استخدام المعلومات التي تم جمعها لأغراض فيروس كورونا المستجد إلا لهذا الغرض المحدد في المؤسسات المعنية. نظرًا لأن فيروس كورونا مشكلة مستجدة، يجب القيام بالمزيد من حيث البحث لفهم كيفية التعامل معه بشكل فعال ومتوازن مع حماية حقوق وحريات الأفراد.

يناقش البحث المبادئ القانونية المتعلقة بحماية الحق في الخصوصية الشخصية في كل من ألمانيا والاتحاد الأوروبي، وذلك من خلال القيام بدراسة مقارنة بين اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) التي دخلت حيز التنفيذ في 25 مايو 2018، وقانون حماية البيانات الفيدرالي الألماني (BDSG) الصادر في 30 يونيو 2017، والمعدل في 20 نوفمبر 2019. بالإضافة لذلك يتم بحث حدود العلاقة بين الحق في حماية البيانات الشخصية والحقوق والحريات الأساسية الأخرى، وأخيرًا، يبين البحث آلية تحقيق التوازن بين الإجراءات التي يمكن أن تساعد في احتواء الوباء وحماية خصوصية الأفراد.

كلمات مفتاحية: الحقوق الأساسية – البيانات الشخصية – التناسب – المراقبة الإلكترونية.

INTRODUCTION:

In late 2019 several patients in Wuhan China were hospitalized with pneumonia like symptoms, with the origins of the disease linked to a seafood and wet animal market. This was later to be known as a new Coronavirus named Covid-19. The major issue with this virus, was that one maybe asymptomatic, meaning that they may be infected and go about their business while infecting the rest of the people they interact with, without exhibiting any symptoms. The disease was found to majorly affect all those who have an underlying problem such as diabetes and hypertension. Further the most vulnerable in the population are the old who may be above the age of 60 years.[1] As a result, the World Health Organization declared the Covid-19 virus a public health emergency of International concern, due to its fast spread of infections and resulting deaths.[2]

One of the ways in which different countries tried to contain the virus is by the use of contact tracing and population surveillance but with a technological angle by the use of phone location data[3] or the use of contact tracing apps.[4] By the introduction of technology that heavily relies on personal data, it begs the question, how well is the data that is collected protected and is it done so in accordance to the data laws in both Germany and the European Union (EU) at large.

The problem this research seeks to investigate is how far the right to privacy, and any other supporting right, may be interfered with so as to enhance the right to health and any other right that seeks to protect the citizenry from the novel Covid-19 virus. This research pursues the

---

[1] Hussin A. Rothan and Siddappa N. Byrareddy, 'The Epidemiology and Pathogenesis of Coronavirus Disease (COVID-19) Outbreak' (2020) 109 Journal of Autoimmunity.

[2] Klaudia Klonowska, Pieter Bindt, ' The COVID-19 pandemic: two waves of technological responses in the European Union' HCSS 2020 <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[3] Remco Takken, 'EU Member States Loosen Privacy Rules for Location Data to Contain COVID-19' <https://www.geospatialworld.net/blogs/eu-member-states-covid-19/> accessed 5 August 2020.

[4] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' HCSS 2020 <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

delicate balance needed to be taken by countries who are using technological ways of disease management, with the protection of rights that may be interfered with in the process for example the right to privacy interfered with by collection of data to monitor movement of the population.

This research is important in understanding the proportionality of the steps taken by nations in combating the Covid-19 pandemic through the use of technology. It contributes to the international discourse on the use of data protection in protecting the general population from a pandemic such as the present one. Apart from that, it is an important discussion on the protection of data and aims to contribute to the discussion that enhances the need to look at technology and data collection closer so as to enhance the right to privacy. The world has been faced by a new situation where the use of technology has been in the frontline in protecting the population. It is timely, as several countries around the European Union have launched the use of contact tracing apps as one way of mitigating the spread of the virus.

The objectives of this research are to analyze the effects of the right to privacy and how different countries have been able to protect this right. It brings awareness to the use of such methods and the standard that should be upheld if countries decide to go down this route. Furthermore, the objective of the study is to unpack what the use of contact tracing and population tracing by the government entails and to analyze whether the steps taken, adhere to the right to personal privacy in Germany and the EU at large.

The research methodology is undertaken through secondary research method by use of already existing data.[5] The division of research involved is descriptive research whereby the idea of this research is to well define an opinion, attitude or behavior by people on a given subject.[6]

The paper will have three chapters that outline the following:

---

[5] 'Secondary Research- Definition, Methods and Examples. Questionpro' (*QuestionPro*, 2020) <https://www.questionpro.com/blog/secondary research/#:~:text=Secondary%20research%20or%20desk%20research,involves%20using%20already%20existing%20data.&text=Secondary%20research%20includes%20research%20material,already%20filled%20in%20surveys%20etc.> accessed 5 August 2020.

[6] Fluid Surveys Team, '3 Types of Survey Research, when to Use Them, And How They Can Benefit Your Organization! - Fluidsurveys' (*FluidSurveys*, 2020) <http://fluidsurveys.com/university/3-types-survey-research-use-can-benefit-organization/> accessed 5 August 2020.

Chapter I: This chapter will discuss the principles on the right to personal privacy in both Germany and the European Union. These approaches will be analyzed in in depth detail. Furthermore, the laws of the Germany and the European Union shall be compared and determined if German privacy laws really adhere to European Union law, as the Union law is always superior to member states laws.

Chapter II: A close study will be carried out in contact tracing and the use of technology; this includes technology surveillance in digital tracing mechanisms, geographic tracing of citizens using applications based on personal data and how it has made it possible to follow developments of the pandemic in Germany and other EU countries. This study will include Germany and other EU member states as well as laws pertaining to this in Germany and the EU.

Chapter III: This chapter will address the relationship between protection of personal data in Germany and other fundamental rights and freedoms in the European Union. This chapter will also study the protection of the right to privacy in Germany while collecting and processing personal data. Furthermore, it will delve deeper on the relationship between the protection of personal data and other fundamental rights and freedoms. Lastly it will study the balancing between measures that could help track and contain the virus while safeguarding the privacy of individuals.

Finally, the paper will discuss the most important conclusions and recommendations on the study of the right to privacy during the corona virus pandemic, which will concentrate on German and European Union laws.

CHAPTER 1: PRINCIPLES ON THE RIGHT TO PERSONAL PRIVACY IN THE EUROPEAN AND UNION GERMANY

1- Europe's position:

Protection of personal data which has been accessed from a person is a fundaments right[7] that is supported by the Functioning of the European Union Treaty (TFEU) which also offers protection to personal data.[8] The charter necessitates the data collected to be processed in the right way and in accordance with the reasons stated or any other reasons provided by the law and with the permission of the person whose date has been collected. [9] The fact that the charter gives a separate right of data protection away from the right to privacy clearly demonstrates that the right to data protection is of much importance.[10] The General Data Protection Regulation (GDPR) is a regulation for protection of data. It is the major law in this matter in the EU. This regulation has acted as an important step when it comes to strengthening the protection of an individual's personal data in this fast growing digital era The GDPR (Regulation (EU) 2016/679) was substituted by directive 95/46/EC. It is directly applicable into member states law and has a consistent effect in all member states.[11] The principle of EU law being directly applicable means those individuals who have been affected can invoke European Union law in national or European courts, dependent on certain European Acts.[12] This conforms to the principle of precedence where European law is always superior to national law.[13] This simply means that

---

[7] European Union Charter of Fundamental Rights article 8(1)
[8] Treaty on the Functioning of the European Union article 16(1)
[9] European Union Charter of Fundamental Rights article 8
[10] Augustin Fuerea, *Manualul Uniunii Europene* (Universul Juridic 2011) at page 147
[11] 'Law in Germany - DLA Piper Global Data Protection Laws of the World' (*Dlapiperdataprotection.com*, 2020) <https://www.dlapiperdataprotection.com/index.html?t=law&c=DE> accessed 5 August 2020.
[12] 'EUR-Lex - L14547 - EN - EUR-Lex' (*Eur-lex.europa.eu*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14547#:~:text=The%20principle%20of%20direct%20effect,relates%20to%20certain%20European%20acts.&text=In%20this%20judgement%2C%20the%20Court,but%20also%20rights%20for%20individuals.> accessed 5 August 2020.
[13] 'Precedence of European law' (*Eur-lex.europa.eu*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548> accessed 5 August 2020.

where national law contradicts European Union law, the Union law is to be applied and national law has to be changed to be in line with the Union law.

The GDPR mainly deals with protecting the interest of the natural person.[14] This is done for three main objectives which include; protection of the privacy of the people and to maintain the social values, cultivating better responsibility of data controllers in relation to how they handle personal data, and making the efficiency and integrity of decision making better.[15] Personal data covers a wide range of data, including delicate data.[16] Special categories of personal data include biometric data which is used to identify a natural person distinctively and data concerning health among others.[17] This subgroup of personal data has been protected more closely than the general category of personal data. This is because it is seen to be in a category that is intimate, which, if disclosed can cause the data subject irreversible and significant harm.[18] The Court of Justice of the European Union ruled that even a mention of the fact that one has lost his leg because of an injury and who is now half disabled, constitutes part of the sensitive data-specifically personal health information, as was stipulated for in Directive 95/46.[19]

The GDPR provides for several provisions permitting the processing of personal information for technical research purposes connected to the COVID-19 pandemic while respecting the fundamental rights to privacy and the protection of personal data.[20] The GDPR also provides for a specific derogation from the prohibition of the processing of certain special categories of personal data, such as health data, which are necessary for the purposes of scientific research.[21]

---

[14] (*Ec.europa.eu*, 2020) <https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf> accessed 6 August 2020.
[15] C.J Bennett, *Regulating privacy. Data protection and Public Policy in Europe and the U.S*, (Cornell University Press, 1992) 44.
[16] 'What Is Personal Data Under GDPR? | The UK Domain' (*The UK Domain*, 2020) <https://www.theukdomain.uk/what-is-personal-data/> accessed 6 August 2020.
[17] GDPR article 9
[18] Mariusz Krzysztofek, '*GDPR: General Data Protection Regulation (EU) 2016/679. Post-Reform Personal Data Protection in The European Union'* (Wolters Kluwer 2019) 114
[19] *Bodil Lindqvist v Åklagarkammaren i Jönköping* (CJEU, 6 November 2003) C-101/01, ECLI:EU:C:2002:513
[20] Article 5 (1) (b) and (e), Article 14 (5) (b) and Article 17 (3) (d) GDPR
[21] Article 9 (2) (j) and Article 89 (2) GDPR.

Fundamental rights of the EU must be taken into account when processing health data for scientific research purposes connected to the COVID-19 pandemic.[22] Regulations enhancing the protection of personal information and the freedom of science as provided for in Article 13 of the EU Charter of Fundamental Rights do not take priority over others; rather, they must be balanced and evaluated taking into account the presence of the two laws.[23]

Article 4(15) of GDPR states that, 'personal information concerning health' refers to *'...personal data is associated with the general health of a natural person, it also includes delivery of health care service, which gives information about one's health status …*' Data concerning health required a greater degree of protection, because the usage of such delicate personal data may possibly cause significant adverse effects on the data subject0.[24]

Health data can be found through various sources, such as:[25]

1. Data collected through patient record by a health care provider (this may include medical history and examinations or treatment findings).

2. Data that is incorporated as health information because of annotation with other information that discloses the state of health or menaces (for example when one may be determined that they have a higher risk of a heart attack because of the analysis of blood pressure data monitored over a period of time).

3. Data from data subject when they answer questions on their health from mediums such as "self-check" survey (for example declaring symptoms).

---

[22] 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (European Data Protection Board 21st April 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf accessed on 11th August 2020.

[23] *Ibid*

[24] Recital 53, GDPR.

[25] 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (European Data Protection Board 21st April 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf> accessed on 11th August 2020.

4. information that ends being including as health data due to how it has been used in a particular context (for example information about a latest tour to or being in a particular place that has been affected by the Covid-19, which may be used by a health expert to make a conclusion on medication).

Recital 59 GDPR attempts to define what 'processing for the purposes of scientific research' entails *'... the term processing of personal data for scientific research purposes should be read comprehensively so as to comprise of examples like technical development and illustration, essential research, practical research and private sources of carrying out research. Further the meaning given should also be considerate of the Union's objective as per Article 179 (1) TFEU of attaining a European Research Mechanism. Studies undertaken for public interest specifically in the health aspect should also be included in scientific research purpose…'.*

Personal data processing with regard to health must be compliant with the principles of processing as provided for in Article 5 GDPR and in line with the provisions and particular derogations as is provided for in Article 6 and Article 9 GDPR to lawfully process the special category of personal data.[26]

The data subject's consent must be collected in harmony with Article 6 (1) (a) and Article 9 (2) (a) GDPR. Conditions set for unequivocal consent stated in Articles 4(11), 6(1) (a), 7 and 9 (2) (a) of the GDPR must be met. This includes permission should be obtained freely, explicit, informed, and unequivocal and it is essential that it is made through a declaration or "clear affirmative action".

The regulator and processor shall respect the protection of data principles concerning the dispensation of personal data whilst paying attention to Article 5 GDPR, keeping in mind that a lot of personal information may be used in the process of technical research. Article 5 holds that:

In the processing of personal data:

[26] Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C: 2014:317.

1. The process shall be in accordance with the law, in an impartial manner and it should be done in an open way with regard to the data subject (‘lawfulness, fairness and transparency’);

2. Gathered for a clearly stated, unambiguous and legitimate purpose and should not go against the stated reasons: moreover if the purpose of the processing is for historical storage in the public interest, scientific or ancient research or for the purpose of statistics, in harmony with Article 89 (1), it should not be taken to be irreconcilable with the original commitments (‘purpose limitation’);

3. Sufficient, pertinent and should be kept to the limits of the purposes they are to be processed (‘data minimization’);

4. Precise and where needed the information be kept current; action should be taken to ensure that any data that is not accurate, keeping in mind the propose for which it is being processed, be removed or corrected without delay (‘accuracy’);

5. Stored in a way that allows for the identification of the data subject not more that is necessary for reasons stated for the processing of the personal data; personal data may be kept for an elongated period as long as it is kept for archiving purposes that is done so for public interest attainment, in line with Article 89(1) on scientific, antique research and or arithmetical purposes should be done so in line with appropriate technical and organizational measures as directed by this Regulation in order to protect the fundamental rights of the data subject (‘storage limitation’);

6. Managed in a way that guarantees the security of the personal data, comprising protection from unapproved or illegal processing and against unintentional loss, obliteration or destruction, relying on appropriate procedural or structural measures (‘integrity and confidentiality’).,

Article 6 GDPR Processing shall be within the law and in reliance with at least one of the following principles applies:

1. Data subject consents to the usage of their sensitive information for a specified purpose;

2. Processing is part of the requirements to fulfill a contract in circumstances where the owner of the data is party to the contract or so as to undertake or act as per the request of the data subject before entering into a contract;

3. Usage is required for the obedience of a responsibility in the law in which the manager is a subject;

4. Processing is needed so as to safeguard critical interest of data subject or any other natural person;

5. Processing is essential for the controller to perform an undertaking in the importance of the public or in the performance of a certified authority;

6. Processing is essential for a reasonable interest pursed by regulator or by a third party excluding a situation where the data owner's interest is superseding the interest of the controller and therefore requires protection of their private data, particularly where the owner of the data is a child.

Under the GDPR article 9, processing of data from this particular group of data is prohibited unless:

a) The data subject gives unequivocal permission to the usage of the data for precise purposes apart from when the law of the particular state does not allow the lifting of the prohibition;

b) It is required for the data to be processed so as to carry out duties and to exercise particular rights of the data owner or controller in the following fields of occupation, social security and social protection, as long as it is within the authorization of the member state's law as a mandate to secure the fundamental rights and interest of the data owner;

c) It is essential in safeguarding the interests of the data owner or any other person in the case where the subject of the data being collected is physically and legally unable to give permission;

d) The usage is done in the course of genuine actions that have the required precautions by a foundation, association or any other not-for-profit body with a specific aim in religion, philosophical, political or trade union and on the premise that the usage only communicates to the affiliates or former affiliates of the particular organization or to those who have consistent

communication with it in line with its purpose and that the processed personal data is not revealed externally of the body unless the data subject has consented to release of the information;

e) The sensitive data that is processed is part of data that is already made openly by the data subject;

f) If the usage is required by the courts in its judicial capacity;

g) It is essential because of its role in public interest however this should be done proportional to the aim being pursued by the member state, whilst providing explicit steps to protect the essential rights and interests of the data owner;

h) If it is required for precautionary or work-related medicine, in order to gauge the functioning capacity of the worker, used in health verdict, in order to facilitate wellbeing or communal care or cure or running of medical or communal care systems and services as per Union or Member State law or in line with a contract between a health professional and the data owner as per the circumstances and precautions provided for in paragraph 3;

i) Usage of personal data is essential for public interest specifically in public health, for example protection from severe trans-border threats to health or safeguarding high quality standards and the safety of health care and medical products or equipment, as provided for in the Union or State law which states appropriate and precise steps to protect the rights and freedoms of the data subject, precisely professional secrecy;

j) Processing is required for historical storage in view of public interest, historical research, statistical or scientific purpose as per Article 89(1) founded on Union or Member State law that is proportional to the objective being pursued, respecting the principle of the right to data protection and offer appropriate and precise steps to protect the data subject's essential human rights and freedoms.

Processing of data under this group without the permission of the data owner because of public interest specifically in the aspect of public health is in recital 54 of Regulation (EU) 2016/679. The notion of public health should be in line with the definition in Regulation (EC) No. 1338/2008 Article 3 of the European Parliament and Council which holds that public health refers to all components of health including health status, the things that determine health status, needs, resources allocated to health care, access to health care and the expenditure and financing as well as causes of mortality.

Any measures taken by a State which is a member of the European Union with regard to Data processing of data so as to mitigate the spread of Covid-19 needs to be proportional, effective and necessary.[27] Due to the fact that the region is experiencing a pandemic, which involves fast spreading and cross-border spread of the Covid-19 virus, processing of personal data can be categorized under the exception in article 9 (2) (i) GDPR as it poses serious threats to human health and provision of national and international healthcare.

Directive 2002/58/EC complements the GDPR. It also known as the E- Privacy directive, lays the rules on how electronic communications services providers should manage their subscriber's data while guaranteeing their subscribers rights. This includes telecom companies and Internet service providers. Member States ought to reassure confidentiality of information over public networks.[28] On the other hand, public electronic communications services providers have to take proper precautions to protect and ensure the security of their services.[29]

Article 9 of the Directive concerns area of geographical data, which relates to user states that geographical data apart from traffic data 'may only be used if the data has been made unidentifiable, or unless the users or subscribers give consent to the degree and duration essential for the provision of benefits when a service is purchased. The one who offers the service has a duty to let the user of the service of the type of location data that will be processed, the purpose and the time taken to process the data and if it will be shared to a third party.

Article 15 of the E- Privacy Directive holds that Member States may implement regulations to limit the scope of obligations and rights as stipulated for in Article 9. This is allowed "when such limitation constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system".

---

[27] Hannah van Kolfschooten and Anniek de Ruijter, *'COVID-19 And Privacy in The European Union: A Legal Perspective On Contact Tracing'* (2020) 41 Contemporary Security Policy.

[28] 'Tracking Mobile Devices to Fight Coronavirus' (*Europarl.europa.eu*, 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf> accessed 19 August 2020.

[29] *Ibid*

However, the Directives' objectives have been hard to meet in member states because of the fragmented implementation across member states.[30] The rules have been incompetently enforced and outdated, as legislators could not match with the pace of developments in technology.[31] Users have been left more vulnerable due to the gap in law consequences of the extensive use of smartphone applications, online profiling, social media, and generally, the explosion of the Internet.[32]

2- Germany's position:

In Germany, data protection's legislation is the European Union's General Data Protection Regulations under Regulation (EU) 2016/679. The GDPR has specific clauses that allow national legislators of EU member states to pass Acts that cover these clauses that are not covered by Regulation 2016/679. In Germany, the data protection Act is known as *Bundesdatenschutzgesetz* or the Federal Data Protection Act(BDSG). It came into force on 25th May 2018, alongside the GDPR.

Prior to this, Germany was the first member state of the European Union to implement the GDPR in the *Datenschutz-Grundverordnung*, also known as the DSGVO.[33] As compared to the DSGVO, the BDSG is a much more detailed law on privacy protection, with 85 paragraphs, as compared to the DSGVO which had 48 and a short annex. The reason the BDSG was preferred to the DSVGO is because it did not only adopt the GDPR, it also adopts the EU Direction 2016/680, which in German is known as *Richtlinie für Justiz und Inneres, JI-Richtlinie.*[34]

Germany has other legislations which it relies on with regard to data protection in various sectors. The Federal Data Protection Act generally provides for data protection in employment

---

[30] 'EPIC - EU Privacy and Electronic Communications (E-Privacy Directive)' (*Epic.org*, 2020) <https://epic.org/international/eu_privacy_and_electronic_comm.html> accessed 19 August 2020.

[31] *Ibid*

[32] *Ibid*

[33] Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L199/1

[34] Protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89

and for CCTV recordings while the German Code of Criminal Procedure regulates interception of communication, monitoring and surveillance of individuals. Germany legislation has also addressed protection of personal data in telecommunication services as it is not widely covered under the GDPR through the Germany Telemedia Act (TMA). This has been possible because of the open clauses in the GDPR which allow national legislators of member states to put in place laws and regulations that impact data protections in sectors that need such laws [35].

Each Federal state in Germany has the mandate of implementing the principles of data protection through authorities referred to as Data Protection Authority(DPA). The DPA audits compliance in the application of data protection laws and where non-compliance is suspected, the authority can investigate and issue warnings or apply measures such as administrative constraint such as an order to ensure compliance with the regulations is undertaken. This usually occurs with institutions and the authority has powers to issue administrative fines as penalties for non-compliance[36].

In order to coordinate implementation of the Data Protections Laws, the Germany Data Protection Authority have a way to come together and address controverted issued together with other members of the European Union in the European Data Protection Board to ensure data protection is properly implemented and arising issues are addressed. The European Union is able to do this through the mandatory private impact assessment (PIAs) which it has introduced. The Regulation requires data collectors in this case companies to carry out PIAs where there is a possibility of high breach of privacy in order to minimize risks to data subjects[37].

---

[35] G. Stepanova, '*The Privacy',* (October 2019). *Data Protection and Cybersecurity Law Review.* Retrieved from The Law Reviews:https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210039/germany, accessed on 11th August 2020.

[36] SKW Schwarz Rechtsanwälte, 'Germany: Data Protection Laws and Regulations 2020', https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany, accessed on 11th August 2020.

[37] D. Wright, P. De Hert, Enforcing Privacy: Regulatory, Legal and Technological Approaches, (Springer, 2016), P. 18.

Germany has an extensive and rich tradition on data protection law.[38] The constitution of Germany is silent on the safeguarding of data protection.[39] The premier custom of data protection in the world, originated from Germany in the Hessian Data Protection Act 1977.[40] The German Federal Constitutional Court of Karlsruhe in 1983 established right to informational self-determination which was new and provided of court precedent.[41] Karlsruhe held that interfering with the informational self-determination right should be founded on a law regulating the interference in a particular and precise area and manner and should be regulated.[42] As a result, States in Germany(Länder) have enacted their own laws with regard to data protection and there are sectored provisions in German law such as the Broadcast Media Act (Telemediengesetz, TMG), Telecommunications Act (Telekommunikationsgesetz, TKG) and the Federal Data Protection Act.[43]

The Federal Data Protection Act (BDSG) is an all-inclusive law that is aimed at the protection of one's right to privacy in line with the handling of their personal data. It applies to the gathering, dispensation and use of personal data by;

1. Federation's public bodies (Bund), which includes public authorities, judicature and public law institution, federal corporations and foundations under public law.
2. Public bodies of the Land (Länder), which refers to authorities' judicature and other public institutions of a land of a municipality, an association of municipalities under public law

---

[38] 'Germany: Land of Data Protection and Security – But Why?' (*home*, 2017) <https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why> accessed 11 August 2020.

[39] Alvar Freude and Trixie Freud, 'Echos of History: Understanding German Data Protection'. http://www.bfna.org/publication/newpolitik/echos-ofhistory-understanding-german-data-protection accessed on 11th August 2020

[40] 'Germany: Privacy | Lexology' (*Lexology.com*, 2020) <https://www.lexology.com/library/detail.aspx?g=1809070b-c64a-480f-bed2-fa7991546946> accessed 11 August 2020.

[41] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review.

[42] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.

[43] *Ibid*

which are under land supervision, to the extent to which data protection is not governed by Land law and in so far as they;

i) Implement federal law or,

ii) Perform duties as bodies of the judicature and are not working with governmental matters

3. Private bodies as long as they develop or use data through data processing systems or gather data for such systems, develop data in or from manual filing systems or gather data for such systems, except when the collection, processing and or use of such data is only for individual or personal undertakings.[44]

There are four parts of BDSG. Part 1 consists of collective provisions applicable to the GDPR and to Directive (EU) 2016/680 and to the processing of personal data that is not provided for by the two legislative texts. It has 6 chapters which contain: the range and definitions; the legal foundation for personal data processing; data protection officers of non-private organizations; Federal Commissioner for Data Protection and Freedom of Information; be part of the European Data Protection Board so as to ensure representation, a one-stop shop, collaboration between federal supervisory authorities and those of member countries in matters of the European Union; legal remedies.

Part 2 deals with the implementation of the processing provisions according to Article 2 of the GDPR. It is organized into 6 chapters: provisions of the law on the processing of personal data; the rights of the data subject; the duties of inspectors and processors; management authorities for data processing by private bodies; punishments; legal remedies[45].

The third part deals with the implementation of Directive (EU) 2016/680. The seven chapters deal with: the range, definitions and general principles of the processing of personal data; provisions of the law on the processing of personal data; the rights of the data subject; the duties of inspectors and processors; sharing of data with third countries and international organizations; collaboration between supervisory authorities; responsibilities and penalties.

Part 4 concerns the processing of personal data with a view to activities that are not part of the GDPR and of Directive (EU) 2016/680. This is required under section 85.

---

[44] 'Federal Data Protection Act (BDSG)' (*Gesetze-im-internet.de*, 2020) <https://www.gesetze-im-internet.de/englisch_bdsg/> accessed 11 August 2020.
[45] Ibid

Article 1 (5) BDSG states that what is provided for in the law does not apply when the GDPR and Regulation (EU) 2016/680 apply directly. The burden of proving this falls on those who apply the law, so they will have to work with the idea that the new law does not go against the GDPR.[46] Section 1 (8) of the BDSG provides that the GDPR and parts 1 and 2 of the BDSG relate to the processing of personal data by non-private bodies in connection with actions that may or may not fall within the scope GDPR and Directive (EU) 2017/680.

Section 26 of the BDSG deals with the processing of data for employment-related purposes. German lawmakers have put in place a structure taking into consideration the opening clause of Article 88 (1) of the GDPR. Section 4 BDSG deals with video surveillance of spaces accessible to the public. A bone of contention is whether this section actually complies with the requirements of the GDPR. Indeed, section 4 BDSG departs from the technological impartiality of the GDPR.[47]

The provisions relating to the Federal Commissioner for Data Protection and Freedom of Information can be found in Sections 8 to 16 of the BDSG. The Commissioner in Bonn is the supervisor of the public bodies of the Federation [48] except for federal courts acting within their judicial mandate [49] and sits on behalf of Germany on the European Data Protection Board. It further specifies that private bodies must be supervised by a state control authority (Länder).[50]

Sections 18 and 19 of the BDSG discusses about the between the Federation (Bund) and the state (Länder). According to Article 77(1) GDPR complaints can be reported *'... with a managing authority, specifically the Member State of their place of residence, work place or where the infringement occurred…'* Member of the EU like Germany, which have numerous administrative/supeervisory authorities, are allowed to regulate the authority that should take the responsibility.[51] A supervisory authority shall forward a complaint, which is not responsible according to Section 19(1) BDSG to the overseeing power of a Land where the controller or

[46] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.
[47] *Ibid*
[48] S. 9 (1) BDSG
[49] S. 9 (2) BDSG, Article 77 GDPR
[50] S. 40 (1) BDSG
[51] S. 19 (1) BDSG

processor has established an institution.[52] If such an institution does not exist, the addressee will be the governor of the Land where the applicant is a resident.[53]

A provision in question is the BDSG S.29. He states that the regulatory authorities in the investigation powers in accordance with Article 58, paragraph 1, e) and f) RGPD, will not apply to people in particular, because it would not go to against the secret duty of the people. They include doctors, lawyers, psychologists and professionals who share confidential customer relationships.[54]

Section 32 to 37 BDSG concerns the limitations on the rights of the data owner, such as the restriction of information to be provided to the data owner,[55] the right of access[56] and the right of erasure,[57] the right to object[58] and computerized personal decision making.[59] However, where secrecy obligations exist, the rights of the data owner are limited.[60]

Section 22(1) (1) BDSG deals with dispensation of exceptional categories of data by public and private bodies. The acceptable processing relates to social security, medicine and public health. However, '…*suitable and precise measures will be taken to protect the interests of the data subject…* '[61]

Section 42 BDSG contains penal provisions. Transmitting *"personal data of a big group of people which may not be accessible publicly"* to a third party or giving accessibility for commercial purposes has a penalty of up to three years imprisonment without a fine.[62] Processing without the requisite permission or acquiring personal data in a fraudulent manner for the exchange of compensation or with the purpose of elevating oneself or someone else or causing detriment to someone has a penalty of being imprisoned for up to two years or a fine.[63] However,

[52] S. 19 (2) BDSG
[53] *Ibid*
[54] S. 203(1) (2a) (3) German Criminal Code
[55] S. 32-33 BDSG
[56] S. 34 BDSG
[57] S. 35 BDSG
[58] S.36 BDSG
[59] S.37 BDSG
[60] S. 29 BDSG
[61] S. 22(2) BDSG
[62] S. 42(1) BDSG
[63] S. 42(2) BDSG

these offences can only be put on trial if the data subject, the regulator or a managerial authority, makes a complaint.[64]

Section 42 (4) and 43 (4) BDSG provides that a notice as per Article 33 GDPR or a message as provided for in Article 34 (1) GDPR can only be used in criminal proceedings and as provided for in the Administrative Offences Act against the one who is mandated to offer a notice or message if that person has offered permission.

Under Article 80 GDPR, subjects of the data have the right to direct a not-for-profit body, organization or association to place a protest for them and to perform the rights as per Articles 77 to 79 GDPR. Member States are allowed to make decisions if the bodies have the mandate to act independently from a data subject's power.[65] This is not explicitly mentioned in the BDSG, but in Section 2(2)(1)(11) UKlaG (Unterlassungsklagengesetz, Injunction Act). This is narrowed to data processing in publicizing, marketing and opinion research, credit bureaus, making of personalities and profiles to be used, address trading, additional types of data that are related to trading and commercial purposes. Section 2(2)(1) (11) UKlaG therefore is not within the range of Article 80(2) GDPR.

The controller and processor of data shall appoint a data protection officer in the situation where they constantly ten people who deal with the computerized processing of personal data, as a rule.[66] In particular circumstances, a data protection officer is to be elected despite the number of people employed in the process.[67]

For purposes of this study, S.22 BDSG on the dispensation of extraordinary categories of data by public and private bodies in light of the current pandemic, which is a public health matter, will be studied in close detail.

Unfortunately, Germany has departed from the provisions of the GDPR.[68] This only goes contrary to the goals the GDPR intends to achieve, which is to complement data protection law

---

[64] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.
[65] Article 80(2) GDPR
[66] S. 38(1)(1) BDSG
[67] S. 38(1)(2) BDSG
[68] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.

within the Europe's boundaries and beyond.[69] It has used the opening clauses of the GDPR in a biased way.[70] As a result of this, the EU undertook infringement proceedings against Germany[71] for not having implemented Directive 2016/680 completely as only 10 out of the 16 states (Länder) had implemented the Data Protection Law Enforcement Directive.[72] From the infringement proceedings, the Commission was not impressed by the Germans' approach and it has clarified that the GDPR simply allows for 'specifications' thereby regulating the verge for member states.[73]

[69] *Ibid*

[70] Alexander Rossnagel, 'Legislation Within the Framework of the General Data Protection Regulation: Tasks and Scope of the German Legislator?' (2017) 41 Data Protection and Data Security-DuD.

[71] https://www.heise.de/newsticker/meldung/Datenschutzreform-EU-Kommission-droht-Deutschland-mit-Vertragsverletzungsverfahren-3689759.html accessed on 12th August 2020

[72] https://eucrim.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/ accessed on 12th August 2020

[73] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.

CHAPTER 2: TRACK CONTACTS AND CONTAIN THE COVID-19 PANDEMIC

The rapid spread of the Corona virus has forced governments to take up steps to protect its citizenry. This steps have included cession of movement and complete lockdown in countries such as Italy and the UK, coupled with population surveillance through location data and contact tracing have been used to try and contain the virus.

The first stages of the pandemic required rapid detection of those that have contracted the virus whilst also tracing those they might have interacted with followed by isolation measures mandatory for those infected persons combined with surveillance and testing measures as necessary steps to control pandemic.[74] The next stage which is where there is a peak in infection cases, brings into focus efforts for control, which includes limitations on social contact and movement.[75] In this state of affairs data collection of the movement of people helps to make the most efficient policies and moreover provides valuable understanding to assist build an accurate epidemiological model used in the spread of diseases.[76] Below, contact tracing and location tracing are unpacked elaborating on how different countries have approached it and digging deeper into why it is being used as well as its legitimacy in containing the pandemic.

1- Contact tracing in the EU:

Since time immemorial management of infectious diseases included using contact tracing through public authorities which try and ascertain people who may have been in contact with an infected person.[77] This is done through active contact tracing, which involves finding each person

[74] Nuria Oliver, '*Mobile phone data for informing health actions across the COVID-19 pandemic life cycle'* (Science Advances, 5th June 2020) < https://advances.sciencemag.org/content/6/23/eabc0764> accessed 27th July 2020

[75] Ibid

[76] Nuria Oliver, '*Mobile phone data for informing health actions across the COVID-19 pandemic life cycle'* (Science Advances, 5th June 2020) < https://advances.sciencemag.org/content/6/23/eabc0764> accessed 27th July 2020

[77] Matthew L Levine, *'Contact Tracing for HIV Infection: A Plea for Privacy'* (1988) 20 Columbia Human Rights Law Review 157

who is infected with the corona virus, and then tracing the people they interacted with a few days before the tests came out to be positive.[78]

Therefore, quite a number of countries have employed the use of contact tracing in a bid to control the novel virus and protecting those that are at risk in society. However, the new virus requires a faster and more reliable tracing method therefore, the old methods needed to enhanced. This is where digitization came in-the use of applications to assist in the contact tracing method.

A different approach that countries around the EU and Germany have used in order to protect their population is location tracing. It is where government is able to access the location information of its population through telecommunication services.[79] This is by the use of geo-location tracking done through the following four steps:[80]

i) Tracking by use of mobile signals via cell towers, which provide data about all the mobile device around a particular area and at a particular time.

ii) The use of mobile cell phone towers, which is able to catch devices around it.

iii) Use of Wi-Fi and Bluetooth in a particular device, only operational in short distances.

iv) The use of apps and web browsing to determine the location of a particular device.

In the beginning stages of the Covid-19 spread mobility data can be used in a way to track the effects of social and mobility measures undertaken by the government and to also check the effectiveness of such measures.[81] The purpose of using anonymized phone location data is to

[78]Nicole Wetsman, 'What Is Contact Tracing?' (*The Verge*, 2020) <https://www.theverge.com/2020/4/10/21216550/contact-tracing-coronavirus-what-is-tracking-spread-how-it-works> accessed 13 August 2020.

[79] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[80] Alexander Klimburg and others, 'Digital Epidemiological Measures to Combat the Coronavirus Pandemic' (Hague Center for Strategic Studies 2020) <https://www.aies.at/download/2020/AIES-Studies-2020-12.pdf> accessed 15 August 2020.

[81] Nuria Oliver, '*Mobile phone data for informing health actions across the COVID-19 pandemic life cycle'* (Science Advances, 5th June 2020) < https://advances.sciencemag.org/content/6/23/eabc0764> accessed 27th July 2020

monitor movements of the population and to observe how effective the lockdown measures are.[1] To achieve anonymization, companies use the k-anonymity method, where location data is clustered into groups such as small crowds of 30 users and presented in a statistical format.[2] This protects the identity of individual behavioral patterns and avoids the re-identification of individuals.[3] Anonymization of location data by telecom companies makes its processing and sharing lawful under EU law, despite without the consent of users.[4]

EU member states are to share information on contact tracing with each other through the Early Warning and Response System (EWRS) for serious cross-border threats.[5] This involves sharing of personal and health data so as to facilitate contact tracing through a web based platform linking the European Commission, European Center for Disease Control and public health authorities in the European Union that are mandated to carry out measures to control very serious cross-border threats to health, like communicable diseases.[6] This collaboration on contact tracing leading to sharing of data creates a risk for the infringement of an individual's right to privacy.[7] With different countries in the EU using a different application the absence of uniformity requires that the apps be looked at individually.

---

[1] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[2] Zakariae El Ouazzani and Hanan El Bakkali, 'A New Technique Ensuring Privacy in Big Data: K -Anonymity Without Prior Value of the Threshold K' (2020) <https://reader.elsevier.com/reader/sd/pii/S187705091830108X?token=49EBDD114E76B38B7739429A79A41387FE793373AE396803F11E8362A135720C00C0DB292045BD85F3A07E9340BDB62A> accessed 15 August 2020.

[3] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[4] Recital 26 GDPR

[5] Decision no.1082/2013/ EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC [2013] OJ L293/1

[6] 'Early Warning and Response System (EWRS)' (*European Centre for Disease Prevention and Control*, 2020) <https://www.ecdc.europa.eu/en/early-warning-and-response-system-ewrs> accessed 13 August 2020.

[7] Karl Schmedders, Josè Parra-Moyano and Michel Avital, 'Coronavirus: Digital Contact Tracing Doesn'T Have to Sacrifice Privacy' (*IMD business school*, 2020)

'Immuni' is Italy's contact tracing app and it has a decentralized system allowing the users to store data on their individual devices and is also voluntary. The only time data is transferred to a server is in the occasion where one tests positive for the COVID-19 virus. Blending Spoons S.p.a., which is the company that developed the app, has given the Italian government rights of use of the app and free updates for the future. [1]

Initially an app was developed in the UK to be used for contact tracing however, this was seen to have technical and ethical problems therefore a second app is being developed in a bid to solve the previous difficulties. The first app had a centralized system where one would upload to a government server once they develop corona like symptoms.[2] Some of the technical issues stemmed from the fact that the NHSX was trying to circumvent the privacy limitations on smartphones such as Apple and Google.[3] This was manifested in the app by it only detecting 25 contacts on Apple phones as the phone would go idle and stop registering Bluetooth matches and it not working on Android phones older than four years. This was manifested in the app by it only detecting 25 contacts on Apple phones as the phone would go idle and stop registering Bluetooth matches and it not working on Android phones older than four years.[4]

2- Contact tracing in Germany:

It developed one named Corona Warn app, which uses Bluetooth technology to contact trace. Once the app has been downloaded it exchanges contact IDs that are anonymous.[5] It broadcasts a 'temporarily valid, authentic and anonymous identification' of an infected person

---

<https://www.imd.org/research-knowledge/articles/coronavirus-digital-contact-tracing-doesnt-have-to-sacrifice-privacy/> accessed 13 August 2020.

[1] Cornelia Wels, 'The Struggle to Create COVID-19 Contact-Tracing Apps' (*Healthcare-in-europe.com*, 2020) <https://healthcare-in-europe.com/en/news/the-struggle-to-create-covid-19-contact-tracing-apps.html> accessed 15 August 2020.

[2] *Ibid*

[3] Hasan Chowdhury, Mathew Field, Margie Murphy, 'When will the UK 'track and trace' app be ready- and how will it work?' (15th July 2020) <https://www.telegraph.co.uk/technology/2020/07/15/track-trace-app-uk-google-apple-when-download/> accessed 27th July 2020

[4] *Ibid*

[5] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

held in an 'encrypted proximity history stored on the phone.'[1] If a person is infected in the network, message alerts are forwarded to others whose contacts are saved in the infected persons' phone history via Bluetooth ID.[2] Collected ID's are only stored for not longer than 21 days.[3] However, a problem that arises is what happens if people are sick for longer than 21 days? This is a new disease and how long it stays in the body is unknown. Some patients have claimed that the coronavirus disease occurred again after healing, some even up to 3 times after contracting it the first time because the virus did not completely disappear from the body.

The app may be categorized as a medical device, which means it has to detect while safeguarding safety rules. According to the provisions of Regulation (EU) 2017/745 on medical devices (MDR), the intention by the manufacturer on the use of the app is what determines whether or not it is considered to be a medical device, if it is used for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease then it qualifies to be a medical device. Thus, the Corona Warn app falls under this definition. The MDR was to be implemented in May 2020, but the Commission opted to adjourn its implementation for one year, to give opportunities to Member States, health institutions and economists to put their attention on combating the pandemic.[4]

Legal academics argue that the use of the Bluetooth technology is the least intrusive method in contact tracing through the use of mobile technology.[5] Similarly, according to the European Data Protection Supervisor, who supports the use of such apps that utilize Bluetooth technology to assist in contact tracing, states that, 'they appear to be a relevant path in achieving

---

[1] 'Overview: How We Preserve Privacy and Maintain Security' (*Pepp-pt.org*, 2020) <https://www.pepp-pt.org/content> accessed 14 August 2020.

[2] Lucette Mascini and others, 'EU Expert On European Response to Virus: 'Telecom Data for Tracking Corona Can Be Made Anonymous' - Innovation Origins' (*Innovation Origins*, 2020) <https://innovationorigins.com/eu-expert-on-european-response-to-virus-telecom-data-for-tracking-corona-can-be-made-anonymous/> accessed 14 August 2020.

[3] 'Overview: How We Preserve Privacy and Maintain Security' (*Pepp-pt.org*, 2020) <https://www.pepp-pt.org/content> accessed 14 August 2020.

[4] 'Tracking Mobile Devices to Fight Coronavirus' (*Europarl.europa.eu*, 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf> accessed 19 August 2020.

[5] Hannah Murphy, 'US and Europe Race to Develop 'Contact Tracing' Apps' (*Ft.com*, 2020) <https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95> accessed 14 August 2020.

privacy and data protection effectively.'[1] The app usage is voluntary[2] and therefore, deciding not to use the app should not affect the right of usage by third parties' services such as malls, supermarkets etc.[3] However, the question arises on the legitimacy of the app. What if a small percentage of people download the app, it will not be a legitimate form of controlling the virus, as it is voluntary. People who opt to use the app are the ones being depended on to provide information on the virus so that the government can put better measures in place. If only a small percentage use the app, how effective is it? For the application to be beneficial, and to have a progressive effect on public health, a large section of the population should have the technology enabled on their smartphones. The collection of additional data is dependent on increased number of people using the app however when the use of the app is voluntary mass adoption might not take place.[4]

Secondly, what if a wrong test is put on the app? It will mislead people into thinking that the said person is positive when they actually do not have the virus. This is a new virus and tests cannot be completely relied on. There were even some cases in America where people were being misdiagnosed. Thirdly, it can lead to identification of people because the app will notify people when an infected person is around. This can lead to bullying and stigmatization of the infected person.

In order to prevent wrong positive diagnosis on the application platform, when ones test results turn to be positive the health facility they tested at will provide them with a barcode that will allow them to upload their status on to the app which is then sent to a centralized system with the same anonymized ID, which will cause a trigger of the alarm where comparison of stored

---

[1] Wojciech Wiewioroski, 'EU Digital Solidarity: A Call for A Pan-European Approach Against the Pandemic' (2020) <https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf> accessed 14 August 2020.

[2] Natasha Lomas, 'Digital Mapping of Coronavirus Contacts' (*Techcrunch.com*, 2020) <https://techcrunch.com/2020/04/15/digital-mapping-of-coronavirus-contacts-will-have-key-role-in-lifting-europes-lockdown-says-commission/> accessed 14 August 2020.

[3] 'An Open Letter to The Members of the Wassenaar Arrangement' (*Human Rights Watch*, 2020) <https://www.hrw.org/news/2014/12/01/open-letter-members-wassenaar-arrangement> accessed 14 August 2020.

[4] 'Digital Contact Tracing During COVID-19: The Pros and Cons We Must Consider' (*UC Institute for Prediction Technology*, 2020) <http://predictiontechnology.ucla.edu/digital-contact-tracing-during-covid-19-the-pros-and-cons-we-must-consider/> accessed 15 August 2020.

ID of third parties are stored.[1] In safeguarding the right to personal privacy, several things have to be considered including the guard from persons who would like to spy, from contacts and from the authorities and a major step is ensuring that a linkage attack is prevented in the course of usage of the app.[2] According to an app assessor, however, the app still presents several privacy-related violations as 'sick people who are conveyed in secret can be de-anonymized, private encounters can be uncovered, and people may be forced into revealing their private data'.[3]

Unfortunately, the contact-tracing app may contribute very little to the overall objective of ensuring that the infections are controlled or prevented because further steps of social distancing, testing and quarantine measures should go alongside it.[4] One challenge for monitoring and forecasting the spread of Covid-19 is the fact that infected people can transmit the virus before they reveal any symptoms and they account for 50% of the transmission. [5] This makes it difficult to trace the people that an infected person has mingled while having the virus.[6] Consequently, the use of a contact tracing app may not be useful in the fight against the virus especially in asymptomatic and presymptomatic patients.

This application system is mostly available to the younger and more digitized generation. Older generations cannot use it, as they do not even know how to use a smart phone, where applications are to be downloaded on. Thus, since this virus is mostly life threatening to old people, it is a counter-intuitive approach. Furthermore, even if they know how to use basic applications in the smart phone, if the app is difficult to use, they may not even input their data

---

[1] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[2] *Ibid*

[3] Costica Dumbrava, 'Tracking Mobile Devices to Fight Coronavirus' (*Europarl.europa.eu*, 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf> accessed 15 August 2020.

[4] *Ibid*

[5] Klaudia Klonowska, Pieter Bindt, 'The COVID-19 pandemic: two waves of technological responses in the European Union' (*Hague Center for Strategic Studies*, 2020) <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020

[6] *Ibid*

on the app not unless sensitization and education takes place. Younger generations often rely on YouTube and Google to understand difficult technological issues. Older generations most often do not do this.

With European borders opening up, and without a unified application system in Europe, other Schengen visitors may visit Germany and carry the virus with them into Germany. If Germans are relying on this method, other Schengen citizens who are not aware of the app will not be able to input their results into it and thus go on infected more people, making containing the virus more difficult.

However, on the other hand, using this type of data through the use of contact tracing apps could help open up countries in the EU sooner. Social media sites like Facebook have been in hot soup for going contrary to privacy rules and giving out too much information on peoples' personal life. Therefore, Europeans ought to weigh up the decision and realize how much less intrusive the app is.

CHAPTER 3: BALANCING MEASURES TO CONTAIN THE VIRUS AND UPHOLDING INDIVIDUAL PRIVACY:

This chapter will discuss the relationship between personal data protection in Germany and other fundamental rights and freedoms in the European Union. This chapter will also study the protection of the right to privacy in Germany while collecting and processing personal data. Furthermore, it will delve deeper on the relationship between the protection of personal data and other fundamental rights and freedoms enshrined by the ECHR. Finally, it will focus on the balance that should be struck between measures that keep track and contain the Covid-19 virus while protecting an individuals' privacy.

The right to protection of personal data arises where personal data requires processing, usage ad storage. It is therefore a process requiring extracting of personal data from an individual and processing it without infringing on the person's rights to protection of data as well as privacy. It should also consider the right to access information especially in institutions such as workplaces and hospitals. It is however in hand to note that data protection requires the permission of the data subject and that other rights should be put into consideration when the same is being exercised.

In his statement on 19th March 2020, the European Data Protection Supervisor (EDPS) upheld that *'emergency is a condition within the law that may allow the limitations of freedoms as long as the proportionality principle is taken into account and the duration of the limitation is only during the emergency period'* and that *'if such steps are taken a Member state has a duty to give protection for example granting right to judicial remedy to the people'*.[1]

Later, in another statement on 6th April 2020, the EDPS held that any EU or member state measures should respect fundamental human rights, including that measures to address the pandemic particularly concerning data protection should not be permanent, should have a precise

[1] Andrea Jelinek, 'Statement On the Processing of Personal Data in The Context of The COVID-19 Outbreak.' (*European Data Protection Board*, 2020) <https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf> accessed 20 August 2020.

purpose and further called for pan-European model of a mobile application that would be harmonized at the EU level.[2]

The chair of the European Data Protection Board has further held that '*public authorities ought to as the first step look to process location data anonymously'* and recalled that *'Member States have a duty offer protection for example ensuring that the users of electronic communications services have a right to a remedy through the court system.'*[3] The actions taken must be proportional and as not interfere with their personal privacy as much as possible and be subject to *'enhanced analysis and protective measures to guarantee the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation)'.*[4]

1- The position of the European Court of Justice in relation to recognizing the right to privacy:

The court can only offer limited help to this area of the Charter because there is ambiguity regarding its scope; nature and limits held in Article 8. The EU court avoided recognizing Article 8 as an autonomous right and instead let it fall under the ambit of the right to privacy. This was seen in the case of *Promusicae v. Telefo´nica de Espana*[5] where the court held that the preamble of the e-Privacy Directive was a direct reference of Article 8 of the Charter that *'expressly proclaims the right to the protection of personal data.'* But, despite this, the Court still held that personal data protection falls under the protection of '*personal life.'* Furthermore, the Court held that the rights at stake were a conflict between the protection of property and the right to respect for private life. Yet, this should have been under the right to protection of personal data.

---

[2] Wojciech Wiewiórowski, 'EU Digital Solidarity: A Call for A Pan-European Approach Against the Pandemic' (*European Data Protection Board*, 2020) <https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf> accessed 20 August 2020.

[3] Andrea Jelinek, 'Statement On the Processing of Personal Data in The Context of The COVID-19 Outbreak.' (*European Data Protection Board*, 2020), <https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf> accessed 20 August 2020.

[4] *Ibid.*

[5] Case C-275/06, *Promusicae v. Telefo´nica de Espana,* [2008] ECR 2008 l-00271

Similarly in the case of *Rijkeboer*[6] the court provided a comprehensive explanation of what it considered to fall under the concept of 'privacy' which according to them encompassed the right to data protection under Article 8 of the Charter. This therefore means that the Court was holding the right to privacy being synonymous with the right to personal data protection. According to the Advocate General Ruiz-Jarabo Colomer , he argues that *'the essential right to privacy, has found 'legislative expression' through the Data Protection Directive as it is seen as a general principle of 'Community law', ' its provisions brought out in Article 8 of the Charter '*[7] Since neither the parties nor the referring courts had mentioned the then Data Protection Directive provisions, it nonetheless found that the question being referred to had to be balanced between two things first the right of the individual to privacy through rectification, erasure and blocking of data, right for legal proceedings and right to object, second the weight of the responsibility to store data has on those who are to process the said data.[8]

Another bone of contention is raised in the case of *Eugen Schmidberger, Internationale Transporte und Planzu¨ge v. Republik O¨ sterreich*[9]*, which* concerns legitimate interference to the freedom of expression and assembly and vaguely covered that for such considerations, Article 8(2) of the Charter foresaw that *'data must be processed fairly in accordance with specified purposes and with the consent of the person concerned or because of a reason stated in the law'.*[10] This raises a question as to whether there is a conflict of interest between Article 8(1), which provides for the general rule to data protection i.e. a prohibition to the processing of personal data, and Article 8(2), the exemptions that could be allowed to such a rule.[11] This tension assumes that the processing of personal data is essentially opposed to the protection of personal data-the

---

[6] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR 2009 I-03889

[7] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR 2009 I-03889, Opinion of AG Colomer, para 8.

[8] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR 2009 I-03889, para. 64.

[9] Case C- 112/00, *Eugen Schmidberger, Internationale Transporte und Planzu¨ge v. Republik O¨ sterreich* [2003] ECR 2003 I-05659.

[10] *Ibid* at para. 49.

[11] Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in The European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology.

non-processing of data. The next question that arises is that while Article 8(2) that *'everyone has the right of access to data that has been collected about them, and the right to have it corrected',* Article 8(3) provides that *'compliance to the above mentioned is to be controlled by an independent authority'.*

These 2 clauses conflict each other because while one gives freedom and rights to the data owner the other strips the data owner off the rights and freedoms through an independent authority. Furthermore, this is antagonistic to the concept of personal data protection law being an enabler of personal data processing but instead comes across as an impediment because personal data protection law is what renders it legally possible to process personal data, by explaining the circumstances that the processing is legitimate. Indeed, '*data protection would not be necessary if information disclosure was prohibited'.*[12]

Thus, there have clearly been challenges in the EU court for construing the right to personal data protection. As the EU Charter rendered it increasingly unjustifiable that protection of personal data is a part of the right to privacy, the Court has noted that protection of personal data is an independent right from the right to privacy, however it is viewed as closely related though independent from each other. 'Privacy thinking' is also present in the EU Court of Justice in construing the right to personal data protection as a *sui generis* or unique right.[13] The Court is applying the *modus operandi* that is applied in private life to protection of personal data as rights. As historian Isaiah Berlin puts it, privacy can be viewed from the lenses of 'positive freedom' as it involves giving a privilege to the individual (Article 8.1 of the ECHR); but, since it is not an absolute right limitations to the right have been provided for in the law (Article 8(2) of the ECHR).[14] On the other hand, data protection can be termed as a 'negative freedom,' whereby giving protection to the individual by not giving them a privilege to determine, but by controlling

[12] Case C-396/98, *The Queen vs. Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, [2000] ECR 2000 I-06751, opinion of AG Siegert Alber, para. 41.
[13] Douwe Korff, 'EC Study On Implementation of Data Protection Directive 95/46/EC' (2002) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667> accessed 27 August 2020.
[14] Isaiah Berlin, *Four Essays On Liberty* (Oxford University Press 1969).

the behaviors of other people as they it might interfere with the freedom of the right holder through control by an independent authority.[15]

2- The Right to Privacy in Balance with other Fundamental Rights:

The Charter and the ECHR are connected by the fact that the definitions and range of the rights provided for in the Charter are similar to the rights in the ECHR as stated in Article 52(3). Article 52(3) holds that *'...In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those provided for by the said Convention. This provision shall not prevent Union law providing more extensive protection…'.*

Milanovic, a legal scholar, summaries the affirmative and destructive obligations of jurisdictions in relation to data protection to human rights treaties in order to protect the right to privacy internationally.[16] Positive obligations give the state a duty to ensure that the right is not obstructed with by a third party. A negative duty is where the state is required to respect and uphold human rights by not obstructing other human rights unless it is justifiably done so. He proposes that: *'...the state's duty to respect human rights is unlimited within its own territory; nevertheless its obligation to secure or ensure human rights goes as far as the areas that are under its control…'*[17]

Under International Human Rights Law, there are 3 types of obligations to safeguard these rights: respect, protect and fulfill.[18]

The obligation to respect suggests that the EU has a negative obligation to ensure that it does participate in any action that could interfere with the enjoyment of the right to data

---

[15] Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in The European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology.

[16] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv lnt'l L J 81, 134 citing Huvig v France App No. 11105/84 (ECHR, 24 April 1990) 35.

[17] Marko Milanovic, The Extraterritorial Application of Human Rights Treaties (OUP, Oxford 2011) at 263

[18] Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds), International Protection of Human Rights: ATextbook (A° bo Akademi University Institute for Human Rights, Turku 2009), 19, 27.

protection does not interfere with their privacy, which concerns personal data.[19] The Charter obliges that the EU 'respect' human rights and under IHRL, the duty to respect would be fundamental to that human rights conventions.[20]

The obligation to protect is an obligation to the European Union that requires them to ensure that a third party does not obstruct or violate another person's right to data protection. The case of Google Spain shows how CJEU and the member states of the European Union are ensuring this protection by forming an affiliate in Spain, Google, Inc. , Which is established in a third country (USA), is responsible for possible interference with data of EU citizens protection rights.[21]

The Obligation to fulfill means a commitment to positive results, a commitment to fulfill a person's right to data protection through the provision of legal and regulatory frameworks, with resources and enforcement mechanisms.[22]

The rights and freedoms must be scrutinized against who weighs the right to data protection against such as the freedom to access information, the right to have documents, the right to freedom of expression, and safeguarding people's interests.[23]

The right to data protection must be balanced with ensuring the free flow of information or the right to freedom of information and the right to freedom of opinion and expression.[24] In the Google Spain case, the court established that the former data protection directive which was repealed by the General Data Protection Regulation (GDPR), was applied to the specific case by ruling that the search engine is the same data controller that processes personal data, despite the personal data that It has been processed in a different place by a third party - Google USA.[25] The

---

[19] Mistale Taylor, 'The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect' (2015) 5 International Data Privacy Law.
[20] *Ibid*
[21] Case C-131/12, *Google Spain v AEPD and Mario Costeja Gonzalez* [2014]
[22] Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds), International Protection of Human Rights: ATextbook (A° bo Akademi University Institute for Human Rights, Turku 2009), 19, 27.
[23] Mistale Taylor, 'The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect' (2015) 5 International Data Privacy Law.
[24] Article 19 of the Universal Declaration of Human Rights.
[25] Case C-131/12, *Google Spain v AEPD and Mario Costeja Gonzalez* [2014] at para 41

judgment in this case established the right to write off where; An EU citizen can request that incorrect, insufficient, irrelevant, disproportionate or out-of-date search results related to them be removed entirely.[26]

In the Digital Rights Ireland case, the applicants fruitfully sought to repeal the 2006 data retention directive, which allowed telecommunications to preserve data for a period of between 6 months and 2 years for counterterrorism determinations. The reasons for revoking the directive were based on 3 articles in the charter; Article 7 Protection of the family and personal life, Article 8 the right to data protection, and Article 11 the right to freedom of expression. Thus, the right to data protection must be balanced with the right to freedom of expression under this article.

Under the European Union Freedom of Speech is recognized as human right that has been provided for under various International law instruments such as the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and the International Covenant on Civil and Political Rights[27].

The European Court of Human Right (ECtHR) has extensively interpreted the right to freedom of expression but has also been flexible to allow member states to put in place their own legislations with regard to freedom of expression vis-à-vis rights to data protection. One of the major case laws leading in the interpretation of the two rights is the freedom of press which is generally envisaged in the freedom of speech. The ECtHR has severally echoed the important role of the press in ensuring democracy which therefore means collecting and circulating information to ensure people are well informed. In addressing the issue on freedom of speech the court has stated that '*freedom of press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes of their political leaders. In particular it gives politicians the opportunity to reflect and comment in the preoccupations of public opinion; it thus enables everyone to participate in the free debate which is at the very core of the concept of a democratic society*'[28].

---

[26] *Ibid* at para 90.

[27] Oshisanya, 'lai Oshitokunbo, An Almanac of Contemporary and Comparative Judicial Restatements (ACCJR Supp. i Private Law): ACCJR Supplement I, (Almanac Foundation, 2020), P. 371.

[28] Castells v. Spain, Judgment of 23 April 1992, Series A no. 236.

The Court has also interpreted the two rights as of equal importance and measure and has gone ahead to interpret the place of data protection in exercise of the freedom of speech/press through precedents in case laws in order for member states to adopt the same in their legislations. The interpretation of the two rights have been addressed in the journalistic exemption interpreted by the ECtHR[29].

Thus, the right to data protection during the pandemic must be balanced against these fundamental rights enshrined in the Charter of Fundamental Rights in the EU and Germany.

3- Germany's position: Relationship between Protection of Personal Data and other Fundamental Rights:

The General Data Protection Regulation pursues to ensure both fairness of completion in addition to protection of fundamental rights; EU politicians are progressively enforcing the Regulation using fundamental rights persuasion.[30]

Section 22 of the BDSG had been corrected so as to give way to the processing of exceptional categories of data by private bodies for sake of public interest. This change was envisioned to support with deradicalization programs and to allow data to be transferred from private entities to public security bodies in these state of affairs enhance counter-terrorism efforts.[31]

Germany has restricted data subjects' rights granted under the GDPR and some of these derogations are controversial. Section 35(1) of the BDSG states that the right to erasure of personal data is will not be allowed if the erasure is of non-computerized processing if it would be unmanageable or would require an uneven amount of effort because of the way the data is stored, as long as the data subject's concern is measured as minimal and if the data is being processed as per the law. As such, restrictions of processing will apply instead of a right to

---

[29] N. J. Reventlow, 'Can the GDPR and Freedom of Expression Coexist?' (2020) *American Journal of international Law*, 31-34.

[30] 'Press Corner' (*European Commission - European Commission*, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> accessed 28 August 2020.

[31] 'Germany - National GDPR Implementation Overview' (*DataGuidance*, 2020) <https://www.dataguidance.com/notes/germany-national-gdpr-implementation-overview> accessed 28 August 2020.

erasure. Thus, this is derogation from the GDPR if data will be processed for solely the pandemic under Article 2 of the GDPR.

Section 27(2) of the BDSG restricts data subjects' right to restriction of processing under Article 18 of the GDPR to the degree it would most likely make it impossible or seriously interfere with the attainment of research or statistical purpose and such a limitation is essential in order to fulfill the research or statistical purpose.

Furthermore, Section 28(4) of the BDSG states that for data processing in light of archiving purposes for public interest the right to restriction of processing will not apply as long as it makes it unmanageable or defeats the purpose of the archiving purposes and limiting it is required in order to fulfill those purposes. Therefore, in relation to processing of personal data in light of the pandemic, going by the BDSG, citizens of Germany cannot bring an action against the government for processing their full data, as this is beneficial in the interest of the public and a threat to public health.

Sections 27 and 28 in conjunction with Section 22(2) of the BDSG sets out the German implementation of Article 89 of the GDPR, which states that processing done for archiving purposes in line with public interest, scientific or historical research or statistical should be done so in line with the suitable precautions for the rights and freedoms of individuals. Furthermore, it requires that where personal data is processed for these intentions, particular rights of data subjects may be restricted in line with suitable safeguards in place. Section 22(2) BDSG sets out the mandate for the safeguards in place that fall under Article 89(1) GDPR. They include: technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization and may include pseudonymisation provided that those purposes can be fulfilled in that manner.[32] Section 27(2) of the BDSG provides that in cases of data processing for purposes of scientific or historical research or for statistical purposes, this particular rights may be restricted to the point that they may render unmanageable or interfere with the above mentioned purposes and such restrictions are required for the fulfilment of research or statistical purposes: right of access, right to rectification, right to object and right to restriction of processing.

[32] Article 89(1) GDPR

Thus, in light of the pandemic, which is an issue on public interest, health and security, data subjects have limited right with regard to the GDPR, despite the BDSG going against the GDPR. Since using technological means to process personal data for purposes of scientific research of the Covid19 pandemic.

Similarly, Section 28 (2) to (4) of the GDPR states that for archiving purpose when processing data in line with public interest, this particular rights will not be used in certain situations: right to rectification, right to data portability, right to object, right of access and right to restriction of processing.

With regard to using video surveillance to process citizens' data, section 4 of the BDSG has particular rules that apply to video surveillance of public areas. It states that video surveillance of public areas should only be allowed to the point that it is essential to the following:

- for public bodies to perform their tasks;
- for determining whether access shall be allowed or denied; or
- to safeguard legitimate interests for specifically defined purposes.

Storage or use of data that has been gathered is allowed only if it essential to attain the proposed use and it does not interfere legitimate interests of data subjects.[33] Further processing of the data collected is only allowed in so far as to prevent threats to state and public security and to prosecute crimes.

The right to personal data protection is related to so many other rights such as the right to respect for private life/right to privacy, right to access information which shall be discussed herein under to bring out the relationship and the gaps that lie among the rights both at the national legislation and jurisdiction level and that of the European Union.

The right to respect private life /right to privacy is an international right provided for under the Universal Declaration of Human Rights (UDHR) and also provided for under the European Convention on Human Rights which is a treaty that Germany complies to. The European Convention on Human Rights provides that every person has the right to respect for his or her

[33] 'Germany - National GDPR Implementation Overview' (*Data Guidance*, 2020) <https://www.dataguidance.com/notes/germany-national-gdpr-implementation-overview> accessed 28 August 2020.

private and family life, correspondence and home. Public authority is prohibited from interfering with this right except where such interference is in accordance with the law.

Under the European Union, there have been stretches to balance the right to privacy and data protection to ensure there are no violations. It has therefore declared that the two rights have to be weighed up to other public interests such as national security of its member states. Therefore, where the state has to protect individual rights, it has to consider public interest and detriment to the society.

In Germany, the current law on Data Protection (Federal Data Protection Act) has provided regulations in ensuring the right to privacy is protected during data collection and processing through various requirements put in place. First the data controllers are required to be registered with the state authority. Secondly, the legislation also limits telemedia service providers to collect and use persona data to a limited extent which is specifically provided for in law and which requires the data subject to consent. Section 13 of the German Telemedia Act protects data subjects by providing that the controller must inform the user of the scope and purpose of the processing of personal data for any consent issued to be valid. Where the consent has been used by the data subject and the consent is given knowingly and unambiguously, the right to privacy is protected because the information will be used for the specified purposes. There are areas where consent is not usually required and this includes where the personal information is used for business-related purposes[34].

Germany legislations have recognized the fact that in collecting data for processing, the right to privacy might be infringed and has therefore put in place remedies under The Federal Data Protection Act to address infringements that may occur. The data subject has a right to access, effect correction, demand erasure and blockage of their information. These rights can be implemented through judicial recourse which issues injunctive orders which have been brought about by the principle of self- determination of the private data in Germany[35].

[34] E. Palmer, 'Library of Congress'. Retrieved from Online Privacy Law: Germany: https://www.loc.gov/law/help/online-privacy-law/2017/germany.php, accessed 28 September 2020.
[35] Ibid

The remedies provided for under data protection have been recognized as right to access to information but limited by one's consent. In Germany, the right of information is limited to public bodies of the Federal Government with limitation to complaints of the data subject and subject matter of the complaint. This therefore means that the government does not require information from individuals without bringing out the reason for requiring information and securing its protection[36].

In cases where searches and seizures are required by law, they are regarded as interfering with the right to privacy and freedom of expression. It is therefore required that there should be regulations by statute that provide for searches and seizures. In Germany the conditions for searches and seizures include that the search or seizure should strictly comply with the law and there has to be necessity and proportionality applied in searches. Search of persons' homes or workplaces for the purposes of collection of date should be compatible with freedom of expression and privacy if ordered by a court of law and consider proportionality principle under the international laws. Where such searches are not in accordance with the law, they are prohibited as they amount to violations of individuals' right to privacy, data protection and freedom of expression and therefore contravention of an individual's human rights[37].

In Germany, the Federal Constitutional Court (FCC) has played a major role in the development of data collection to ensure the protection of fundamental rights. This was possible through the main decision Micro Census which ruled that it is contrary to human dignity to catalog and record an individual and there must be a ban where nobody can interfere and so that a person can enjoy privacy[38].

In 2009, the Federal Court of Justice in a decision in which a teacher had asked for an injunction against an Internet portal that published evaluations of its performance by the students, the court held that the teacher on information disclosure was authorized because it was provided

[36] D. Grimm, M. Wendel and T. Reinbacher, European Constitutionalism and the German Basic Law, https://link.springer.com/chapter/10.1007/978-94-6265-273-6_10, accessed 28 September 2020.

[37] *The Global Principles on the Protection of Freedom of Expression and Privacy*'. (2019). London: Free World Centre.

[38] Decisions of the Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts – BVerfGE) 65, 14, 15. December 1983, http://www.bverfg.de/e/rs19831215_1bvr020983.html, accessed 28 September 2020.

to a circle of people interested in the information and in the work environment, the rights to data protection are minimal[1]. Other courts have also played a great role in redefining the limits in data protection and clearing the controversy and confusion that arises in regard to protection of other constitutional rights. One of the major controversies that the courts have dealt with, is the balancing of competing interests between right to privacy and the right to informational self-determination.

The right to informational self-determination was implemented by the Federal Constitutional Court in 2008 allowing the processing of personal data where it is permitted by statute or consent for by the data subject. This was further expanded in2009 by echoing the constitutional guarantee of confidentiality and integrity of IT systems in the use of personal data[2].

The European Union Court of Justice has endeavored to differentiate between the right to privacy and data protection through interpretation. In its interpretation, the Court has placed the right to privacy to be limited to legal persons while right to data protection applies to all persons including organizations and institutions as it covers information. This differentiation has been raised in the Data Protection Convention and the Data Protection Directive. Although the Court has endeavored to do this differentiation, the GDPR does not create obligations among private parties with regard to data protection. It is therefore left for the member states to address issues of data protection among private parties[3].

Freedom of speech versus the right to data protection has created debates both in the legal system in Germany and the European Union. In Germany, the German Data Protection Act regulates the intrusion of privacy in collection of data which therefore means reduced data processing and therefore limiting the freedom of expression. This is the provided for strict

---

[1] Decisions of the Federal Court of Justice, 23 June 2009, Docket No. VI ZR 196/08, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=e299e63452248193f28e4ef4031e7ae7&nr4860&pos=16&anz=23, accessed 28 September 2020.

[2] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -, paras. 1-333, http://www.bverfg.de/e/rs20080227_1bvr037007en.html, accessed 28 September 2020

[3] E. Büyüksagis, Towards a Transatlantic Concept of Data Privacy, *(2019),*The *Fordham Intellectual Property, Media and Entertainment Law Journal, V. 30, N. 1,* https://ir.lawnet.fordham.edu/iplj/vol30/iss1/*,* accessed 28 September 2020.

interpretation of the law which generally prohibits personal data processing unless the data subject's consents to the same. The Constitution has clearly stipulated the freedom of speech as one of the human rights which should be freely embraced but with the provisions of the Data Protection Act, there arises a conflict on how to balance the right to data protection and exercising the freedom of speech.

The German Constitutional Court, in the interpretation of the two rights has held that the freedom of speech is a 'special' constitutional right and that it is required to be exercised with caution in order to safe guard other rights such as the data protection rights. In instances where the data protection rights collide with freedom of expression, none of the rights should be rated to be superior to the other and this has been applicable in public debates as well as matters of public interest. However, in order to ensure a balance between the two, courts have recognized a presumption in favour of speech to ensure self- actualization especially in matters of public interest. This does not however apply to private sector as the courts have restricted forms of expressions that breach data protection[1].

The Court in many instances has dealt with the conflict between data protection laws and the freedom of speech on a case to case basis and there is no specific legal principle that addresses the same and one may see a controversy in some provisions of the Data Protection Act when compared to Article 5 of the German Federal Constitution which provides for freedom of expression but courts are not in trying to increase the controversy and are therefore restricted to narrow interpretation[2].

An example of case law where the court had to interpret the right to data protection and freedom of press was Germany Federal Constitutional Court/1BvR 16/13[3]**.** In this case, the plaintiff, a man convicted of murder in 1982 and released in 2002, filed a constitutional appeal

---

[1] BVerfG, Order of the First Senate of 04 November 2009 - 1 BvR 2150/08 - paras. 1-87), https://www.bundesverfassungsgericht.de/e/rs20091104_1bvr215008en.html, accessed 28 September 2020.

[2] Z. Efroni, '*Data Protection and Free Speech in Germany*'. (2010, November 1). Retrieved from The Centre for Internet and Society at Stanford Law School: http://cyberlaw.stanford.edu/blog/2010/11/data-protection-and-free-speech-germany, accessed 28 September 2020.

[3] BVerfG, Order of the First Senate of 06 November 2019 - 1 BvR 16/13 -, paras. 1-157, http://www.bverfg.de/e/rs20191106_1bvr001613en.htm, accessed 28 September 2020.

against a judgment of the Federal Court of Justice (Bundesgerichtshof). The legal question that arose was the relationship between the plaintiff's right to data protection to the news magazine's right to freedom of speech and freedom of press. The court in determination of this legal questions raised an issue of whether online press archives may be required to take measures to protect individual's right of forgotten which is a right under individual data protection. In deciding this court the court recognized the position of the ordinary national courts in in addressing matters that were affected by the EU legislations which has not been fully adopted into national law[1].

The Federal Constitutional Court held that claims for protection against dissemination of old press articles must be reviewed taking into consideration the conflicting interests between individual data protection and freedom of press/freedom of expression. Therefore, the operator of an online archive should take into consideration the privacy of the affected person in ensuring the right to data protection is not violated while exercising the freedom of speech. Although the matter was referred back to the Federal Court of Justice, the Constitutional Court addressed the issue of failure to harmonise the laws between the European Union and its member states. It therefore relied on the national law of Germany in determining the issues at hand and stated that the EU law will only be applicable where the national laws do not substantively address the issues at hand [2].

The GDPR under Article 85 provides member states shall adopt legislation that reconciles the right to the protection of personal data with the right to freedom of expression and information, including the processing of journalistic, academic and artistic information. The challenges that come with the flexibility is that member states are at liberty to adopt these provisions into their national legislations and therefore a state can fail to adopt the same in order to fulfil the provisions of the GDPR. Reviews have indicated that states have been slow in adopting the journalistic exemption which therefore means that states are more sided in implementing the protection of data rather than the freedom of press that is a branch of the

[1] Z. Efroni, '*Data Protection and Free Speech in Germany*'. (2010, November 1). Retrieved from The Centre for Internet and Society at Stanford Law School: http://cyberlaw.stanford.edu/blog/2010/11/data-protection-and-free-speech-germany, accessed 28 September 2020.

[2] E. M. HERZOG, Dialogue and Diversity. The "Right to be forgotten" – decisions of the Federal Constitutional Court, http://www.medialaws.eu/rivista/dialogue-and-diversity-the-right-to-be-forgotten-decisions-of-the-federal-constitutional-court/, accessed 28 September 2020.

freedom of expression and countries in adopting the data protection laws should consider a balance in ensuring both the freedom of speech and data protection law[1]. Further, that member states have not brought out a clear picture on whether they are finding means of balancing the data protection obligation while also protecting the freedom of expression.

Freedom of expression requires that sources of information are protected and it therefore accompanies a non-disclosure clause unless there is consent by the source of information, necessity or a court order after fair hearing is obtained and dictates that the source of information can be revealed.

In Germany, the right to information has been recognized under the right to data protection through the GDPR which gives a person a right to information with regard to a person under their care. Upon such request being made, the responsible person must provide information required relating to that person within a month. However, companies have faced challenges where such information is not processed directly and there is a risk of being accessed by a third party.

The Covid-19 pandemic has brought about confusion in very many stakeholders and dealing with data protection has not been exemption. Issues arising as a result of the covid-19 especially in data protection include how to manage the virus while protecting human dignity including data protection. The world has shown links between the use of personal data in preventing more infections of the virus which therefore raises the question on how to reduce or ensure data protection while managing the pandemic[2].

Currently there are two divisions with regard to the covid-19 pandemic and the status of data protection. There are those who believe that the use of private data is essential in the management of the pandemic while there are those who believe data protection and individual privacy should still be paramount in management of the virus and therefore creates a conflict on the management of the virus while ensuring data protection[3].

---

[1] N. J. Reventlow,.'Can the GDPR and Freedom of Expression Coexist?' (2020) *American Journal of international Law*, 31-34.

[2] F. Zampati, '*Covid 19 and Privacy: Persona Data Rights*'. (2020).Retrieved from Global Open Data for Agriculture & Nutrition: https://www.godan.info/news/covid-19-and-privacy-personal-data-rights, accessed 28 September 2020.

[3] Ibid.

The European Union is addressing the issue set a series of guidelines on the processing of personal data with regard to dealing with corona virus which include creating a balance between the general public health and personal data protection in dealing the corona virus. The European Data Protection Board reminded the member states to take into consideration the E- Privacy Directive in the processing of electronic communication. It also recognizes that governments have the power to invoke the state of emergency in such circumstances and brings to the attention on its member states to use the data from the subjects by the data controllers for that particular purpose to ensure lawful processing of personal data[1].

In Germany, the Government has put in place special provisions to address the issue of data protection while managing the corona virus. The German PDAs have put reminders that the testing and management of the virus should take into consideration the German Federal Data Protection Act. Some of the regulations put in place include: data processing for employment related purposes where necessary for entering into, carrying out or terminating employment contract or any other employment-related purpose, the processing of personal data shall be in accordance with the provided legal obligations under the employment laws, social security and social protection law and there should be no reason to believe that the data subject has an overriding legitimate interest in not processing the data. Further that processing of personal data shall be permitted by public and private bodies where the main reason for such processing is public interest in the public health sector and therefore protecting the people against threats to health[2].

In terms on collecting and sharing information, contacts and physical addresses may be required for tracing and therefore protecting others who have been in contact with the data subject involved. Information about the health status may also be shared to manage other employees in case of a workplace and therefore essential. However, despite all the requirements the consent of

[1] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009XX0606(04), accessed 28 September 2020.

[2] D. G. Arms, '*Covid -19 and Data Protection Compliance in Germany*' (2020, April 3), Retrieved from white & Case: https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance-germany, accessed 28 September 2020.

the data subject is still required and therefore the requirements of data collection and processing are still recognized in the management of the corona virus. It is therefore required that the personal data shall not be kept longer than is required on the grounds of covid-19 pandemic persistence and the data shall be processed in a manner that ensures protection of the individual's privacy and avoid unauthorized data processing and consumption[1].

In conclusion, data protection has a narrow sense in differentiating it with the right to privacy and despite the European Court of Justice and national courts of Germany trying to differentiate the two, there in a connection between the two rights and therefore protection of both rights are intertwined. Data protection is related to other rights such as the freedom of expression, right to access information and courts have created strides in interpreting the conflicts on interests that come hand in hand with respecting those rights and freedoms.

Although the European Union Court of Justice has made interpretations between the freedom of expression and the right to data protection, the Germany jurisdiction has been different due to the flexibility granted the European Court of Justice in member states adopting the interpretation. It is therefore paramount for the legislation of Germany to balance between al the competing rights including the freedom of press to ensure no right is infringed while trying to protect another right.

The relationship between the right to data protection and right to information is basically based on the remedies a person has where their data has been subject to terms they did not consent to and therefore can seek remedy of rectification, delete and even being de-listed from the search specifications. It also allows an individual who is the data subject to question where institutions share personal data to a third party without their consent.

The European Union Court of Justice is therefore the greatest tool that can address the gaps that arise among the rights and freedoms discussed herein and share the directives for adoption by the member states to ensure that the gaps are addressed and that no right or freedom is treated as inferior compared to another especially in instances where member states have failed to address such issued through legislation.

[1] Ibid.

In dealing with covid-19, the state should take into consideration the need to balance between the rights of its citizens to good health and the right to protection of data as contact tracing and following up on infections is paramount in managing the corona virus pandemic. This can be through setting out legislation that limits the use of information collected for the purposes of corona-virus for that limited purpose in the required institutions. Since corona virus is an emerging issue and there is yet more to be done in terms of research to understand how well to deal with it while protecting the people's rights, it is well to note that Germany still has time to discover on how to protect both health interest and personal interests on the its people. It is also well to recognize that the European Union is playing an important role in creating directives which can be adopted by its member states in ensuring all rights are taken care of for the benefit of its people.

CONCLUSIONS AND RECOMMENDATIONS:

In conclusion, there are a lot of problems concerning the protection of personal data in Germany and the EU in general. The laws that have been created to solve this very important issue do not seem to give enough protection to Germans and Europeans in general. Despite there being laws that cover this important area, it has not been officially recognized as an autonomous right in the EU. In Germany, the data protection laws (BDSG) even go contrary to what is expected of them under the GDPR. As it is well known, the GDPR is a binding legal document on all European Union member states that takes precedence over national laws. However, German lawmakers have not given it the supremacy it deserves.

With regard to the use of technology in containing and controlling the spread of the virus, the fact that downloading and using the app is voluntary is in itself ineffective. Secondly, education levels with regard to the use of technology in containing the virus are low. The use of technology is only effective in reaching the younger generation and the more reasonably thinking ones. In fact, technology is pretty ineffective in containing the virus as we speak. Thus, a lot has to be done. Below are some recommendations that can be taken into account to make it more effective and eventually curbing the spread of this deadly virus.

Recommendations:

The use of technology in controlling and eliminating the spread of the virus

The use of the Corona-Warn app in Germany is of voluntary use. Those who want to download it can use it. However, if it is voluntary, only a small percentage of the population will download it not knowing the importance. First, the app should be made mandatory for all citizens of Germany to have it on their smartphones. If they do not own a smartphone, there should be a system of keying in your results on a PC or through a central health center. Second, citizens ought to be educated on the importance of the use of technology during this pandemic. Just the way everybody has an application on their phones for transport, the same should go for the Corona-Warn app. The German government should continuously reassure its citizens of their data protection through television adverts, radio adverts and other channels used to advertise people's rights in using technology to fight the virus. The government has a responsibility towards its citizens to protect their data, which under human rights law falls under a negative obligation. The

German government should continuously educate them on how hackers are using new technologies and work around those to protect data.

The need for clarity from the EU Court of Justice:

The Court of Justice needs to come clear on the need for recognizing the right to data protection and not classify it as a right to privacy. With technology developing at a fast speed, the Court of Justice needs to acquaint itself with latest technology and from there realize that due to the change in technology, data protection needs to be recognized as an autonomous right. Furthermore, with more cases coming to the ECJ for preliminary ruling to explain Article 8 of the Charter, there is a growing and urgent need for the Court to recognize this autonomous right.

Limitations recognized under Article 52 of the Charter should not include data protection because of the ever-changing technological landscape in Europe. Europe has already realized the need for recognizing the right to data protection and its importance in European society. Therefore, why should it have limitations? The purpose of Article 52(1) of the Charter is to reproduce some of the rights laid down in the Convention of Human Rights like privacy and freedom of religion, which determines the conditions to interfere with these rights.[1] Since data protection is an autonomous right on its own, why then should it be equated to the convention rights and have interferences?

E - Privacy Directive 2002/58/EC

The E- Privacy Directive, safeguards the confidentiality of electronic communications in the EU. The E- Privacy Directive is a key instrument to protect privacy and it includes specific rules on data protection in the area of telecommunication in public electronic networks. However, there are short falls with this Directive and for it to be effective and up to date in this era with the pandemic at hand, the following recommendations should be considered:

- The Directive should be replaced with a Regulation. Directives are not directly applicable in EU member states. A directive is a goal from the European Union and it is up to

[1] Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in The European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology.

the member state on how to reach that goal. A regulation on the other hand is uniformly applied legislative act binding on all EU member states.

- The new law should refer to the GDPR definition.
- The scope of the rules should extend from telecom services to also include applications such as Google, WhatsApp and Facebook.
- There should be more transparency in reporting.

BDSG recommendations to enhance improved data protection to Germans

Germany has relied on the opening clauses contained in the GDPR in a rather a biased manner.[2] The European Commission has already threatened to start an contravention procedure against Germany.[3] However, the following recommendations should be taken into consideration to ensure that there is thorough data protection of its citizens especially during this pandemic when the use of technology is of importance to help contain and curb the virus. The margin for German legislators left by the GDPR is profoundly condemned. The GDPR talks about "specifications or restrictions of its rules by Member State law".[4] German legislators have in the alternative used the terms "Öffnungsklauseln" (opening clauses) and "Regelungsaufträge" (regulatory mandates) for classification.[5] The total number of legal mandates and preferences is at roughly 70.[6] The GDPR is therefore said to resemble in parts a Directive as its is up to the member state to implement it to achieve the desired goal of the European Union.

Article 1(5) BDSG states that the provisions of the Act shall not apply where the GDPR and Regulation (EU) 2016/680 directly applies. Thus, the following Acts need to be reconsidered so that they fall within what is permitted by the GDPR:

---

[2] Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020

[3] *Ibid*

[4] Recital 8 GDPR

[5] Roßnagel, A. and others, National Implementation of the GDPR: Challenges, Approaches, Strategies Policy Paper, January 2018.

[6] (*Dip21.bundestag.de*, 2020) <https://dip21.bundestag.de/dip21/btd/18/113/1811325.pdf> accessed 28 August 2020.

- Section 27 & 28 BDSG, which concerns the right to restriction of processing data.
- Section 29 BDSG, the investigatory powers of supervisory authorities.
- Section 32 & 33 BDSG, which concerns when information must not be provided to data subjects.
- Section 35 BDSG, which deals with the right to erasure.

These are important sections of the Act, which are applicable to data protection during the pandemic, and if they are not reviewed, it will be hard using technology to process people's personal data so that it can help contain the virus. This will also enable people to gain trust from the government.

BIBLIOGRAPHY

1- ARTICLES:

- Alexander Klimburg and others, 'Digital Epidemiological Measures to Combat the Coronavirus Pandemic' (Hague Center for Strategic Studies 2020) <https://www.aies.at/download/2020/AIES-Studies-2020-12.pdf> accessed 15 August 2020.
- Alexander Rossnagel, 'Legislation Within the Framework of the General Data Protection Regulation: Tasks and Scope of the German Legislator?' (2017) 41 Data Protection and Data Security-DuD.
- Alvar Freude and Trixie Freud, 'Echos Of History: Understanding German Data Protection'.http://www.bfna.org/publication/newpolitik/echos-ofhistory-understanding-german-data-protection accessed on 11th August 2020
- B. van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law.
- Bart Van Der Sloot, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right* (Springer 2017).
- Ch. Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.
- D. G. Arms, '*Covid -19 and Data Protection Compliance in Germany*' (2020, April 3), Retrieved from white & Case: https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance-germany, accessed 28 September 2020.
- D. Grimm, M. Wendel and T. Reinbacher, European Constitutionalism and the German Basic Law, https://link.springer.com/chapter/10.1007/978-94-6265-273-6_10, accessed 28 September 2020.
- D. Korff, 'EC Study On Implementation of Data Protection Directive 95/46/EC' (2002) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667> accessed 27 August 2020.
- E. Büyüksagis, Towards a Transatlantic Concept of Data Privacy, *(2019),*The *Fordham Intellectual Property, Media and Entertainment Law Journal, V. 30, N. 1,* https://ir.lawnet.fordham.edu/iplj/vol30/iss1/, accessed 28 September 2020.
- E. M. HERZOG, Dialogue and Diversity. The "Right to be forgotten" – decisions of the Federal Constitutional Court, http://www.medialaws.eu/rivista/dialogue-and-diversity-the-right-to-be-forgotten-decisions-of-the-federal-constitutional-court/, accessed 28 September 2020.
- E. Palmer, '*Library of Congress*'. Retrieved from Online Privacy LaW:Germany: https://www.loc.gov/law/help/online-privacy-law/2017/germany.php, accessed 28 September 2020.
- European Union, 'The GDPR: new opportunities, new obligations' (*Ec. europa.eu*, 2020) <https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf> accessed 6 August 2020.

- FluidSurveys Team, '3 Types of Survey Research, when to Use Them, And How They Can Benefit Your Organization! - Fluidsurveys' (*FluidSurveys*, 2020) <http://fluidsurveys.com/university/3-types-survey-research-use-can-benefit-organization/> accessed 5 August 2020.
- F. Zampati, '*Covid 19 and Privacy: Persona Data Rights*'. (2020).Retrieved from Global Open Data for Agriculture & Nutrition: https://www.godan.info/news/covid-19-and-privacy-personal-data-rights, accessed 28 September 2020.
- J. Kokott and C. Sobotta, 'The Distinction Between Privacy and Data Protection in The Jurisprudence of The CJEU and The Ecthr' (2013) 3 International Data Privacy Law.
- Hannah van Kolfschooten and Anniek de Ruijter, *'COVID-19 And Privacy in The European Union: A Legal Perspective On Contact Tracing'* (2020) 41 Contemporary Security Policy.
- Hussin A. Rothan and Siddappa N. Byrareddy, 'The Epidemiology and Pathogenesis of Coronavirus Disease (COVID-19) Outbreak' (2020) 109 Journal of Autoimmunity.
- Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in The European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology.
- Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review.
- G. Stepanova, '*The Privacy',* (2019, October 2019). *Data Protection and Cybersecurity Law Review.* Retrieved from The Law Reviews: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210039/germany, accessed 28 September 2020.
- Klaudia Klonowska, Pieter Bindt, ' The COVID-19 pandemic: two waves of technological responses in the European Union' HCSS 2020 <https://www.jstor.org/stable/resrep24004?refreqid=excelsior%3Ab578f8667f7a429a3be69325900ace5b&seq=1#metadata_info_tab_contents> last accessed on 27th July 2020
- Luiz Costa and Yves Poullet, 'Privacy and The Regulation of 2012' (2012) 28 Computer Law & Security Review.
- Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv lnt'l L J 81, 134 citing Huvig v France App No. 11105/84 (ECHR, 24 April 1990) 35.
- Matthew L Levine, *'Contact Tracing for HIV Infection: A Plea for Privacy'* (1988) 20 Columbia Human Rights Law Review 157.
- Mistale Taylor, 'The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect' (2015) 5 International Data Privacy Law.
- N. J. Reventlow,.'Can the GDPR and Freedom of Expression Coexist?' (2020) *American Journal of international Law*, 31-34.
- Nuria Oliver, '*Mobile phone data for informing health actions across the COVID-19 pandemic life cycle'* (Science Advances*,* 5th June 2020) < https://advances.sciencemag.org/content/6/23/eabc0764> accessed 27th July 2020
- Remco Takken, 'EU Member States Loosen Privacy Rules for Location Data to Contain COVID-19' <https://www.geospatialworld.net/blogs/eu-member-states-covid-19/> accessed 5 August 2020.

- 'Secondary Research- Definition, Methods and Examples. | Questionpro' (*QuestionPro*, 2020) <https://www.questionpro.com/blog/secondary research/#:~:text=Secondary%20research%20or%20desk%20research,involves%20using %20already%20existing%20data.&text=Secondary%20research%20includes%20researc h%20material,already%20filled%20in%20surveys%20etc.> accessed 5 August 2020.
- SKW Schwarz Rechtsanwälte, 'Germany: Data Protection Laws and Regulations 2020', https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany
- Steven Feldstein, *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace, 2019) https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 accessed on 12th August 2020
- Z. Efroni, '*Data Protection and Free Speech in Germany*'. Retrieved from The Centre for Internet and Society at Stanford Law School: http://cyberlaw.stanford.edu/blog/2010/11/data-protection-and-free-speech-germany, accessed 28 September 2020.

2- BOOKS:

- Augustin Fuerea, Manualul Uniunii Europene (Universul Juridic 2011).
- C.J Bennett, Regulating privacy. Data protection and Public Policy in Europe and the U.S, (Cornell University Press, 1992).
- D. Wright, P. De Hert, Enforcing Privacy: Regulatory, Legal and Technological Approaches, (Springer, 2016).
- Isaiah Berlin, Four Essays On Liberty (Oxford University Press 1969).
- Marko Milanovic, The Extraterritorial Application of Human Rights Treaties (OUP, Oxford 2011)
- Mariusz Krzysztofek, 'GDPR: General Data Protection Regulation (EU) 2016/679. Post-Reform Personal Data Protection in The European Union' (Wolters Kluwer 2019)
- Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds), International Protection of Human Rights: ATextbook (A° bo Akademi University Institute for Human Rights, Turku 2009)
- Oshisanya, 'lai Oshitokunbo, An Almanac of Contemporary and Comparative Judicial Restatements (ACCJR Supp. i Private Law): ACCJR Supplement I, (Almanac Foundation, 2020).
- Ronald Leenes and others, *Data Protection and Privacy: (In)Visibilities and Infrastructures* (36th edn, springer 2017).
- Ulrich Dammann, Otto Mallmann and Spiros Simitis, *Data Protection Legislation* (Metzner 1977).

3- LEGISLATIONS:

- EUROPEAN LAW

- European Union Charter of Fundamental Rights, 2012/C 326/02.
- Decision no.1082/2013/ EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC [2013] OJ L293/1

- General Data Protection Regulation (GDPR), regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Treaty on the Functioning of the European Union.
- Universal Declaration of Human Rights.

- GERMAN LAW

- 'Federal Data Protection Act (BDSG)' of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

4- EU CASES:

- *Bodil Lindqvist v Åklagarkammaren i Jönköping* (CJEU, 6 November 2003) C-101/01, ECLI:EU:C:2002:513.
- Case C- 112/00, *Eugen Schmidberger, Internationale Transporte und Planzu¨ge v. Republik O¨ sterreich* [2003] ECR 2003 I-05659.
- Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C: 2014:317.
- Case C-275/06, *Promusicae v. Telefo´nica de Espana,* [2008] ECR 2008 l-00271
- Case C-396/98, *The Queen vs. Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, [2000] ECR 2000 I-06751.
- Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR 2009 I-03889.
- Castells v. Spain, ECR, Judgment of 23 April 1992, Series A no. 236.

5- WEBPAGES:

- 'An Open Letter to The Members of the Wassenaar Arrangement' (*Human Rights Watch*, 2020) <https://www.hrw.org/news/2014/12/01/open-letter-members-wassenaar-arrangement> accessed 14 August 2020.
- Andrea Jelinek, 'Statement On the Processing of Personal Data in The Context of The COVID-19 Outbreak.' (*European Data Protection Board*, 2020) <https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf> accessed 20 August 2020.
- Center for Economic and Social Justice, 'Economic, Social and Cultural Rights – A Guide to the Legal Framework', http://www.cesr.org/ downloads/Legal%20Duties.pdf. accessed on 27th August 2020.
- Christian Geminn, 'The New Federal Data Protection Act – Implementation of The GDPR in Germany' <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 August 2020.
- Cornelia Wels, 'The Struggle to Create COVID-19 Contact-Tracing Apps' (*Healthcare-in-europe.com*, 2020) <https://healthcare-in-europe.com/en/news/the-struggle-to-create-covid-19-contact-tracing-apps.html> accessed 15 August 2020.

- Costica Dumbrava, 'Tracking Mobile Devices to Fight Coronavirus' (*Europarl.europa.eu*, 2020). <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf> accessed 15 August 2020.
- 'Digital Contact Tracing During COVID-19: The Pros and Cons We Must Consider' (*UC Institute for Prediction Technology*, 2020) <http://predictiontechnology.ucla.edu/digital-contact-tracing-during-covid-19-the-pros-and-cons-we-must-consider/> accessed 15 August 2020.
- 'Early Warning and Response System (EWRS)' (*European Centre for Disease Prevention and Control*, 2020) <https://www.ecdc.europa.eu/en/early-warning-and-response-system-ewrs> accessed 13 August 2020.
- 'EPIC - EU Privacy and Electronic Communications (E-Privacy Directive)' (*Epic.org*, 2020) <https://epic.org/international/eu_privacy_and_electronic_comm.html> accessed 19 August 2020.
- 'EUR-Lex - L14547 - EN - EUR-Lex' (*Eur-lex.europa.eu*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14547#:~:text=The%20principle%20of%20direct%20effect,relates%20to%20certain%20European%20acts.&text=In%20this%20judgement%2C%20the%20Court,but%20also%20rights%20for%20individuals.> accessed 5 August 2020.
- Jon Cohen and Kai Kupferschmidt, 'Mass Testing, School Closings, Lockdowns: Countries Pick Tactics in 'War' Against Coronavirus' (*Science | AAAS*, 2020) <https://www.sciencemag.org/news/2020/03/mass-testing-school-closings-lockdowns-countries-pick-tactics-war-against-coronavirus> accessed 15 August 2020.
- Hannah Murphy, 'US and Europe Race to Develop 'Contact Tracing' Apps' (*Ft.com*, 2020) <https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95> accessed 14 August 2020.
- Hasan Chowdhury, Mathew Field, Margie Murphy, 'When will the UK 'track and trace' app be ready- and how will it work?' (15th July 2020) <https://www.telegraph.co.uk/technology/2020/07/15/track-trace-app-uk-google-apple-when-download/> accessed 27th July 2020.
- 'Germany: Land of Data Protection and Security – But Why?' (*home*, 2017) <https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why> accessed 11 August 2020.
- 'Germany: Privacy | Lexology' (*Lexology.com*, 2020) <https://www.lexology.com/library/detail.aspx?g=1809070b-c64a-480f-bed2-fa7991546946> accessed 11 August 2020.
- 'Germany - National GDPR Implementation Overview' (*DataGuidance*, 2020) <https://www.dataguidance.com/notes/germany-national-gdpr-implementation-overview> accessed 28 August 2020.
- 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (European Data Protection Board 21st April 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf accessed on 11th August 2020.

- Karl Schmedders, Josè Parra-Moyano and Michel Avital, 'Coronavirus: Digital Contact Tracing Doesn'T Have to Sacrifice Privacy' (*IMD business school*, 2020) <https://www.imd.org/research-knowledge/articles/coronavirus-digital-contact-tracing-doesnt-have-to-sacrifice-privacy/> accessed 13 August 2020.
- 'Law in Germany - DLA Piper Global Data Protection Laws of the World' (*Dlapiperdataprotection.com*, 2020) <https://www.dlapiperdataprotection.com/index.html?t=law&c=DE> accessed 5 August 2020.
- Lucette Mascini and others, 'EU Expert On European Response to Virus: 'Telecom Data for Tracking Corona Can Be Made Anonymous' - Innovation Origins' (*Innovation Origins*, 2020) <https://innovationorigins.com/eu-expert-on-european-response-to-virus-telecom-data-for-tracking-corona-can-be-made-anonymous/> accessed 14 August 2020.
- Megan Bourdon and Ruqqayah Moynihan, 'One of The Largest Cities in France Is Using Drones to Enforce the Country's Lockdown After the Mayor Worried Residents Weren't Taking Containment Measures Seriously' (*Business Insider*, 2020) <https://www.businessinsider.com/coronavirus-drones-france-covid-19-epidemic-pandemic-outbreak-virus-containment-2020-3?IR=T> accessed 15 August 2020.
- Natasha Lomas, 'Digital Mapping of Coronavirus Contacts' (*Techcrunch.com*, 2020) <https://techcrunch.com/2020/04/15/digital-mapping-of-coronavirus-contacts-will-have-key-role-in-lifting-europes-lockdown-says-commission/> accessed 14 August 2020.
- Nicole Wetsman, 'What Is Contact Tracing?' (*The Verge*, 2020) <https://www.theverge.com/2020/4/10/21216550/contact-tracing-coronavirus-what-is-tracking-spread-how-it-works> accessed 13 August 2020.
- Nuria Oliver, '*Mobile phone data for informing health actions across the COVID-19 pandemic life cycle'* (Science Advances*,* 5th June 2020) < https://advances.sciencemag.org/content/6/23/eabc0764> accessed 27th July 2020.
- 'Overview: How We Preserve Privacy and Maintain Security' (*Pepp-pt.org*, 2020) <https://www.pepp-pt.org/content> accessed 14 August 2020.
- 'Precedence of European law' (*Eur-lex.europa.eu*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548> accessed 5 August 2020.
- 'Press Corner' (*European Commission - European Commission*, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> accessed 28 August 2020.
- Roßnagel, A. and others, National Implementation of the GDPR: Challenges, Approaches, Strategies Policy Paper, January 2018.
- (*Dip21.bundestag.de*, 2020) <https://dip21.bundestag.de/dip21/btd/18/113/1811325.pdf> accessed 28 August 2020.
- 'Statement on the processing of personal data in the context of the COVID-19 outbreak' (European Data Protection Board 20th March 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en> accessed on 11th August 2020
- Stefan Krempl,'Datenschutzreform: EU-Kommission droht Deutschland mit Vertragsverletzungsverfahren'<https://www.heise.de/newsticker/meldung/Datenschutzreform-EU-Kommission-droht-Deutschland-mit-Vertragsverletzungsverfahren-3689759.html > accessed on 12th August 2020

- 'Timeline: How The New Coronavirus Spread' (*Aljazeera.com*, 2020) <https://www.aljazeera.com/news/2020/01/timeline-china-coronavirus-spread-200126061554884.html> accessed 4 August 2020.
- Thomas Wahl, 'Infringment Proceedings for Not Having Transposed EU Data Protection Directive' <https://eucrim.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/ > accessed on 12th August 2020.
- 'Tracking Mobile Devices to Fight Coronavirus' (*Europarl.europa.eu*, 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf> accessed 19 August 2020.
- 'What Is Personal Data Under GDPR? | The UK Domain' (*The UK Domain*, 2020) <https://www.theukdomain.uk/what-is-personal-data/> accessed 6 August 2020.
- 'Why Is (Big) Phone Data So Valuable in Combatting The COVID-19 Pandemic?' (*Orange.com*, 2020) <https://www.orange.com/en/news/2020/April/Why-is-big-phone-data-so-valuable-in-combatting-the-COVID-19-pandemic> accessed 15 August 2020.
- Wojciech Wiewioroski, 'EU Digital Solidarity: A Call for A Pan-European Approach Against the Pandemic' (2020) <https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf> accessed 14 August 2020.
- Zakariae El Ouazzani and Hanan El Bakkali, 'A New Technique Ensuring Privacy in Big Data: K -Anonymity Without Prior Value of the Threshold K' (2020) <https://reader.elsevier.com/reader/sd/pii/S187705091830108X?token=49EBDD114E76B38B7739429A79A41387FE793373AE396803F11E8362A135720C00C0DB292045BD85F3A07E9340BDB62A> accessed 15 August 2020.