PROTECTING DIGITAL DATA PRIVACY AS A TRANSNATIONAL RIGHT AND NATIONAL SECURITY CONSIDERATIONS: A Study of the Judgement of Germany Federal Constitutional Court of 19 May 2020

اعداد

الدكتور/ محمد أبو بكر عبد المقصود عبد الهادى

مجلة حقوق دمياط للدراسات القانونية والاقتصادية – كلية الحقوق – جامعة دمياط

العدد السادس يوليو - 2022

Abstract

Protection of national security is among the major duties of the government agencies, and the acquisition of intelligence has become a major security measure. The Federal Intelligence Service is tasked with the role and its modaze of operation targets maximum acquisition of intelligence. It might be useful in averting potential security threats amidst continuous terror attacks, but its impacts on the infringement of personal privacy are a major cause for concern. In light of the Judgment of the Federal Constitutional Court, it is evident that the Federal Intelligence Service contravenes the fundamental right to privacy in its activities. The activities extend beyond the mere collection of intelligence on criminal activities to piling large volumes of personal data, especially on foreign nationals. This study utilizes a literature survey methodology to delve into the

matter and obtain meaningful findings. The findings are used to formulate viable conclusions and recommendations.

INTRODUCTION

Digital data protection and national security are crucial considerations in the security infrastructure of any given country. The EU General Data Protection Regulation (GDPR) is the main information protection law that currently offers the legal framework for protecting personal information and promoting responsible data processing.[1] This law is perceived to be effective, but the advancements in technology make it challenging for it to comprehensively address privacy issues. Some of the technological advancements resulting digital data protection challenges include identity, Big Data, social media,

[1] Edward S. Dove, 'The EU General Data Protection Regulation: Implications for International Scientific Research in The Digital Era'.

and biometrics.[1] These advancements have made it easier for government agencies to monitor personal data and filter intelligence for national security purposes. Protection of national security within this scope might be justified, but the infringement of personal privacy that accompanies it is daunting. The rapid transformations in technology have outgrown existing legal frameworks and increased the capabilities and information superiority to states, resulting in a shift in the balance between digital privacy and the protection of state security. It is worth noting that the premises of surveillance and its role in governance seem to override the value of digital privacy. The main course of worry is that the territorial limits of digital surveillance seem undefined.[2] In light of the judgment by the Germany Federal Constitutional

[1] Itay Perah Fainmesser, Andrea Galeotti and Ruslan Momot, 'Digital Privacy'.

[2] Lorenza Violini and Antonia Baraggia, *The Fragmented Landscape of Fundamental Rights Protection in Europe* (Edward Elgar Publishing 2018).

Court of 19 May 2020, several digital privacy issues, especially in the international space, need to be addressed. [1]This court ruled that intelligence services are under no legal obligation to randomly search digital information for foreigners living abroad.[2] The ruling follows findings that the German foreign intelligence agency BND has been operating in violation of the universal right to privacy. This raging

[1] *"The constitutional complaint challenges the statutory provisions authorising the Federal Intelligence Service to carry out surveillance of foreign telecommunications, to share the intelligence thus obtained with domestic and foreign bodies and to cooperate with foreign intelligence services in this context. Insofar as they concern cooperation and the surveillance of foreign telecommunications, the challenged provisions were inserted into the Federal Intelligence Service Act of 20 December 1990, last amended by Art. 4 of the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 of 30 June 2017, through the Act on the Surveillance of Foreign Telecommunications by the Federal Intelligence Service of 23 December 2016, which entered into force on 31 December 2016. The law was amended in response to findings and discussions in the First Committee of Inquiry of the 18th German Bundestag and served to clarify the legal framework given that the Federal Intelligence Service had been engaging in these practices prior to the amendment. By contrast, the challenged provisions on data sharing predate the amendment and their wording was not changed by it; however, they now also extend to the sharing of intelligence gathered on the basis of the newly added surveillance powers".* **BVerfG, judgment of May 19, 2020 - 1 BvR 2835/17.**

[2] Ibid.

debate and onslaught of legal battles make it necessary to address balancing digital data protection and the protection of national security.

Changes in information technology have transformed the way of conducting different tasks. Some of these changes have allowed government monitoring of online information for surveillance and other security purposes. As much as online data management is essential for protecting national security, instances abound where it interferes with the individuals' digital privacy. Efforts made towards harmonizing digital data protection while at the same time protecting national security are yet to bear fruit. The struggles between the community advocating for privacy and government agencies seeking to protect its territories through digital surveillance have been characteristic of the recent court cases. This struggle has led to the development of competing interests between protecting

individuals' privacy and law enforcement. Thus, the need to balance digital data protection and national security is still a challenge that necessitates suitable interventions.

This study will address the challenge of digital data privacy within the context of state security, which seems to be a very crucial aspect of the sustainability of any given nation. It will seek to establish the limitations in the existing legal frameworks which allow national intelligence agencies to circumvent individual privacy restrictions, especially in the international space. The study will also provide suitable interventions that can be used to address loopholes in the legal frameworks to ensure that the national intelligence agencies operate with restrictions to respect personal privacy. Additionally, the study will devise countermeasures to ensure that lessening restrictions and surveillance activities by the

national intelligence agencies do not interfere with the protection of national security.

This study is structured into two chapters, Chapter one covers digital privacy and national security as the two major issues causing a stalemate in the activities of the national intelligence agencies. It also addresses the need to balance digital privacy and the protection of national security using highlights from research publications. Chapter two addresses the core issue of balancing digital privacy and the protection of national security. It entails a cross-examination of the EU and German constitutional systems and insights from the revelations on the surveillance schemes used by national intelligence agencies in data acquisition. The role of courts in balancing digital data privacy and the state security is also discussed in light of rulings from various court cases, including the Judgment of the German Federal Constitutional Court of 19 May 2020.

CHAPTER ONE: DIGITAL PRIVACY AND NATIONAL SECURITY

1- Digital Privacy Protection

The increase in online activity over the past decades has increased the availability and amounts of digital data.[1] This trend has been accompanied by negative consequences owing to the increased accessibility to individual-level data. The main opportunity for data exploitation is through the government intelligence agencies. These entities constitute government adversaries, and their data usage and access may be harmful to the public. In most cases, government intelligence agencies seek digital data to track down individuals and make arrests.[2] According to Weber, the transition towards the digital world raises privacy challenges because digital privacy laws and the

[1] Fainmesser, Andrea G. and Ruslan M., 'Digital Privacy'

[2] Ibid., 29.

concept of digital privacy are being exposed to immense limitations arising from technological advancements such as digital identity and biometrics.[1] The existing privacy protection frameworks include fundamental rights and specific laws. Fundamental rights are crucial to the international legal structure and relate to personal privacy rights. Despite their levels of sophistication, these rights do not suffice to address all privacy challenges manifesting in the digital space.[2] National laws attempt to compensate for these limitations by extending the fundamental privacy protections to emerging technologies and scenarios. According to the UN Universal Declaration of Human Rights, protecting human dignity is a

[1] Rolf H. Weber, 'The Digital Future – A Challenge for Privacy?'.

[2] Ibid., 235.

fundamental requirement.[1] The European Convention on Human Rights also has prompt protection for human rights, which applies to government and private sectors.[2] Specific laws addressing privacy issues entail constitutional safeguards that have been amended over the years to include different facets of conduct.[3] Federal laws have also been instituted towards the same.

Current privacy concerns include third-party access to online information, social media logins, profiling, and government data.[4] As much as most of these concerns constitute a threat to online privacy, profiling and government

[1] United Nations, 'Universal Declaration of Human Rights' (United Nations 2015) <https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf> accessed 2 July 2021.

[2] European Court of Human Rights, 'European Convention On Human Rights' (1950) <https://www.echr.coe.int/documents/convention_eng.pdf> accessed 2 July 2021.

[3] Weber, 'The Digital Future, 235.

[4] Ibid.

data serve as the major threats within national intelligence agencies. Profiling entails any form of automated personal data processing whose main aim is to analyze or determine the personality or any other aspects of a given individual.[1] It mainly involves analyzing health, employment performance, economic metrics, behavior, or personal preferences. According to the EU Data Protection Regulation (DPR), profiling should be limited, especially when personal data will be used for legal decisions.[2] The governments collect huge chunks of information from the citizens based on different administrative laws. This accumulation of huge amounts of consumer data increases privacy risks when combined with

[1] Out-Law.com, Profiling rules should not apply unless individuals' rights are 'significantly affected', says privacy body, 23.05.2013, <http://www.out-law.com/articles/2013/may/profilingrules-should-not-apply-unless-individuals-rights-aresignificantly-affected-says-privacy-body/>.

[2] Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance And The Scope Of EU Law At The Court Of Justice Of European Union' [2021] The Modern Law Review.

additional data in the public domain.[1] Secret service agencies can use the data for various forms of targeted action, which infringes individuals' privacy rights.

Privacy protection measures for government data should include stringent regulations of the collected and stored data concerning the amount and type of information allowed to be reserved.[2] The role of usability, confidentiality, and safeguarding personal information is increasing due to digital technologies' impacts on people's daily financial, personal and corporate activities.[3] This aspect is covered under the data protection rights, which guarantee individuals' rights of disposal over any personality-related information. The fundamental right to personal information protection is

[1] Weber, 'The Digital Future, 238.

[2] Ibid.

[3] Chuleeporn Changchit, 'Data Protection and Privacy Issue' (2008), 1.

covered by the major national and international legal frameworks.[1] It operates between the right to privacy and the possibility of suppressing the prevalence of privacy. Within the digital space, collection, storage, and processing of large amounts of data can potentially result in privacy infraction.[2] To cater to this issue, individuals should be entitled to knowing the kind of personal information communicated to the public or any given entity. This aspect will serve as a control measure over the information held by other people about the individual and personal identity information. The need to monitor special operations and enforce surveillance through the technology system using intelligence agencies raises intense concerns about personal privacy. Its

[1] Ibid., 2.

[2] David Banisar& Simon Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1 (1999)

manifestation alongside the numerous models implemented towards personal data protection also raises debates concerning the necessity of these models. The models of data protection include sectoral regulation, comprehensive legislation, and sectoral legislation and technology protections.[1] Countries guaranteeing the best right to personal information protection combine these models to achieve the required levels of effectiveness.

The comprehensive legislation model builds on common regulations concerning the accumulation, use, and distribution of personal information. It was deployed in the Data Protection Directive 95/46 in Europe, which puts the member states under obligation to implement common levels of personal data protection when processed or transferred outside EU

[1] Chuleeporn Changchit, 'Data Protection, 3.

countries.[1] This approach ensures that private sectors, special agencies of commissions monitor the implementation of personal data protection. Self-regulation is very common and entails setting limitations on specifications and possible violations by various entities in different spheres of operation.[2] This method capitalizes on how the different entities know the specific kinds of personal information collected and how it is utilized. The use of information technology has made it easier to collect and disseminate personal information, and its associated privacy challenges necessitate the need for personal

[1]European Commission, 'Directive 95/46/EC of the European Parliament and of The Council of 24 October 1995 On The Protection of Individuals with Regard to The Processing of Personal Data and On the Free Movement of Such Data' (European Commission 1995) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3AHTML> accessed 2 July 2021.

[2] Changchit, 'Data Protection, 3.

data protection.[1] This initiative deploys different technical tools which provide different levels of communication and personal privacy protection. Such systems will help limit the distribution of personal information by providing individuals access to their information and communication surveillance.[2] Despite the availability of different digital privacy protection models, comprehensive legislation is the most widely used, and its deployment will be analyzed in government surveillance agencies.

2- The Impact of National Security in The Information Privacy

The debate on digital privacy and national security cuts across the main basic values of an individual. These basic

[1] Jorida Xhafaj and Almarin Frakulli, 'The Impact of Public Interest in The Information Privacy: Analyze of The Ecthr Decisions' (2017) 6 International Journal of Business & Technology.

[2] Ibid.

values include freedom of expression, public interest, confidentiality, information security, national and public security, and criminal disclosures.[1] Based on this puzzle, it is evident that some of the freedoms and other interventions aimed at providing personal security to the citizens might be sacrificed to protect national security. The protection of national security majorly entails protecting the citizens from threats regardless of the source.[2] This obligation implies that the country has a huge task of deploying all possible means to ensure that the citizens are safe. However, the main challenge is the need for boundaries in protecting national security while not infringing on personal privacy. Since legislative

[1] Olga Gurkova and Jovan Ananiev, 'National Security V. Protection of Personal Data in the EU' (2012) 3 Iustinianus Primus L Rev 1.

[2] Gurkova and Jovan Ananiev, 'National Security v. Protection of Personal Data in the EU',7.

interventions are the major tool deployed in this case, it raises numerous legal questions than answers.

Different areas of human rights and national security overlap, and these areas are indispensable and mutually reinforcing for each other.[1] Human rights are analyzed within the scope of human security, and its main significance is respecting the fundamental freedoms and rights as a way of achieving individual, national and international security. Human security and National security can coexist because human security strengthens national security and compels nations to protect fundamental human rights.[2] The debate on this relationship has culminated into the need to weigh between personal privacy and national security. Major concerns revolve around suppressing some of the fundamental

[1] Ibid., (10).

[2] Ibid., 2.

human rights for national security gains, such as fighting terrorism or any other threat to the nation's security. Another challenge regards the possibility of holding rights to protecting personal privacy in situations where national security is being threatened. For successful national security protection, especially in the case of national intelligence agencies, there must be personal information of all kinds for criminal investigations.[1] However, its necessity at times culminates into disparities concerning the protection of personal information.

The need to strike a balance between digital privacy and national surveillance is continuously increasing. This increase is fueled by the rapid technological changes which enable intelligence agencies to use various smart techniques in

[1] Gurkova and Jovan Ananiev, 'National Security (2012),9.

surveillance.[1] The adoption of such techniques might be helpful to national security, but individual privacy is perceived to be at risk. Most individuals perceive surveillance as a negative activity that encompasses coercion, loss of freedom, and covert spying.[2] These activities pose a great threat to privacy, and the threat is even greater considering the technological enhancements that have increased the capabilities of surveillance systems. Research findings show that the increasing use of surveillance systems and analytics by intelligence organizations within the digital space is continuously transforming nations into less personal environments.[3]

[1] Daniel J. Power, Ciara Heavin and Yvonne O'Connor, 'Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide' [2021] Journal of Business Analytics (1).

[2] Ibid., 1.

[3] Ibid., .

In the case of national intelligence agencies, personal privacy is even worse because of the centralized controls and access to large amounts of data from government agencies.[1] Many people in different countries are affected by surveillance, especially when collecting evidence about crimes. The main influence towards digital surveillance bases on the observation the current society is built on information.[2] This perception has led to the government drive towards acquiring information for various purposes, including criminal policing.[3] Increased data collection by government agencies at all levels has escalated the threat to digital privacy from

[1] Wullianallur Raghupathi and Viju Raghupathi, 'Big Data Analytics In Healthcare: Promise And Potential' (2014) 2 Health Information Science and Systems.

[2] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and The Prospects Of An Information Civilization' (2015) 30 Journal of Information Technology.

[3] Danah Boyd and Kate Crawford, 'Critical Questions for Big Data' (2012) 15 Information, Communication & Society.

national surveillance and other institutions. [1]National surveillance has numerous harms to the individuals, including reduced intellectual privacy, altering power dynamics between the leaders and subordinates, and in extreme cases, blackmail and other behaviors.[2]

The EU General Data Protection Regulation (GDPR) is a legal framework for protecting personal data in the EU region. It attempts to counterbalance digital privacy and the protection of national security by acknowledging the fast changes in digital technology, which have escalated the magnitude of personal data collected and distributed.[3] Data

[1] Zuboff, 'Big Other, 76.

[2] Richards, N. (2013). The dangers of surveillance. Harvard Law Review. May 20, 126 Harv. L. Rev. 1934, https://harvardlawreview.org/2013/05/the-dangers-ofsurveillance

[3] Edward S. Dove, 'The EU General Data Protection Regulation: Implications for International Scientific Research in The Digital Era' (2018) 46 Journal of Law, Medicine & Ethics (1013).

protection laws have been existent in Europe within its political and cultural contexts. Some of these contexts include the secret police surveillance in Germany. These laws contextualize the long-standing tradition in Europe where citizens and governments strive to minimize interference into individuals' private lives.[1] The data protection law in Europe is distinct because processing personal data is prohibited, and the exception only applies where valid legal reasons are allowing it. In this context, all the personal data collected, processed, or disseminated must be regulated. The Directives under the EU law require the individual nations to transpose the Directives into their national legal framework.[2] This aspect leaves the enforcement aspect at the discretion of the individual nations. The discrepancy might explain the reason

[1] Ibid., 1014.

[2] Y. Poullet, "EU Data Protection Policy. The Directive 95/46/EC: Ten Years After," Computer Law & Security Review 22, no. 3 (2006): 206-217, at 206.

for digital data privacy issues associated with Germany's national intelligence agency activities. Over the years, the 1995 Directive has been losing relevance due to the advancements in digital technology because of increased large volume data flows.[1] The legal framework has also failed to prevent fragmentation in the implementation of the Directive. This limitation has fueled legal uncertainty concerning the risks to protecting personal information accumulated through online activities.[2]

The US and EU data protection laws resemble several aspects, including the fundamental principles regulating their operations. Among the similar fundamental principles is the principle of proportionality and clarity in the processing of

[1] Dove, 'The EU General Data Protection Regulation, 1013.

[2] Y. Poullet, "EU Data Protection Policy, 208.

personal data.[1] The main discrepancy is that surveillance for state security is exempt from the legal framework. This discrepancy is perceived as a loophole in the protection of digital privacy because it allows the national intelligence agency to access and process personal information without legal protections. The legal exemption for national security is attributed to the terrorist attacks that compelled the government to prioritize national security. As a threat to national security, terrorism has made many nations, including the US and Germany, accord the intelligence and law enforcement officer's greater authority in collecting and

[1] Bignami, F. 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens'. (2015) Study for the LIBE Committee, European Parliament, PE 519.215, pp. 1–40.

disseminating personal information acquired through electronic and wire surveillance[1].

Additionally, national intelligence agencies are at liberty to sacrifice individuals' right to privacy and increase the scope of their surveillance activities. They are also allowed to contravene data protection protocols to access all sorts of information for foreign intelligence and investigate international terrorism threats.[2] Over the years, policymakers have made efforts to strengthen the legal frameworks on privacy and information security, but many legal gaps still exist. These legal loopholes enable intelligence agencies to have an upper edge on the domestic and foreign surveillance

[1] Doyle, Ch. 'Terrorism: Section by Section Analysis of the USA Patriot Act'. (2001) CRS Report for Congress, 10 December.

[2] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts Before and After The NSA Affair' (2017) 56 JCMS: Journal of Common Market Studies (4).

regulations. In Europe, EU Law regards privacy and information security as a fundamental right.[1] It provides legal foundations for protecting individuals' right to privacy by limiting incursion from third parties, particularly government agencies. Since being recognized as a fundamental right, the scope of the right to privacy and information safety has been intensifying within and outside Europe.[2] This expansion is crucial because the rules apply in the EU and other international institutions are required to abide by the EU laws.

[1] Horsley, T. '"The Court Hereby Rules ..." – Legal Developments in EU Fundamental Rights Protection'. (2015) JCMS, Vol. 53, Annual Review, pp. 108–27.

[2] Brkan, M. 'The Unstoppable Expansion of EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) Maastricht Journal of European and Comparative Law, Vol. 23, No. 5, pp. 812–41.

CHAPTER TWO: BALANCING DIGITAL PRIVACY AND NATIONAL SECURITY

Analysis of the US and EU constitutional systems shows an intense battle between the safeguarding of personal privacy and state security.[1] This battle mainly arises from the escalating challenge of global terrorism, which poses a great threat to state security. The threat compelled the countries to devise massive secret surveillance programs tapping large amounts of personal data through collaboration with telephone and internet providers.[2] Revelations of the surveillance programs by the national intelligence agencies have raised doubt concerning the balance between digital privacy and the

[1] Luca Pietro, Vanoni. "Balancing privacy and national security in the global digital era: A comparative perspective of EU and US constitutional systems" [2018] ELECD 894; in Violini, Lorenza; Baraggia, Antonia (eds), "The Fragmented Landscape of Fundamental Rights Protection in Europe" (Edward Elgar Publishing, 2018) 114

[2] Ibid., 114.

protection of national security in the digital terrorism era. The availability of a legislative framework for safeguarding personal privacy in the EU has not been sufficient to cover up for the faults and derogations affecting the capacity to protect the right to privacy.[1] In national security, the main discrepancy under the EU law is that it heavily relies on member state competence. The implementations might not be in sync with the Union law. This delicate balance has resulted in a system where state governments are expected to protect the citizens against security threats such as terror attacks. At the same time, the Union provides a high level of protection for personal data.[2] Despite attaining some level of efficacy, the power balance and jurisdictional references make it challenging to balance digital data protection and state security.

[1] Ibid., 116.

[2] Vanoni. "Balancing privacy and national security in the global digital era: A comparative perspective of EU and US constitutional systems", 120.

To establish a proper balance between state security and digital information protection, one needs to appreciate the role of surveillance in governance. In the digital technology era, surveillance helps governments gather adequate information about their territories and exercise control.[1] It also helps the government fulfill its basic roles, but unregulated surveillance is a major challenge because it undermines the privileges of a democratic society. Surveillance has gradually transformed into a governance technique whereby governments face increasing needs of massive control of a continuously changing human society.[2] Despite the increasing importance of surveillance, its necessity must be analyzed in the scope of the fundamental right to privacy. Surveillance accounts for the

[1] Jing, Ran. "Striking the Balance between Privacy and Governance in the Age of Technology." SPICE: Student Perspectives on Institutions, Choices and Ethics 11, no. 1 (2016): 2, (18).

[2] Ibid, (20).

need for information superiority in governance and law enforcement.[1] This aspect becomes a disadvantage by making it easier to compromise privacy when government agencies increase surveillance to accommodate the need for information on national security issues.

1- Role of The European Court of Human Rights in balancing Digital Privacy and the Protection of National Security

Applying case law in the European court context capitalizes on distinctions between public security and national security.[2] In this context, state security is restricted within the scope of member countries rather than the entire Union. Data

[1]Janne, Hagen and Olav Lysne. "Protecting the Digitized Society—the Challenge of Balancing Surveillance and Privacy." The Cyber Defense Review 1, no. 1 (2016): 75-90. Accessed June 28, 2021. http://www.jstor.org/stable/26267300.

[2] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection (2017) 56 (1).

privacy legislation is mostly used in public security, and it encompasses a broader context that includes security within the Union. Public security relates to the safety of the European community, and it is found in other grounds of EU law. The GDPR does not apply to public security or national security, and this makes it inapplicable to data analysis related to state security.[1] Directive 2016/680 is the main legal instrument enabling data processing for national security purposes.[2] It regulates the protection of personal information in the context of investing, preventing, detaining, or prosecuting criminals and averting threats to national security.[3] The same Directive

[1] Ibid., 5.

[2] Juraj, Sajfert and Quintel, Teresa, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3285873

[3] Ibid.

also allows the countries to limit information on various subjects to protect state or public security.

Case law on balancing digital privacy and national security is found in the jurisprudence of the ECtHR. It expresses the possibility of balancing between the two crucial security aspects as it states in Article 8 ECHR that individuals have a right to private life. Still, this right can be tampered with to protect national security.[1] In *Klass and Others v Germany* (1978), the ECtHR failed to establish violations of the right to respect private life.[2] This conclusion based on the establishment that the law restricting secrecy of telecommunications and email was vital for protecting national security and preventing crimes. Secret surveillance during

[1] Greer, S. (1997) The Exceptions to Articles 8 to 11 of the European Convention on Human Rights (Strasbourg: Council of Europe Publishing) (18).

[2] Klass and others v Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978.

anti-government protests on the demonstrators was found to violate Article 8 ECHR as per the ruling in *Association '21 December 1989' and Others v Romania* (2011). This ruling was arrived at because the Romanian system of storing information lacked adequate precautions to safeguard the privacy of the demonstrators.[1] In the case of terrorism, the ECtHR holds that the fight against terrorism supersedes an individual's right to access their data in police databases as per the case *Segerstedt-Wiberg and Others v Sweden* (2006). Despite the interference with the rights under Article 8 ECHR, storage of the information was necessary to protect national security.[2]

[1]Association "21 December 1989" and Others v. Romania, No. 33810/07, ECtHR (Third Section), 24 May 2011

[2] Segerstedt-Wiberg and ors v Sweden, Merits and just satisfaction, App no 62332/00, ECHR 2006-VII, (2007) 44 EHRR 2, IHRL 3288 (ECHR 2006), 6th June 2006, European Court of Human Rights [ECHR]

These cases projected a certain trend that case law in European courts initially strived to balance data protection and state security in a neutral manner.[1] However, after Snowden's revelations on mass surveillance measures, the courts started tilting the balance towards privacy protection rather than national security. This move can be understood as a countermeasure to check on the immense data privacy infringements committed by the national intelligence agencies in the name of safeguarding national security.[2] Additionally, leaning towards privacy protection was the only suitable intervention that could help the citizens reserve their rights under Article 8 ECHR.

[1] Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection (2017),12.

[2] Ibid.

The Court of Justice of the European Union (CJEU) has been elemental in this shift by providing policymaking infrastructure to support privacy protection. In *Digital Rights Ireland* (2014), the CJEU annulled the data retention directive designated as Directive 2006/24/EC.[1] This decision aimed at addressing interference with the fundamental rights because the communications service providers were mandated to hold personal data for a certain period, and government agencies had access to this data. In this case, the CJEU acts as a policy change catalyst to challenge the balance between digital data protection and state security.[2] According to the CJEU, the EU legislator challenged the balance by adopting the Data Retention Directive because it imposed compulsory data

[1] Digital Rights Ireland Ltd V Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C-594/12) EU:C:2014:238 (08 April 2014)

[2] Dimitrova and Brkan, 'Balancing National Security and Data Protection (2017),13.

retention schemes without catering to privacy rights and data protection.[1] The main reason driving the decision the serious nature of the Directive's interference with Article 8 ECHR because the scope and duration of data retention, the potentials of mapping and profiling, and the risk of unlawful use of the data were very high. Thus, it was viewed that the intensity of jurisdictive review must be proportional to the level of discretion available to the EU legislator.

2- Analyze of the Germany Federal Constitutional Court Judgment of 19 May 2020

The First Senate of the Federal Constitutional Court ruled that the authorities of the Federal Intelligence Service conduct surveillance of foreign telecommunications infringe

[1] Granger, M. - P., and K. Irion. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection." European Law Review 39, no. 4 (2014): 835-850.

the fundamental rights of the basic law.[1] This ruling followed complaints from various parties, including journalists reporting human rights violations in authoritarian states and conflict zones. They raised a constitutional complaint challenging the amended version of the Federal Intelligence Service Act of 2016 and the probable surveillance measures that could be subjected under this legislation.[2] The amended Act granted the Federal Intelligence Surveillance Service powers to access networks and telecommunications transmission routes. This power was meant to enable them to collect data of interest to the intelligence services through analytic tools. Since the data collection is a form of strategic surveillance, this power is not tied to specific suspicions. It relates to the telecommunications

[1] BVerfG, judgment of the First Senate of May 19, 2020 - 1 BvR 2835/17 -, Rn. 1-332, http://www.bverfg.de/e/rs20200519_1bvr283517.html

[2] Sebastian, Klein. "Federal Administrative Court Prohibits Storage and Use of Telecommunications Metadata by the Federal Intelligence Service." Eur. Data Prot. L. Rev. 4 (2018): 110.

between foreigners in foreign countries, and the data is majorly used for national security protection, including obtaining crucial information concerning security threats.

The constitutional complaint was majorly against the legal provisions granting the Federal Intelligence Service the rights to collect, store and compute data in the surveillance of foreign telecommunications.[1] It also challenged the preexisting provisions that allowed the Federal Intelligence Service to share the information obtained with foreign public and private entities and the domestic public entities, including the police. Cooperation with foreign intelligence agencies was also a major cause of concern because it escalated the digital data protection issue. In light of these complaints, the First Senate of the Federal Constitutional Court found that the statutory

[1] BVerfG, judgment of the First Senate of May 19, 2020 - 1 BvR 2835/17 -, Rn. 1-332, http://www.bverfg.de/e/rs20200519_1bvr283517.html

bases of the Federal Intelligence Service (Bundesnachrichtendienst – BND) violate the fundamental right to privacy of telecommunications and the freedom of the journalists.[1] The court decision also capitalized on the rights against state interference, the need for protection against telecommunications surveillance, and protecting the foreigners in other countries.[2] It established that the surveillance measures lack necessary restrictions and lack various safeguards such as the protection of journalists and lawyers. The data-sharing provisions are also a threat to digital privacy because they lack limits for protecting any legal interests that meet the required statutory thresholds.

[1] Klein. "Federal Administrative Court Prohibits Storage and Use of Telecommunications Metadata by the Federal Intelligence Service." Eur. Data Prot. L. Rev. 4 (2018): 110.

[2] Melissa Eddy, 'Right To Privacy Extends To Foreign Internet Users, German Court Rules (Published 2020)' (*Nytimes.com*, 2020) <https://www.nytimes.com/2020/05/19/world/europe/germany-privacy.html> accessed 3 July 2021.

Another cause of concern is that inadequate provisions are governing the cooperation with foreign intelligence agencies.[1] The lack of these restrictions poses a threat to the privacy of various entities, especially legal interests. Additionally, the powers granted to the Federal Intelligence Service are not subject to independent oversight. Such immense power raises questions about the possibility and ease of abuse of power to infringe individuals' privacy because lack of continuous legal oversight makes it challenging to scrutinize the surveillance process. These concerns validated the ruling that the right to privacy applies to foreign internet users. It is a crucial step towards attaining digital privacy because it limits the powers of the intelligence services from

[1] BVerfG, judgment of the First Senate of May 19, 2020 - 1 BvR 2835/17 -, Rn. 1-332, http://www.bverfg.de/e/rs20200519_1bvr283517.html

randomly searching digital data of foreigners living abroad.[1] The court decision also provides necessary checks and balances in the operations of the Federal Intelligence Service to minimize cases of intentional violation of the individuals' privacy using statutory provisions. Additionally, it has also shed light on the preemptive legal measures that provide legal cover for the intelligence agency's violations of the foreign individuals' right to privacy.

The Court concluded in its ruling a set of legal principles that, under Art. 1(3) of the Basic Law, Fundamental rights bind the German state authority; yet, the obligatory influence is not delimited to Germany territory alone. The security that individual fundamental rights yield differs depending on an individual residence, whether in Germany or abroad. In any

[1] Eddy, 'Right To Privacy Extends To Foreign Internet Users.

event, Art. 10(1) and Art. 5(1) second sentence of the Basic Law, which, in their dimension as rights against state interference, afford protection against telecommunications surveillance and protect foreigners in other countries.

The contemporary legal structure on the scrutiny of remote telecommunications, the allocation of intellect thus acquired with other bodies, and the collaboration with overseas intelligence services infringes the prerequisite to explicitly stipulate the affected fundamental rights, which is enshrined in Art. 19(1) second sentence of the Basic Law (Elisabeth, 2019). The lawmakers purposefully considered the existing legal structure not to affect fundamental, yet they are a fundamental facet in this scenario. The existing legislative structure7809- also does not alleviate crucial fundamental necessities arising from fundamental rights.

Art. 10(1) of the Basic Law safeguards the discretion of individual communications as such. It implies that people`s freedom and right to private communications should be respected. Those that violate their fundamental rights in respect to the same matters are not excluded from the protection afforded by the basic rights of the Basic Law just by the virtual of acting as representatives of foreign legal entities. Overseas Legal Aptitude Regulates affairs concerning foreign intelligence. This legislation is spelled out within the meaning of Art. 73(1) no. 1 of the Basic Law. Based on this capability, the Confederacy can deliberate upon the Federal Intelligence Service the duty of availing intelligence to the Federal authority concerning foreign and security policy but also the separate task of the early detection of dangers with an international dimension that originates from abroad, so far as it does not bring about operational powers. It is a must that these

perils be of such nature and severity that they can distress the position of the Federal Republic of Germany in the intercontinental environment. They ought to be substantial to the overseas foreign safety policy precisely for the same reason.

In standard, the premeditated shadowing of overseas telecommunications is not unharmonious with Art. 10(1) of the Basic Law. Nevertheless, the legal requirement is not based on explicit requirements. Essentially, it is guided and constrained only by the drive. The authority to conduct strategic surveillance is an incomparable influence that must be constrained to congregating external aptitude piloted by an authority that lacks operative controls; it is only the authority's particular tasks and the specific conditions under which it performs them that can vindicate them.

Consequently, the lawmaker must provide for the exclusion of telecommunications statistics of Germans and individuals within Germany. Limits to data that may be gathered, the grit of particular surveillance drives, the organizing of surveillance grounded on especially resolute procedures, special requirements for the targeted surveillance of specific individuals, limits to traffic data retention, a framework governing data analysis, safeguards to protect confidential relationships of trust, the guaranteed protection of the core of private life and obligations to delete data. Such measures ensure that while such data is crucially obtained for enhancing the administration of justice, other vital provisions of basic human rights are upheld. Through such mechanisms, the system of administering justice enhances the element of fairness and equal treatment for suspects.

Sharing private files originating from premeditated scrutiny is only allowable for the resolution of safeguarding legal interests of predominantly great weight. It entails indications of a recognizable vulnerability (konkretisierte Gefahrenlage) or adequately specific grounds for detecting felonious conduct (hinreichend konkretisierter Tatverdacht). Reports delivered to the Federal Government are immune to these necessities as they are exclusively envisioned to offer dogmatic intelligence and formulate government verdicts. The sharing of personal data necessitates an official decision by the Federal Intelligence Service and must be documented, stipulating a valid legal basis. Before data is shared with foreign bodies, it must be established that the addressee will handle the information in agreement with the rule of law; should there be a suggestion that data sharing could endanger an individual affected by it, a valuation of probable jeopardies

in the explicit occasion is paramount. The absence of such valuation is considered unlawful, and necessary legal actions may follow.

A legislative framework on the collaboration with overseas aptitude services only gratifies the statutory necessities if it certifies the limits set by the rule of law. The limits are not set aside through the mutual sharing of intelligence, and that the Federal Intelligence Service remains accountable for the information it has gathered and scrutinized. The federal intelligence service also-rans checks on data collected to identify biases and inaccuracies. Identified setbacks must be eliminated before the data is thereof put in any use or transferred.

Suppose the Federal Intelligence Service needs to use quest conditions persistent by a partner intelligence service to

share any matches without any detailed content-related analysis robotically. In that case, these search terms and the resulting matches must be checked thoroughly. The requirements to obtain assurances that apply to the sharing of data with other countries apply accordingly. The sharing of traffic data in its entirety with partner intelligence services requires a competitive necessity for intelligence concerning specific indications of an identifiable hazard. The Federal Intelligence Service must obtain substantial assurances from the partner services regarding their handling of the shared data. The mandate to run premeditated investigation measures to share the intelligence thus obtained and cooperate with foreign intelligence services is only companionable with the proportionality necessities if they are complemented by independent oversight. Such oversight must be deliberated as intermittent legal oversight allowing for wide-ranging access

to scrutinize the surveillance process. The measures are geared towards ensuring effective administration of justice in the society.

Alternatively, it must be guaranteed that the key bureaucratic steps of deliberated shadowing are subject to sovereign oversight similar to legal assessment by a body that has the power to make ultimate critical decisions. More so, the procedures must be subject to administrative oversight by a body that conducts randomized oversight of the legality of the entire surveillance process on its initiative and without interference from any foreign bodies.

The utilitarian individuality of the oversight organizations must be certain. This considers that the oversight bodies have a detached budget, autonomous personnel supervision, and bureaucratic independence. They should be

armed with the workforces and means necessary for the operational performance of their tasks. They must have all controls compulsory for directing operative oversight vis-à-vis the Federal Intelligence Service. It also must be guaranteed that the third-party rule does not obstruct oversight.

Digital privacy has become a major challenge due to the increase in online activity, and the EU legislative structures have been struggling to address it through legal frameworks. The main threat to digital privacy is government agencies, specifically the Federal Intelligence Service, which seeks intelligence to protect national security. It seeks digital data to track down individuals, make arrests and detect security threats related to terrorism. However, intelligence-seeking ventures end up sacrificing personal privacy for the attainment of national security. Fundamental rights and specific laws constitute the majority of the current privacy frameworks.

These frameworks have not been effective enough due to the systemic loopholes and legal exceptions that allow the Federal Intelligence Service to conduct excessive surveillance. The major loophole in the protection of digital privacy has been the escalating threats of terrorism, increasing in multitude due to increasing online activity. Surveillance, especially when seeking evidence for crimes, affects many citizens, including foreigners in other countries, because of the digital surveillance systems' immense capabilities. The enforcement of EU laws and directives is also left at the discretion of individual nations, making them cherry-pick the specific aspects of the legal frameworks that should be enforced. It has resulted in the exploitation of legal loopholes in the domestic and foreign surveillance regulations[1].

[1] Rojszczak, M. (2021). Extraterritorial Bulk Surveillance after the German =

Countries contravene the individual's right to privacy by deploying massive secret surveillance programs that tap huge volumes of data by collaborating with telecommunications and internet providers. Notable incidents of case law on balancing state security and personal privacy include secret surveillance during anti-government protests, which violate Article 8 ECHR. Snowden's revelations of massive surveillance measures have also raised concern on the role of courts in balancing privacy protection and national security[1]. The Judgment of the Federal Constitutional Court in May 2020 provides answers to the surveillance issues raised. The Federal

=

BND Act Judgment. European Constitutional Law Review, 17(1), 53-77, See at: https://www.cambridge.org/core/journals/european-constitutional-law-review/article/extraterritorial-bulk-surveillance-after-the-german-bnd-act-judgment/D6B51E73049E18D9EEB563F36CEB679E

[1] Malgieri, Gianclaudio and De Hert, Paul, European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges (October 30, 2016). D. Gray and S. Henderson (eds.), Cambridge Handbook of Surveillance Law, 2017, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2948270

Intelligence Service commits numerous human rights violations in the course of its surveillance schemes. The privacy infringements were concerning telecommunications between foreigners in foreign countries. It portrays a major legal loophole allowing the Federal Intelligence Service to collect, store and compute data in surveillance of foreign telecommunications. Preexisting provisions allowing the intelligence agency to share information and collaboration with foreign intelligence agencies also constitutes a major challenge to digital privacy.

Increasing online activity seems to be a major incentive to the Federal Intelligence Service due to the ease of collecting large amounts of data. The levels of sophistication of the tools also enable them to escalate the degree of personal privacy infringements because it results in the collection of more data which is advantageous to national security. The intelligence

agency uses the same techniques of tracking down criminals on ordinary civilians hence casting a threat to their privacy. The surveillance schemes deployed by the intelligence agency mainly focus on one side of the divide, which is national security, and their immense capabilities in collecting intelligence leave the privacy of the ordinary individuals at their mercy. Enforcement discrepancies in the EU Laws and Directives also seem to be advantageous to the government agency. Since the government controls the entire system, they end up deciding the exceptions for the intelligence agencies. The other concern is the immense power available to these agencies, which seem to be unregulated. Lack of regulation enables them to apply criminal-level intelligence measures on ordinary foreigners who pose no threats to national security. For instance, registered lawyers and journalists in foreign countries are subjected to stringent surveillance, yet they

should be exempt under the law. Their data can also be analyzed, but the scrutiny deployed should not be as massive as whatever has been reported through the complaints. Tapping data from the telecommunications and internet service companies is extensive abuse of power by the intelligence agency because it has scaled beyond the limits of its activities. Their limits are within the public space but extending to private communications and sharing the same information with foreign intelligence agencies violates fundamental privacy rights[1].

[1] Bakir V. (2021) Freedom or Security? Mass Surveillance of Citizens. In: Ward S.J. (eds) Handbook of Global Media Ethics. Springer, Cham. https://doi.org/10.1007/978-3-319-32103-5_47

CONCLUSION AND RECOMMENDATIONS

Digital transformation and increasing online activity have escalated privacy-related concerns in the context of state security surveillance. It has provided numerous avenues for government intelligence agencies to gather and analyze large amounts of personal information at the expense of their privacy. These activities result in numerous challenges in balancing digital data protection and state security. Massive secret surveillance programs are deployed in all situations without any exceptions to the scenarios posing greater threats to national security. Since criminal investigation level intelligence acquisition interventions are used, ordinary individuals suffer massive privacy infringements. The extents of information-seeking ventures by government agencies, including tapping information from telecommunications and internet companies, escalate the threat to personal privacy.

These privacy infringements mainly arise from the immense powers availed to the national intelligence agencies. The power is unregulated because the institutions operate under the government, which is the same body required to enforce the privacy laws and directives. This challenge exposes the extensive legal loopholes exploited in the operation of the national intelligence agency, which affects the balancing digital privacy and state security.

Therefore, Suitable independent oversight bodies should be formulated to regulate the collection and management of personal information obtained by the Federal Intelligence Service. The oversight bodies will ensure that the information collected is within lawful limits provided by the legislative frameworks and its use does not contravene the fundamental right to privacy. They will also provide avenues for the citizens to raise issues concerning incidences of privacy

infringements by government intelligence agencies and possibly institute litigation on behalf of the citizens.

The Federal Intelligence Service should be made accountable to the EU Courts and other regulatory agencies tasked with safeguarding digital privacy rights. Measures to improve accountability should include full disclosures of the surveillance systems and data collection and analysis techniques used by the relevant regulatory organizations upon request. This will ensure that the Federal Intelligence Service does not use uncouth means of obtaining intelligence by targeting parties of interest that do not pose any security threats. Accountability will also help ensure that the intelligence agency avoids intentional infringements of the fundamental right to privacy which has been the case due to lack of regulation.

The EU legislative structures should develop legal frameworks restricting the forms of technology used for surveillance. It will combine with adequate oversight and accountability to ensure that the Federal Intelligence Service does not violate the privacy of innocent individuals in the course of surveillance for criminal convictions. The legal frameworks should also provide adequate provisions to allow certain notable individuals from the surveillance process. These include foreign journalists and legal practitioners whose credibility and the licensing institutions can regulate codes of conduct.

Non-state actors, including private organizations, should be sensitized on the need to promote the right to privacy. It will guide them against releasing personal information to government agencies without permission or court orders. This will apply in telecommunications and internet companies

colluding with the intelligence agencies to infringe individuals' privacy. Punitive measures should also be deployed against private actors disseminating personal information without consent to minimize cases of pilferage and abuse of power. It will also curtail the secret initiatives of the secret service, whose major aim to collect unnecessary data and infringing the rights of innocent individuals in the name of protecting national security.

Creating public awareness on the issue of privacy on the internet will encourage users to develop changes that will result in privacy protection from the users' side. Implementing privacy protection from the users' side is a suitable solution to the infringements on personal privacy by the national intelligence agencies because it will prevent them from accessing the large amounts of personal data using their analytic tools. This initiative will also include increased media

coverage on the same issue and technical education. Educating the masses will equip them with useful knowledge on technological surveillance and result in the development of suitable mechanisms of protecting their privacy. There is also need for joint efforts from the society as well as the technicians involved technology industry to cater to the technical aspects of promoting a safer and secure cyberspace.

References

Bignami, F. (2015) 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens'. Study for the LIBE Committee, European Parliament, PE 519.215, pp. 1–40.< https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2433&context=faculty_publications>

Bakir V. (2021) Freedom or Security? Mass Surveillance of Citizens. In: Ward S.J. (eds) Handbook of Global Media Ethics. Springer, Cham. https://doi.org/10.1007/978-3-319-32103-5_47

Boyd, Danah, and Kate Crawford. (2012). "CRITICAL QUESTIONS FOR BIG DATA". *Information, Communication & Society* 15 (5): 662-679. https://doi.org/10.1080/1369118X.2012.678878

Brkan, Maja. 2016. "The Unstoppable Expansion of The EU Fundamental Right to Data Protection". *Maastricht Journal of European And Comparative Law* 23 (5): 812-841. doi:10.1177/1023263x1602300505.BVerfG, judgment of the First Senate of 19 May, 2020 - 1 BvR 2835/17 -, Rn. 1-332, http://www.bverfg.de/e/rs20200519_1bvr283517.html

Changchit, Chuleeporn. 2008. "Data Protection and Privacy Issue". *Journal Of Information Privacy And Security* 4 (3): 1-2.https://doi.org/10.1080/2333696X.2008.10855842

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C-594/12) EU:C:2014:238 (08 April 2014). https://uk.practicallaw.thomsonreuters.com/D-025-6285?transitionType=Default&contextData=(sc.Default)

Segerstedt-Wiberg and ors v Sweden, Merits and just satisfaction, App no 62332/00, ECHR 2006-VII, (2007) 44 EHRR 2, IHRL 3288 (ECHR

2006), 6 June 2006, European Court of Human Rights [ECHR]. https://opil.ouplaw.com/view/10.1093/law:ihrl/3288echr06.case.1/law-ihrl-3288echr06

David Banisar& Simon Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1 (1999). < https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1174&context=jitpl>

Dimitrova, Anna, and Maja Brkan. 2017. "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts Before and After the NSA Affair". *JCMS: Journal of Common Market Studies* 56 (4): 751-767. https://onlinelibrary.wiley.com/journal/14685965

Dove, Edward S. 2018. "The EU General Data Protection Regulation: Implications for International Scientific Research in The Digital Era". *Journal of Law, Medicine & Ethics* 46 (4): 1013-1030. https://doi.org/10.1177%2F1073110518822003

Doyle, Ch. (2001) 'Terrorism: Section by Section Analysis of the USA Patriot Act'. CRS Report for Congress, 10 December.< https://fas.org/irp/crs/RL31377.pdf>

Eddy M, 'Right To Privacy Extends To Foreign Internet Users, German Court Rules (Published 2020)' (Nytimes.com, 2020) https://www.nytimes.com/2020/05/19/world/europe/germany-privacy.html>

European Commission, 'Directive 95/46/EC Of The European Parliament And Of The Council Of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data' (European Commission 1995) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3AHTML>

European Court of Human Rights, 'European Convention On Human Rights' (1950) https://www.echr.coe.int/documents/convention_eng.pdf>

Granger, M. - P., and K. Irion. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection." European Law Review 39, no. 4 (2014): 835-850. < http://publications.ceu.edu/sites/default/files/publications/2014el-rev6grangeroffprint.pdf>

Fainmesser, Itay Perah, Andrea Galeotti, and Ruslan Momot. 2019. "Digital Privacy". *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.3459274

Hagen, Janne, and Olav Lysne. "Protecting the Digitized Society—the Challenge of Balancing Surveillance and Privacy." The Cyber Defense Review 1, no. 1 (2016): 75-90. http://www.jstor.org/stable/26267300.

Horsley, T. (2015) '"The Court Hereby Rules ..." – Legal Developments in EU Fundamental Rights Protection'. JCMS, Vol. 53, Annual Review, pp. 108–27. < https://econpapers.repec.org/article/blajcmkts/v_3a53_3ay_3a2015_3ai_3a_3ap_3a108-127.htm>

Jing, Ran. "Striking the Balance between Privacy and Governance in the Age of Technology." SPICE: Student Perspectives on Institutions, Choices and Ethics 11, no. 1 (2016): 2.< https://repository.upenn.edu/cgi/viewcontent.cgi?article=1054&context=spice>

Juraj, Sajfert and Quintel, Teresa, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities (1 December, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3285873

Klass and others v Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978

Klein, Sebastian. “Federal Administrative Court Prohibits Storage and Use of Telecommunications Metadata by the Federal Intelligence Service.” Eur. Data Prot. L. Rev. 4 (2018): 110. < https://doi.org/10.21552/edpl/2018/1/16>

Luca Pietro, Vanoni. “Balancing privacy and national security in the global digital era: A comparative perspective of EU and US constitutional systems” [2018] ELECD 894; in Violini, Lorenza; Baraggia, Antonia (eds), “The Fragmented Landscape of Fundamental Rights Protection in Europe” (Edward Elgar Publishing, 2018) 114.< https://doi.org/10.4337/9781786436054>

Malgieri, Gianclaudio and De Hert, Paul, European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges (October 30, 2016). D. Gray and S. Henderson (eds.), Cambridge Handbook of Surveillance Law, 2017, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2948270

Olga Gurkova and Jovan Ananiev, ‘National Security v. Protection of Personal Data in the EU’ (2012) 3 Iustinianus Primus L Rev 1. <

https://eprints.ugd.edu.mk/6882/1/NATIONAL%20SECURITY%20VS%20PROTECTION%20ON%20PERSONAL%20DATA%20ANANIEV%20I%20OLGA.pdf>

Out-Law.com, Profiling rules should not apply unless individuals’ rights are ‘significantly affected’, says privacy body, 23.05.2013, http://www.out-law.com/articles/2013/may/profilingrules-should-not-apply-unless-individuals-rights-aresignificantly-affected-says-privacy-body/

Power D, Heavin C, and O'Connor Y, 'Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide' [2021] Journal of Business Analytics. < https://doi.org/10.1080/2573234X.2021.1920856>

Raghupathi W, and Raghupathi V, 'Big Data Analytics In Healthcare: Promise And Potential' (2014) 2 Health Information Science and Systems.< https://doi.org/10.1186/2047-2501-2-3>

Ran, Jing. "Striking the Balance between Privacy and Governance in the Age of Technology," (2016) 11:1 Penn Journal of Philosophy, Politics & Economics. Available at: https://repository.upenn.edu/spice/vol11/iss1/2

Richards, N. (2013). The dangers of surveillance. Harvard Law Review. 20 May, 126 Harv. L. Rev. 1934, https://harvardlawreview.org/2013/05/the-dangers-ofsurveillance

Segerstedt-Wiberg and ors v Sweden, Merits and just satisfaction, App no 62332/00, ECHR 2006-VII, (2007) 44 EHRR 2, IHRL 3288 (ECHR 2006), 6 June 2006, European Court of Human Rights [ECHR]

Rojszczak, M. (2021). Extraterritorial Bulk Surveillance after the German BND Act Judgment. European Constitutional Law Review, 17(1), 53-77, See at: https://www.cambridge.org/core/journals/european-constitutional-law-review/article/extraterritorial-bulk-surveillance-after-the-german-bnd-act-judgment/D6B51E73049E18D9EEB563F36CEB679E

United Nations, 'Universal Declaration Of Human Rights' (United Nations 2015) https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf>

Violini L, and Baraggia A, The Fragmented Landscape of Fundamental Rights Protection in Europe (Edward Elgar Publishing 2018). < https://air.unimi.it/retrieve/handle/2434/620622/1157426/Violini-Fragmented_landscape%2010%2009%2018.pdf>

Weber R, 'The Digital Future – A Challenge for Privacy?' (2015) 31 Computer Law & Security Review. < https://doi.org/10.1016/j.clsr.2015.01.003>

Xhafaj J, and Frakulli A, 'The Impact of Public Interest in The Information Privacy: Analyze of The ECtHR Decisions' (2017) 6 International Journal of Business & Technology. < https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=1076&context=ijbte>

Y. Poullet, "EU Data Protection Policy. The Directive 95/46/EC: Ten Years After," Computer Law & Security Review 22, no. 3 (2006): 206-217, at 206. < https://doi.org/10.1016/J.CLSR.2006.03.004>

Zalnieriute M, 'A Struggle for Competence: National Security, Surveillance and The Scope of EU Law at The Court of Justice of European Union' [2021] The Modern Law Review. https://doi.org/10.1111/1468-2230.12652

Zuboff S, 'Big Other: Surveillance Capitalism And The Prospects Of An Information Civilization' (2015) 30 Journal of Information Technology.< https://doi.org/10.1057/jit.2015.5