



LAW COURSEWORK SAMPLE



WRITING
METIER

TOPIC



THE IMPACT OF SOCIAL MEDIA ON PRIVACY AND DATA
PROTECTION LAWS

ORDER CUSTOM
LAW COURSEWORK
AT OUR WEBSITE:



WRITINGMETIER.COM

The Impact of Social Media on Privacy and Data Protection Laws

[Author]

[Institution]

Introduction

The rise of social media has increased the risk to our data and privacy in several ways. Social media platforms collect and store a vast amount of personal information from their users, including their name, age, location, interests, and online behavior. This information can be used to create detailed profiles of individuals and can be sold to third-party advertisers or used for targeted advertising. One of the most significant risks to data and privacy is data breaches. Social media platforms can be vulnerable to cyber-attacks and hacks, which can result in the loss or theft of personal data. In some cases, this data can be sold on the dark web or used for identity theft and fraud.

Another risk is the use of personal data for political campaigns or propaganda. This can be done by analyzing an individual's online behavior and interests to determine their political views and then targeting them with political content that reinforces those views. Social media platforms can also be used to conduct surveillance on individuals, both by government agencies and private companies. Hence, privacy and data protection laws around the world have come into action to protect individuals and their privacy from such risks. In this paper, we will discuss the privacy and data protection laws in Germany and the role they play to protect individuals' from risks of cyber-attacks, data theft, fraud, etc (Singh & Hill, 2003).

Overview

Currently, there are three pieces of legislation that regulate the data protection and privacy laws in Germany. The first is the General Data Protection Regulation (GDPR) that was adopted by the European Union (EU) in 2018 applicable for all EU countries. The GDPR

replaced the Data Protection Directive of 1995 with more strict requirements and stringent regulations for data controllers. It also now included the requirement of consent for data collection and other enforcement requirements (Von dem Bussche, & Stamm, 2013).

The German Federal Data Protection Act or *Bundesdatenschutzgesetz* (BDSG) was first adopted in 1978. Since then there have been many changes, however, the new BDSG was enforced in 2018 and is currently being followed. The law was redesigned to bring the German federal law on par with the EU GDPR. The new BDSG ensures protection of all types of personal data, whether processed by advanced technology or traditional methods.

The third is the Telecommunications-Telemedia-Data Protection Act or *Telekommunikation Telemedien Datenschutzgesetz* (TTDSG), which is not fully in effect yet. It was introduced in 2021 and is set to be enforced in 2023. This law is sector-specific and provides data protection of personal data for all electronic communications such as websites, emails, phone, or apps.

Analysis

Even though the history of German data protection laws goes back to the 1970s when they were first introduced. The landscape of regulations has changed vastly ever since. The increase in the use of technology and internet in the 1990s led to a change in laws focusing more on the principle that individuals had the right to decide what personal information they want to be published. The 2000s came with a greater need for change in data protection and privacy laws now that electronic media such as emails, websites and other software programs were being used. The rise of social media in 2010s with new apps such as Twitter, Facebook, WhatsApp and

more recent ones such as Instagram and Tiktok, the risk of data leaks and privacy breaches became more concerning.

Social media platforms today are used for a much broader purpose. Some marketing companies only base their strategies on the data they acquire from social media information. Since users enter vast amounts of personal data on social media platforms, from personal information to pictures, location, interests, etc, their privacy becomes more vulnerable. Internet identity and online behaviour are major concerns for advertisers and marketing team for targeted advertising, which has proved quite successful in recent years. But the question is, how ethical is it?

Social media has thus, greatly affected data protection and privacy laws and how they are regulated. The German data protection and privacy laws affect businesses, their marketing, and other agencies who tend to use this information for their benefit. There are some key frameworks that are covered under these laws to ensure maximum security and protection of data. The first one is the location and transfer of data, which means that every business must ensure that data originating from Germany stays within its international borders. According to law, any sort of transfer of personal user data across borders is unlawful activity and is regulated under articles 44-50 of the GDPR. This law ensures that sensitive private data is not transferred outside the country without consent (Laybats & Davies, 2018).

The second framework covered under these laws is privacy provisions and consent. Data controllers and processors who receive sensitive personal data are only allowed to use this personal data according to the regulations set in article 6 of GDPR. Under these regulations, the

collectors must seek consent of the users before using their data. The consent can be gained automatically or could be a preinformed message to the user when they enter their data on a certain online platform (Voigt & Bussche2017). However, it is essential to note that the user can withdraw their consent at any given time. Data processors must also inform the users the purpose to which their data will be used or processed.

The third framework is data protection enforcements and fines, under which huge penalties and fines are imposed on businesses or agencies that violate the regulations and engage in data privacy breaches. The more serious the violation, the bigger the penalties imposed by data protection agencies (DPAs). For example, H&M, the fashion chain giant, was fined for €35 million for unlawful surveillance of employees at one of their stores. DPAs give breachers 72 hours to notify of the breaches or they can be fined for up to €10 million. With the compliance of regulations covering these three essential frameworks, Germany is able to reduce the risk of online data and privacy breaches to a great extent.

Comparison

Similar to Germany, all other EU countries are regulated under the GDPR, which is considered superior to federal laws. The key regulations and directives are same for all EU countries, in addition to the commissions that are required to be set up under the GDPR. Every country has a different Data Protection Commission (DPC) that is a national independent authority formed under the GDPR to give it further effect. Some countries have their federal laws as well relating to data privacy and social media regulation. In Ireland, the main regulation that is followed is GDPR along with the Data Protection Act 2018, under which the DPC ensures

application of GDPR regulations. The DPC actively handles complaints and breaches, however, the enforcement is not as strict as German laws. Ireland has faced several data privacy and security breaches issues in the last few years. However, the DPC is trying their best to deal with the breaches as they recently fined Meta Platforms Inc., for \$400 million for their data handling practices and advertising that is in breach of GDPR (Miglicco, 2018).

Another example to be considered is of Switzerland where data privacy is taken more seriously. While they have adapted the EU GDPR, their new and revised Federal Data Protection Act (revFADP) is introduced to strengthen the rights of consumers and reduce the risk of data privacy breaches. The revFADP is a revised law that brings together the provisions of the Ordinance to the Federal Data Protection Act and Ordinance on Data Protection Certification. The regulations regarding privacy of data acquired through electronic and digital sources will be stricter and will require businesses to alter their policies of data privacy (Miglicco, 2018).

France, on the other hand, follows the GDPR and in addition to that, they have the "Loi Informatique et Libertés" (Data Protection Act). The Data Protection Act was first introduced in 1978 and has been updated several times since then to reflect changes in technology and the evolving data privacy landscape impacted by the increased use of social media. The French Data Protection Authority (CNIL) is responsible for enforcing data privacy laws in France. It has the power to investigate and sanction organizations that violate data privacy regulations, including imposing fines and other penalties.

In the Netherlands, in addition to the GDPR, the General Data Protection Regulation also called "Algemene Verordening Gegevensbescherming" (AVG) is implemented. The AVG was

introduced in 2018 and is aligned with the GDPR. The AVG sets out specific requirements for processing personal data, such as the appointment of a Data Protection Officer (DPO) for certain organizations, and the mandatory notification of data breaches to the Dutch Data Protection Authority (DPA) (Tankard, 2016).

Critical Analysis

Lawmakers face a number of challenges when balancing the rights of individuals to privacy and the interests of businesses to collect and use personal data since it is a complex legal and ethical area. Businesses collect and use personal data for targeted advertising to learn online buying behavior and interests. This has been a very successful tool in online advertising and social media marketing leading to high sales for business products. However, using personal information collected through online mediums is a controversial issue and there is no right answer on whether businesses should do so or not (Tankard, 2016).

On one hand, targeted advertising can be useful for businesses, as it allows them to tailor their marketing messages to specific audiences. On the other hand, many individuals are uncomfortable with the idea of their personal information being used for advertising purposes, as it can feel intrusive and raise concerns about privacy. From a legal perspective, the use of personal information for targeted advertising is generally allowed under GDPR. However, it is conditional that businesses must obtain explicit consent from individuals before using their personal information for advertising purposes, and individuals have the right to opt-out of targeted advertising whenever they want (Raul, 2020).

The challenges for lawmakers, thus, when drafting policies and regulating laws that balance both areas are essential to consider. The biggest challenge is the complexity of data privacy laws and its implementation. The regulations under GDPR are complex and can be difficult to navigate. Furthermore, the rapidly evolving technology makes it challenging for lawmakers to keep up with the latest trends and to ensure that data privacy laws remain relevant and effective. As new technologies emerge, lawmakers must work to update regulations and address new challenges related to data privacy (Kročil & Pospíšil, 2020).

International cooperation can also become challenging for lawmakers as data privacy is a global issue. It can be challenging for lawmakers to ensure that regulations are consistent across different jurisdictions. In order to protect individuals' privacy rights, lawmakers must work together across borders to establish common standards and regulations. Enforcement is another challenge as lawmakers need the resources and tools to investigate and sanction organizations that violate data privacy regulations (Tankard, 2016).

Evaluation of Effectiveness

The current privacy and data protection laws in Germany have had a significantly positive impact on regulating social media. Some of the biggest players in social media are WhatsApp, Facebook, YouTube, Instagram, and TikTok. As there are more than 3.4 billion social media users globally, which is almost half of the entire world population, it is an effective platform for marketers to advertise their products. Not just companies, but financial fraud, identity theft, and other forms of cybercrimes are also common, which can greatly impact the privacy of users. It was reported that about \$200 billion was spent on social media advertising in

2022. This shows that social media advertising is a major marketing tool for businesses and thus it needs regulation (Matei, Rebillard & Rochelandet, 2021).

Under the GDPR, the personal use of social media is not covered. It covers the professional capacity in which social media data is used and thus, according to the law, the collection, processing, storing or sharing of data by third-parties without consent is strictly not allowed. The GDPR is applicable to all private and government-owned companies that have the capacity to hold personal data of users. The GDPR protects users that are residents and citizens of any of the EU countries. The law has been able to regulate social media as it makes it obligatory for social media companies to ask for consent before collecting personal data. Explicit content is required on how the data will be collected, processed and used, and whether it will be transferred to any third party or not (Voigt & Bussche, 2017).

Any company or business that wants to use social media marketing must take consent from users as strictly required by the GDPR. Privacy notices are also explicitly given to users when they are using a certain platform. The GDPR regulations require consent and once consent is taken, there is less direct effect on social media marketing. Advertising and marketing is not an issue under GDPR as it doesn't require collection or use of data. Posting content and engaging with users is allowed and not a risk to user privacy. GDPR also doesn't have laws regarding using anonymized data, which includes tracking behavior, engagement, or following pages and trends, as this also doesn't include personal data (Tankard, 2016).

The areas of law that have impacted social media marketers are when they try to extract personal information from social media users and use it for other purposes of business. The

GDPR includes strict laws against remarketing advertisements or retargeting cookies that enables businesses to create ads that follow their website visitors to their social media platforms. The GDPR and other German federal laws also compel social media platforms to give an explicit privacy notice and suitable disclaimer with no pre-ticked boxes. The laws also restrict analytics to track social media user behavior, which restricts data collection from personal chats and browsing. With the strict laws and its implementation in Germany, it can be said that the laws are quite effective in regulating the use of social media (Laybats & Davies, 2018).

Discussion

While the GDPR and other German federal laws are doing a good job in regulating social media, certain reforms can be implemented to better regulate social media and protect the privacy of individuals. Some of the reforms include strengthening data protection laws for social media companies to protect user privacy on personal and professional capacities. Stricter fines and penalties can be imposed for violation. Increased transparency by social media companies about their data collection and processing policies can be done. Users should be given more control over their personal data and how it can be used by social media companies. Users should be given a transparent method to opt-out of such data collection practices whenever they feel like. Users should have the ability to delete their data (Witzleb, Lindsay & Paterson, 2014). Education and awareness is another possible reform to help users better understand their rights and how to protect their privacy on social media platforms. They should also know how to reach out to the relevant departments and make complaints.

Conclusion

Overall, the rise of social media has had a significant impact on privacy and data protection laws around the world, especially in Germany. The EU and German federal laws have been able to provide users with the protection of their data and personal information by regulaitng social media and imposing strict penalties.

References

Matei S., Rebillard F. & Rochelandet F. (2021). *Digital and Social Media Regulation: A Comparative Perspective of the US and Europe*. Springer International Publishing

Voigt P. & Bussche A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing

Raul A. (2020). *The Privacy, Data Protection and Cybersecurity Law Review*. Law Business Research Limited

Witzleb N., Lindsay D., & Paterson M. (2014). *Emerging Challenges in Privacy Law: Comparative Perspectives*. Cambridge University Press

Von dem Bussche A., & Stamm M. (2013). *Data protection in Germany*. Beck

Singh T., & Hill M. (2003). Consumer privacy and the Internet in Europe: a view from Germany. *Journal of consumer marketing*, 20(7), 634-651

Miglicco G. (2018). GDPR is here and it is time to get serious. *Computer Fraud & Security*, 2018(9), 9-12

Kročil O., & Pospíšil R. (2020). The influence of GDPR on activities of social enterprises. *Mobile Networks and Applications*, 25, 860-867

Laybats C., & Davies J. (2018). GDPR: Implementing the regulations. *Business Information Review*, 35(2), 81-83

Tankard C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8

ORDER CUSTOM
LAW COURSEWORK
AT OUR WEBSITE:



WRITINGMETIER.COM