Type of the Article/ Makale Türü: Review Article/ Derleme Makalesi

BALANCING ECONOMIC GROWTH AND PRIVACY: THE ROLE OF USER DATA IN TARGETED ADVERTISING

Oday Alkahlout[1]
Sara Bader[2]

Abstract

This study sheds light on the importance of internet users' data as a valuable resource targeted by targeted advertisers. These data are the fuel that ignites the digital economy engine. However, the use of this data raises questions about the balance between digital economy and user privacy. Targeted advertising studies reveal the potential violations of users' privacy, necessitating the presence of legislation to protect user data and preserve their rights. Additionally, balancing economic development and maintaining privacy in a connected technological world is required.

The researchers also concluded that social media platforms, as private commercial entities, provide free services by using and selling user data to third parties for commercial purposes. These companies need to comply with legislation and laws that protect user privacy and ensure their right to digital forgetting. The study relies on an inductive methodology, reviewing and analyzing previously available and published sources on a specific topic, providing a comprehensive overview of the concept of targeted advertising and its use of user data. Based on this analysis, the focus is on the impact of these practices on user privacy and the need for a sustainable balance between economic development and privacy rights in the connected digital world.

Keywords: Targeted advertisements, Privacy, Personal data, Digital transformation

1. Introduction

In an era where technological advancement is accelerating, targeted advertising has become indispensable in the world of digital marketing. Directing advertisements towards a precisely targeted audience is not only essential for the success of advertising campaigns but also represents a revolutionary shift in shaping consumer behavior. These advertisements rely on intelligent analysis of personal data, enabling them to deliver promotional messages that align with the interests and needs of everyone.

The rapid advancement of technology provides marketers with the ability to enhance their strategies and communicate with customers on a personal level. The era of generic and non-targeted advertisements is gradually evolving into a more complex and precise approach, considering each customer as a unique entity with distinct preferences and behaviors.

[1] Sakarya Üniversitesi, e-posta: oday46kh@gmail.com, ORCİD: 0000-0002-3581-3592
[2] Sakarya Üniversitesi, e-posta: sara.bader@ogr.sakarya.edu.tr, ORCİD: 0009-0008-6688-9400

These radical transformations are fueled by meticulous analysis of personal data, allowing advertisers to discern patterns, preferences, and trends with utmost precision. As a result, the advertising landscape is evolving from mere information dissemination to an interactive and personalized experience that resonates with each consumer.

Despite the achievements of targeted advertising in reaching the appropriate audience, a gap has emerged concurrently with this advancement, namely the concern of users about the violation of their privacy. Commercial companies that own most social media platforms possess databases that can be used to achieve profitable goals by selling this information to third parties, while offering all services for free to users. This may pose a fundamental problem for users in protecting the privacy of their data and complying with the regulations imposed to safeguard this right. Hence, it is imperative to shed light on the significance of studying the nature of targeted advertising, where personal data serves as fuel for its operation, and the consequent violation of user privacy.

Research Significance

The importance of this study is highlighted by the concurrent evolution and increasing role of social media platforms in our lives, coupled with the rapid and notable advancement of smart devices such as phones and computers. Giant companies releasing numerous free applications have often disregarded the sensitivity of data collection and usage for other purposes that may harm users and threaten their privacy. Some have overlooked the existence of a legal framework serving the user's interest in protecting their privacy from infringement.

Moreover, the importance of this research stems from the right to digital oblivion of the user, which entails the respect by companies providing social media services for the user's freedom not to continuously retain data if the user decides not to use these applications again. Based on this right, there must be a balance between this right and the company's right to maintain its customers in case the relationship between the service provider and the data subject is severed.

Methodology:

In this, we adopted the review methodology, which is a research approach relying on the review and analysis of previously available and published sources on a specific topic. This methodology has assisted us in understanding the nature of personal data, its types, targeted advertising, its nature, and forms. It also guided us in identifying real-life examples of user privacy violations on some well-known platforms. Furthermore, it helped us grasp the concept of privacy, the manifestations of its violations, and how to protect user privacy by considering previous experiments and various studies.

1. Literature reviews

We can categorize previous studies into more than one axis:

The First Axis: Studies related to the awareness of social media users about their privacy rights:

Most of the field studies focus on exploring the awareness of social media users regarding the risks that threaten their privacy on these platforms and their response to using the available privacy settings. A study by Sophie (2021) found that despite users' awareness of privacy risks related to their information on social media, they avoid using the privacy settings available on those sites. This was confirmed by the results of another study (Ayesha Shahid & Umair Abdulla, 2021), indicating that users allowed public access to their personal data without altering the initial privacy settings on their accounts. Additionally, a study by Hyang-Sook Kim (2016) revealed that a group of students does not fundamentally care about privacy and has no issue sharing their personal information and geographical location on Facebook when using mobile phones. Results from Sylvia Kowalewski and others (2015) confirmed that German users feel they do not have the right to protect their personal data on these sites, and the responsibility for data protection lies with the site administrators.

Moreover, a study by Abdul Amir Faisal and Esraa Hashem (2017) indicated that most users in Iraq have a clear gap between their general understanding of the concept and importance of privacy, especially in the absence of legal awareness, despite the law guaranteeing the right to privacy. This is noteworthy considering that most of them hold postgraduate qualifications. Another study by Tawfiq Barhoom and others (2014) observed the impact of security and technical awareness on the privacy protection of social media users, specifically students in middle and high school stages in Gaza. The study demonstrated significant positive results in improving the participants' awareness of privacy and their interest in it on these sites due to awareness-raising efforts.

Regarding factors affecting the interest of social media users in protecting their privacy, there is a significant impact of gender on users' interest in protecting their personal data. The results of a study by Jeffrey Child and Shawn Starcher (2016) highlighted clear and statistically significant differences between females and males, Facebook users, regarding their interest in protecting their data privacy on the site, with females showing higher interest.

The Second Axis: Studies Related to the Legal Framework Regulating the Right to Privacy:

The topic of the right to privacy and its protection has garnered the attention of numerous researchers in digital environments. A study by Sagge Sethu & Devika Ramachandran (2021) (64) analyzed the laws of several Arab countries, such as Bahrain, Qatar, and the UAE, to confirm the extent of their protection of the right to privacy. The study found that these countries have updated some texts and enacted new laws to protect the privacy of social media users and their data. The study emphasized users' right to access or delete their data and protection from violations.

Additionally, Eugenia Georgiades (2021) (65) affirmed that Australian law guarantees the protection of personal images on social media. It confirmed the right to digital forgetfulness, allowing users to delete their data whenever they wish. Another study by Muhammad Al-Maadowi (2018) (66) highlighted the obligations of the French Information and Liberties Law for individuals processing electronic data. It emphasized the duty to maintain the confidentiality of this data, requiring prior user consent before data usage, referred to as "opt-in." The study concluded that contractual law should be applied, and data processors must commit to strict confidentiality. Users are entitled to file a lawsuit if their privacy is violated on social media.

A study by Mohammed Al-Qahtani (2015) (67) focused on revealing the extent of Saudi Arabian law's protection of personal privacy on social media. The study found that Saudi law has issued several laws, including provisions and penalties, to deter violators of privacy on social media and any information system. The study also identified various forms of information and personal data violations, emphasizing the need for strong legal protections.

According to a report by the United Nations Human Rights Commission (2015) (68), international human rights law contains clear provisions to enhance and protect the right to privacy. However, various practices in many countries reveal a lack of means to safeguard privacy, especially regarding legislation and laws. Ineffective oversight and the absence of robust procedural guarantees played a role in the lack of accountability for those intervening arbitrarily or unlawfully in the right to privacy.

Sarah Al-Sharif's study (2014) (69) focused on studying and analyzing the protective capacity of Egyptian law for the privacy of digital data. The study concluded that Egyptian law lacks any provisions for the protection of users' digital privacy online, leading to various problems resulting in violations of users' digital privacy, all under the absence of a legal legislative framework protecting the user.

The Third Axis: Studies Related to the Technical Aspects of Privacy Protection on Social Networks.

Numerous studies have focused on the technical aspects of privacy settings on social media platforms, revealing their impact on users' utilization and understanding. Some researchers have aimed to innovate new technologies to empower users in protecting their privacy. One prominent technique is content encryption, which obscures the view of service providers and shields users from untrusted applications. A study by Ankit Jain & others (2021) emphasized the multiple risks of privacy violation and security breaches of user accounts on social media platforms, including identity theft, fake accounts, account hacking, and stealing user data through malicious links, known as phishing.

Additionally, a study by Ali Altable & Faris Kateb (2021) introduced a technological program designed to safeguard the privacy of Facebook users. The researchers demonstrated its effectiveness through practical experimentation.

2. Targeted Advertisements

Research has shown that the concept of targeting significantly enhances consumer responses to advertisements (John et al., 2018). Targeted advertisements can be defined as the use of data input by internet users when registering on networks and social media platforms or collected through cookies to track user behavior. This information is then used to create a database of internet users and shared with advertising companies, allowing them to target specific individuals (Al-Ma'dawi, 2018, p. 1976).

This means that advertisements only target users genuinely interested in their content, as evidenced by their likes, clicks, and sharing activities. The provision of free communication services is often coupled with retaining personal information and allowing companies that own electronic platforms, such as WhatsApp and Facebook, to handle and use this data as they see fit. This poses a privacy concern for users, especially as their personal data, including names, addresses, and preferences, is sold to advertising companies for profit (Ibn Burghouth, 2021, p. 277).

2.1.Methods of Targeted Advertising

In the evolving world of digital marketing, targeted advertisements have become indispensable for advertisers seeking to maximize the effectiveness of their marketing campaigns. This method allows advertisers to direct their advertising messages toward specific segments of the audience, enhancing ad effectiveness and enabling better interaction with consumers. In this paragraph, we will review some popular methods of targeted advertising, which have become a fundamental pillar in modern marketing strategies (Ashraf Gaber, 2015, p.14).

Search Engine Advertising: This method enables advertisers to identify the most searched keywords by users of search engines. For example, choosing the keyword "laptop" allows the advertiser's ad to appear when this keyword is searched, either above or next to the search box directly. A prominent example of search engine advertising is Google AdWords. This method excels in reaching the targeted audience by selecting keywords for ad display and ensuring the ad reaches users expected to be interested in the presented content. Additionally, it allows advertisers to achieve localized and regional targeting by specifying a geographical scope for ad visibility, such as displaying the ad only to users in a specific city or within a certain distance from the advertiser's location. Lastly, this method is flexible, allowing advertisers to adjust ad content at any time in response to emerging developments.

Website Advertising: Advertising on websites is another type of targeted advertising where advertisers arrange with the website or forum owner to display their ads on the site's pages. This is typically done by paying a certain amount to the site owner for displaying ads to visitors. The main forms of website advertisements include:

Banner Ads: Placing a banner on the website, usually at the top or bottom, containing an image and text to attract visitors' attention.

Pop-up Ads: Ads appearing in a pop-up window above the original site page, containing images, text, or links to direct visitors to a specific page.

Text Ads: Textual links within the website's content, often short and attention-grabbing.

Video Ads: Short video clips displayed to visitors, usually played before starting the original video content or during intervals in longer videos.

Sponsored Content: Advertisers fund specific content on the website, including articles, reviews, or any other type of content. Choosing among these formats depends on the advertiser's strategy and the target audience.

Example of Targeted Advertisements via Facebook:

In general, all websites strive for the same goal, which is to increase financial resources. Therefore, they tend towards using personalized data marketing to achieve their business objectives. This source may constitute the most important financial resource for them.

These resources take several forms; income sources may include pay-per-click advertisements (PPC), sponsorship advertisements, gift shops, and virtual currencies ,Facebook credits (Habash, 2012)

Despite Facebook offering free registration, it fully relies on analyzing personal data collected during the login process and utilizes it for commercial and marketing purposes to maximize financial returns.

Types of Facebook Advertisements:

- **Social Ads:**

This innovative marketing strategy relies on analyzing user data on the Facebook platform to deliver advertising messages in an efficient and targeted manner. These ads collect specific personal information without revealing the identity of users, employing this data to analyze their interests and behaviors on the platform. Facebook's privacy policy is centered around protecting user data and not sharing it with third parties, yet it allows for intelligent analysis of this data to target ads effectively without compromising user privacy. Targeted consumers are identified based on specific criteria such as age, geographical location, and personal interests, with ads displayed to members whose profiles match these criteria. When users interact with the ad, they are directed to the advertiser's page for more information or to take the desired action. Through this strategy, advertisers can achieve their marketing objectives with greater efficiency and precision, contributing to the effectiveness of their advertising campaigns and achieving more positive results (Kadwani, 2022)

- **Beacon or Guided Advertisement:**

When a Facebook user purchases products from other websites or shares their opinions on forums, these activities are displayed on their friends' pages using the "Beacon" system. This system aims to encourage social interaction in online shopping processes, sharing users' commercial activities with their friends on Facebook as part of a social shopping experience (marie, 2008, p33) Achieving this requires partnership agreements between Facebook and other websites, enabling these sites to share users' commercial activities with their friends on the Facebook platform.

Email Advertising: Email advertising is considered an effective method in the field of digital marketing, allowing advertisers to send promotional messages directly to the targeted audience. This type of advertising is distinguished by precise targeting, as advertisers can select message recipients based on accurate criteria such as interests and demographics. It also enables customization of message content to align with each individual's interests, increasing the effectiveness of the advertising campaign. Another advantage of email advertising is its measurability, allowing advertisers to assess the success of the campaign through open and click-through rates, facilitating continuous evaluation and improvement. Email also allows recipients to interact directly with messages, either by clicking on links or taking immediate actions, enhancing interaction and response effectiveness. Additionally, email campaigns are cost-effective, making them a suitable option for many companies compared to other advertising methods. Advertisers must comply with email laws and privacy regulations to ensure the legal and ethical aspects of the campaign. Ultimately, email advertising contributes to building strong customer relationships and increasing conversion and sales opportunities.

3. Privacy:

Privacy is one of the fundamental human rights, where each individual possesses information and secrets placed within their own sphere. Whether the information is of a personal or professional nature, privacy holds a special significance due to its diverse characteristics and distinctive types. In the rapidly advancing technological era we live in, our personal information exists in a digital world controlled by massive databases and information banks. Digital privacy introduces challenges and threats in the realm of digitization, involving the collection, storage, and processing of personal data for individuals and users. Every individual, in order to benefit from various communication services or mobile applications, is often required to disclose some of their secrets and personal data.

Some view privacy as the freedom of an individual to disclose their secrets at a time they deem appropriate and to those they choose to reveal them to (Saleh, 2016, p.23). We will address the concept of digital privacy in this study.

Digital Privacy:

There are many definitions for digital privacy, but perhaps the most comprehensive is as follows: it describes the protection of personal data that is published and exchanged through digital media. Digital personal data includes email, bank account numbers, personal photos, and various other data shared during online interactions or on social media platforms (Belassel, Maqdour, 2021, p.6).

3.1. Risks of Privacy Violation:

In the era of modern technology, issues of online privacy have become a vital matter deserving attention and serious consideration. With the rapid advancements in the digital communication world, challenges facing user privacy are increasing, manifested in risks such as data leaks, cyber attacks, and digital tracking. Understanding these risks and working towards safeguarding user privacy is of utmost importance. In this context, we must delve deeper into exploring these risks, understanding how to enhance awareness of privacy rights, and developing legislation and technologies to reinforce the protection of personal information (Herweal & Hiba, 2018). Among these risks we mention them below:

Surveillance:

The rapid advancements in the information revolution have introduced new dimensions to the issue of online privacy. Technological developments have allowed for the creation and improvement of devices used for eavesdropping, wiretapping, and surveillance. Such devices pose a risk to privacy, as they can easily reveal individuals' secrets without their knowledge.

Online surveillance occurs through the interaction between the user and the server, typically via smartphones and internet-connected computers. This interaction poses a significant danger, as surveillance can be exploited to steal sensitive information related to the user's privacy. Websites engaged in surveillance can benefit from secret information. Additionally, chat rooms and email are susceptible to monitoring and tracking, threatening privacy and necessitating strong security measures and user awareness regarding the importance of protecting their personal data online.

For example, individuals might receive targeted advertisements based on their recent conversations. The process of surveillance is not only about tracking online activities but also involves sending deceptive messages through email, presenting themselves as advertisements for various websites. The goal is to access the user's sensitive information and monitor their behavior for consumer marketing purposes (Bouhlel, 2019, p.30).

Exposure to Targeted Advertisements:

Targeted advertising plays a crucial role in increasing sales. Users spend extended periods in the digital environment, and targeted advertisements are based on individual interests. This type of advertising relies on the data infrastructure and intermediary technologies within the digital space (Ullah et al., 2022, p.489). Major electronic companies and advertisers use applications on phones to promote their advertisements and target audiences. These applications have data analysis systems that track and monitor user behavior, and this data is sent to advertising agencies (Cheriet, 2017, p.422).

A survey conducted by the Pew Research Center in 2019 revealed that 72% of Americans expressed concern that everything they do online or through mobile phones is tracked by advertisers and technology companies (Brook et al., 2019, p.6).

Assault on Credit Cards:

Privacy in the realm of banking transactions is one of the most important secrets that individuals strive to keep confidential. It involves various information related to one's account number, personal details, and the amount of money transferred, among other things. Users aim to secure this data because it can be vulnerable to hacking through the exchange of information that hackers acquire, resulting in unauthorized access to user data (Wali, Baghdadi, 2021, p.171).

The technological advancement has influenced various aspects of individuals' daily lives and transactions, including their credit cards. With e-commerce facilitated by the internet, individuals find it easy to enter their personal information during online shopping or through social media sites. This ease of entering personal data during digital transactions makes personal balances easily accessible and susceptible to unauthorized intrusion (Ibn Bargouth, 2021, p.277).

3.2. The Right to Privacy in the Digital Transformation Era:

It is defined as using technology in processes that affect the organizational future in order to increase the quality of the products and services offered by organizations (Alkahlout, 7).

Internet websites in general, and social media platforms in particular, face numerous challenges. Recently, privacy has become a concern for many users, as their personal data has become easily accessible by these companies.

Given the importance of preserving user privacy, this section will address the most important rights of users on social media platforms covered by international legislation:

In religious texts and ancient laws, the right to privacy has been recognized, and this concept has evolved and been embodied in several forms and components. Since the nineteenth century, these rights have begun to attract attention in courts and international forums. In modern times, they have been officially adopted in many charters and international agreements such as the Universal Declaration of Human Rights (2), and the International Covenant on Civil and Political Rights, in addition to regional agreements such as the European Convention on Human Rights and the American Convention on Human Rights (3).

The concept of privacy has historically evolved to include three main stages. The first relates to the recognition of physical privacy, while the second involves protecting the values and intellectual aspects of the individual, known as mental privacy. The third relates to privacy as a right extending to protect individuals from interference and assaults in their lives in all its forms and stages.

In the current context, a new concept of privacy has emerged, related to the impact of technology on personal life, leading to the emergence of what is known as information privacy. This entails individuals' right to control their information and data in the face of challenges posed by the digital revolution. (4)

In general, it can be succinctly stated that the concept of data protection in advanced charters requires that personal data (Khadija, et al, 2018).

- Be obtained lawfully and fairly.
- Be used for the declared and specified original purpose and not disclosed to unauthorized parties.
- Be related to the intended purpose of collection and not exceed it, confined accordingly.
- Be accurate and subject to updating and correction processes.
- Be accessible with the right to be notified of processing or transfer activities, and the right to correction, modification, and even deletion.
- Be safeguarded and protected in accordance with appropriate information security standards and inclusive processing.
- Be destroyed when the purpose of its collection is exhausted.

4. Personal Data

The world is currently experiencing a massive surge in the amount of generated data, necessitating the development of effective means to manage and process this data. This is aimed at improving the accuracy of identifying customer requirements, thereby enhancing the quality of products and services, increasing productivity, and reducing losses across various business sectors. This unprecedented growth in data volume is attributed to the significant increase in the number of electronic devices, the spread of cloud computing, and the expansion of social media applications.

Personal data technologies represent a new generation of technological tools designed to extract economic value from vast and diverse amounts of data. Many institutions and various sectors invest in big data technologies to enable them to exploit the commercial value potential of this data. In the telecommunications sector, for example, Personal data technologies are used by integrating them with advanced analytics to analyze risks, customer behavior, and network performance, in addition to enhancing IT security and accelerating the evolution of business processes.

This investment in Personal data helps organizations make more accurate and strategic decisions, contributing to achieving competitive advantages and sustainable growth in different markets.

4.1. The Concept of Personal Data

Before delving into the definition of big data, it is essential to understand the concept of data. Data refers to the raw form of information before any sorting, organizing, or processing takes place, making it unusable in its initial form. Raw data can be divided into three types, as noted by Habash (2013):

- Structured Data: This is data that is organized into tables or databases in preparation for processing.
- Unstructured Data: This refers to data generated daily by individuals, such as text writings, images, videos, messages, and clicks on websites. It constitutes the majority of data.
- Semi-structured Data: This is a type of structured data, but it is not designed in tables or databases.

Big data is defined as a collection of extremely large and complex data sets that are difficult to process using a single database management tool or traditional data processing applications. The challenges associated with big data include duration, storage, search, sharing, transfer, analysis, and visualization (Vance, 2010). The Big Data Institute defines big data as any data set that is too large for traditional database tools to capture, store, manage, and analyze (McKinsey, 2011).

In 2012, Gartner updated the definition to describe big data as "high-volume, high-velocity, and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (Beyer, 2011). The International Organization for Standardization (ISO) defines personal data as "a set or sets of data that have unique characteristics (such as volume, velocity, variety, variability, and veracity) that cannot be efficiently processed using current and traditional technologies to extract value" (Douglas, 2012).

Ghoneim (2021) noted that personal data is named as such due to its large volume and high degree of variety, as well as its rapid generation and the need for swift processing.

From the previous definitions, we can conclude that personal data is generated through our extensive use of various electronic devices, internet tools and applications, and mobile phones. This involves numerous daily life activities such as making calls, sending messages or tweets, sharing various types of files, completing purchase transactions, and other diverse practices and activities.

These uses create an increasing amount of digital data, forming personal data, which is difficult to manage and analyze with traditional database management systems. Therefore, managing and analyzing personal data relies on multiple artificial intelligence algorithms with immense capabilities to derive new and innovative information that aids in decision-making or problem-solving.

4.2. The Importance of Personal Data

Personal data is highly significant for various business sectors as it helps them sustain and achieve a competitive advantage by attracting new customers and increasing their profits and services. Personal data provides a deeper understanding to infer some unclear patterns and practices, which is a crucial factor in understanding customer requirements and making effective decisions.

For instance, by using personal data analysis tools, Walmart improved its online product results by 10-15%, as reported by McKinsey in 2011. The report indicated that the healthcare sector in the United States could have saved more than $300 million annually from its healthcare budget, which is about two-thirds of the budget, if personal data analysis techniques were used effectively and efficiently, by reducing spending costs by 8%. According to a previous survey conducted by Gartner, 64% of companies and organizations invested in adopting new technologies to handle personal data in 2013. The benefits of personal data are not limited to businesses and commercial projects but extend to many other fields, including energy, education, healthcare, and large scientific projects (Prashad, 2011).

Personal data is considered a part of the new era of computing, helping to achieve added value through the scanning and processing of data. Over time, the data generated by users grows increasingly due to various reasons, including buyer data in all sectors and applications. With the rapid and advanced development in technologies and devices connected to the Internet (Internet of Things), it will contribute to the increase in the amount of generated data (Hadi et al, 2014).

Personal data is highly significant for various business sectors as it helps them sustain and achieve a competitive advantage by attracting new customers and increasing their profits and services. Personal data provides a deeper understanding to infer some unclear patterns and practices, which is a crucial factor in understanding customer requirements and making effective decisions.

For instance, by using personal data analysis tools, Walmart improved its online product results by 10-15%, as reported by McKinsey in 2011. The report indicated that the healthcare sector in the United States could have saved more than $300 million annually from its healthcare budget, which is about two-thirds of the budget, if personal data analysis techniques

were used effectively and efficiently, by reducing spending costs by 8%. According to a previous survey conducted by Gartner, 64% of companies and organizations invested in adopting new technologies to handle personal data in 2013. The benefits of personal data are not limited to businesses and commercial projects but extend to many other fields, including energy, education, healthcare, and large scientific projects (Prashad, 2011).

Personal data is considered a part of the new era of computing, helping to achieve added value through the scanning and processing of data. Over time, the data generated by users grows increasingly due to various reasons, including buyer data in all sectors and applications. With the rapid and advanced development in technologies and devices connected to the Internet (Internet of Things), it will contribute to the increase in the amount of generated data (Hadi et al, 2014).

4.3. Types of Data

Data comes in various types, and some of the most important are:

First Type: Small pieces of "dumb" data such as numbers or facts, which Alex Sandy Pentland described as "digital breadcrumbs." Examples include call detail records collected by mobile companies (Bouillet et al., 2012).

Second Type: Data exchanged through social media networks, such as video files, messages, documents, tweets, and other content from social media applications. This data is mostly unstructured, making it difficult to analyze.

Third Type: Big data collected remotely through digital sensors, such as smart devices installed in homes to record electricity consumption or satellite images capturing physical information like vegetation as an indicator of deforestation (Prashad, 2011).

Fourth Type: Additional data types considered part of big data, including price and purchase data, climate data, or other sources of digital information.

4.4. Practical Framework

In this framework, the researcher reviewed how the technology of personal data is applied in the telecommunications sector through the following axes:

Descriptive Axis: This axis involved describing and presenting the application of personal data technology on various websites and social media platforms. It focused on identifying the main reasons for using personal data technology for targeted advertising and included a case study of Vodafone's application of big data technology in New Zealand.

Analytical Axis: This axis involved analyzing and presenting the results using SWOT analysis. This included analyzing the internal environment (strengths and weaknesses) and the external environment (opportunities and threats).

Recommendations and Future Visions Axis: This axis provided recommendations and future visions based on the analysis.

4.5. Examples of Some Risks of Processing User Data for Advertising Purposes

The risks associated with processing personal data for advertising purposes vary, and some websites have played a significant and influential role in disseminating malicious software through the use of targeted advertisements as a primary means. In this research paper, we will present some of these models.

The first case: The targeted advertisement may be for hacking online banking accounts (YouTube case 2014).

In this case, the targeted ad infiltrates malicious programs into the user's device. The danger lies in its ability to operate automatically upon the appearance of the ad on the device, without the need to click on it to view it. These programs launch a virus specifically designed to hack online banking accounts, such as the "banking Trojan" virus, conducting unauthorized money transfer operations for the user. These programs primarily operate on unprotected versions of Internet Explorer. This actually occurred in February 2014 for one of the YouTube users, who specializes in information security. She discovered that a malicious program had infiltrated her device through a YouTube link, spying on her personal information simply by watching the video on the site, even without clicking on the ad. Undoubtedly, the danger of such programs is impossible for non-experts to detect. (Reference postponed)

The Second Case: Malicious Software Attacks Through Targeted Advertisements for Yahoo Users (Yahoo Case 2013-2014).

In the days leading up to the end of 2014, a group of internet hackers managed, through a targeted advertising network on the Yahoo website, to disseminate advertisements containing malicious programs that were difficult to detect. These ads automatically initiated without the need for user clicks and were triggered simply by users accessing Yahoo's ad pages. Users' browsers were redirected to the advertisers' servers, which then sent the malicious software to these browsers instead of displaying the advertised content.

The severity of this malware was such that it breached the security system of Yahoo, known for having one of the most robust security systems. If it weren't for the fact that the malware had infected a device belonging to a Yahoo team member, it would have been challenging to detect. This incident underscores the significant threat posed by such malicious programs to ordinary users who interact with targeted advertisements on regular websites that may lack the level of protection available on Yahoo.

The third case: The Cambridge Analytica case

In 2018, the Cambridge Analytica-Facebook data scandal exposed the unauthorized collection of personal data from millions of users through the Facebook platform without their explicit consent, utilizing the acquired data for political advertising campaigns. The controversy originated when a journalist reported on the illicit data collection in 2015. As events unfolded, the media revealed details, leading to public outrage and a significant decline in Facebook's stock value.

The gathered data included information about 87 million users, with Cambridge Analytica using this data to target political advertisements and influence the details of election campaigns. The scandal became a focal point for media attention, raising concerns about privacy rights and the ethics of utilizing personal data. This event is considered a "turning point" in public understanding of the negative impact of using data for political and advertising purposes, prompting calls for tighter regulations and the development of privacy protection policies.

In this context, Alexander Kogan, a data scientist at the University of Cambridge, developed an application called "This Is Your Digital Life" before presenting it to Cambridge Analytica. Many Facebook users agreed to complete the survey published by the company, claiming it was for academic purposes only. However, Facebook's design allowed this application to collect personal information from all individuals on the user's friend list or those with whom they interacted, without their knowledge. In this way, Cambridge Analytica succeeded in gathering data from millions of users on the Facebook platform without their awareness.

The fourth case: Equifax data breach FAQ:(2017)

In March 2017, personally identifying data of hundreds of millions of people was stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States.

As we'll see, the breach spawned a number of scandals and controversies: Equifax was criticized for everything ranging from their lax security posture to their bumbling response to the breach, and top executives were accused of corruption in the aftermath. And the question of who was behind the breach has serious implications for the global political landscape.

Equifax specifically traffics in personal data, and so the information that was compromised and spirited away by the attackers was quite in-depth and covered a huge number of people. It potentially affected 143 million people — more than 40 percent of the population of the United States — whose names, addresses, dates of birth, Social Security numbers, and drivers' licenses numbers were exposed. A small subset of the records — on the order of about 200,000 — also included credit card numbers; this group probably consisted of people who had paid Equifax directly in order to order to see their own credit report.

The fifth case: The Zoom program issue

Reports in 2020 highlighted the inappropriate exploitation of user data by the video conferencing platform Zoom. Facebook was among the leading platforms that benefited from this by collecting user data, including geographical location and device type. This situation led to a public lawsuit against the Zoom application, seeking to hold those responsible accountable.

Eventually, Zoom agreed to pay $85 million to settle the case related to providing false information about encrypting user data end-to-end and transferring user data to Facebook and Google without explicit user consent. This case resulted in the phenomenon known as Zoombombings.

The sixth case: the Tik Tok case

TikTok has been fined €345 million by Irish regulatory authorities for violating children's privacy in 2020, particularly concerning age verification and privacy settings. This marks the largest penalty imposed on TikTok to date, according to regulatory authorities. While the social media platform expressed respect for the decision, it contested the level of the fine, emphasizing adjustments made to privacy settings for accounts of users under the age of 16 long before the commencement of the investigation. The company highlighted improvements implemented in this regard.

Case Study 2: Implementing Big Data Technology in the Telecommunications Sector

This case study illustrates the application of big data technology in the telecommunications sector through an experience by Vodafone in New Zealand. Before using big data technology, the company faced challenges in marketing its services and products and had difficulty attracting new customers. For instance, Vodafone did not require any identity data for prepaid cards, making it difficult to understand the demographic characteristics of its customers.

Vodafone began to seek modern technologies to address these issues and decided to adopt big data technology based on Hadoop from Teradata Aster. This technology helped the company achieve several benefits, including:

Future Predictions for Marketing Services and Products: Big data technology assisted Vodafone in making future predictions for marketing its various services and products.

Analyzing Prepaid Card Customer Characteristics: The company was able to determine the characteristics of prepaid card customers by analyzing the time and amount of calls and data consumed on the network. This helped in directing more effective marketing campaigns and increasing the number of benefiting customers.

Identifying the Most Consuming Segments: Vodafone found that young people were the most frequent users of the company's applications, especially in the evening. This prediction was accurate by 89%. The company targeted this segment with suitable marketing campaigns and offers, leading to significant successes and increased number of customers and financial gains.

Analyzing Diverse Data Fields: The technology helped in analyzing various data fields such as bills, device types, time on the network, purchased deals, average revenue, age, gender (if known), contact patterns, upload and download volumes per session on the internet, and daily internet usage time.

Precise Customer Targeting: The technology ensured that the right messages were sent to the right customers at the right time, enhancing the effectiveness of marketing offers.

Maintaining Competitive Advantage: Big data technology helped Vodafone maintain its competitive edge and stay in the market competition with similar companies.

By implementing big data technology, Vodafone was able to overcome previous challenges and achieve substantial growth in both customer numbers and financial profits.

4.6. Opportunities and Threats

4.6.1. Opportunities:

Big data technologies can significantly contribute to the development of various operations and functions of telecommunications companies, offering numerous opportunities that need to be exploited, supported, and activated. Here are some examples:

1. Improving Customer Interaction:

Activating social media applications and other unstructured data sources to efficiently access customer information.

Combining unstructured data with structured data to gain a comprehensive view of customers.

2. Enhancing Product Improvement:

Big data can help understand how others perceive the company’s products, allowing for adjustments based on needs.

Analyzing social media content (unstructured data) to understand customer opinions and their distribution across different geographic locations.

Big data enables rapid testing of thousands of computer-supported designs, helping to assess minor changes in one factor that affect the final outcome. For example, a slight change in materials could impact cost, market launch time, and performance. This allows for enhancing the efficiency of the product process based on these tests.

3. Implementing Risk Analysis:

Predictive analytics supported by big data allows for managing and analyzing health reports or information from social media applications to keep up with the latest developments in the telecommunications company’s products, services, and surrounding environment.

Providing accurate and detailed information about service providers and customers, enabling the implementation of necessary measures to avoid some expected risks.

4. Data security:

. Mapping the entire data environment in the telecommunications company by taking advantage of big data tools as much as possible From insider threat analysis. Accurately monitor important and unprotected information.

5. Real-time personalization

Big data helps the analyst design the form and content of the telecommunications company's website

Real time to suit every subscriber browsing the website.

6. Reduce maintenance cost

Proactive monitoring is designed to identify network devices and anticipate when they will need to be updated.

4.6.2. Threats

There are several risks and challenges associated with the implementation of big data technology in the telecommunications sector that require caution and effective management. These challenges include:

Legal Threats:

Currently, there are no specific laws and regulations governing big data, so sectors interested in big data analytics must adhere to electronic data regulations. Some of the legal challenges that may face big data management processes will be reviewed.

Privacy:

Protecting personal data privacy becomes more challenging with the increase in data volume and its rapid dissemination. For example, although the United States does not have comprehensive data protection laws like Europe, U.S. law requires the protection of the confidentiality of customer information and imposes restrictions on the use, disclosure, and access of certain data, while allowing the use of aggregated customer information.

Responsibility:

Responsibility is understood as internal control in dealing with data, requiring the establishment of internal policies, procedures, and audit reports to implement such controls.

Security Threats:

As data transfer and the diversity of data sources and patterns increase, the security of big data becomes more important. Analyzing big data outside the jurisdiction of the data owner is an additional challenge in securing any data.

Social Threats Related to Organizational Culture:

Revolves around employees' reluctance to accept new technology and ineffective training on it, as well as decreased trust in data or refusal to share information within the company.

Ethical Threats:

Involve the misuse of big data technologies by some employees and the unethical invasion of customers' personal data without ethical constraints.

Technical Threats:

Include some employees' lack of skills in using big data technologies, as well as poor design of big data architecture and insufficient big data tools.

Conclusion

This study has found that internet users' data is a valuable asset that attracts the attention of targeted advertising makers. It is the fuel that ignites the digital economy engine driving internet companies and social media platforms to success. However, despite this economic attractiveness, the use of this data for advertising purposes raises questions about the balance between promoting the digital economy and preserving users' privacy. Targeted advertising studies also reveal the level of privacy violations users may be subjected to, as aspects of their personalities may be breached in an unacceptable manner, exceeding acceptable boundaries. The use of user data in advertising is an essential part of modern commercial competition, as companies strive to innovate advertising policies that ensure the continuity of their services while maintaining updates and developments that maximize their benefit from this data. However, this competition comes at a cost, as the risks associated with violating users' privacy increase. With legislation aimed at protecting user data, there is still a need for a sustainable balance between economic development and privacy rights in our connected and technologically advanced world.

The researchers also observed that social media platforms are privately owned commercial companies, whose operating principle is to provide free services by profiting from collecting user information and selling it to third parties for commercial purposes. This behavior is justified from the perspective of these companies as they provide all their services for free online.

Therefore, it is imperative for social media companies to adhere to legislation and laws that safeguard users' rights to not access their data, use it, or exercise the right to digital forgetfulness if they choose not to use these applications again.

References

Abdulamir, F., and Israa, H.,(2017) Violation of Privacy on Social Media Sites, Al-Baheth Al-Ilamiya Magazine, no. 36, p. 213.

Alderi, A. A., & Ismaeil, M. M. S. (2012). Electronic Crimes: A Legal Comparative Judicial Study. Cairo: National Center for Legal Publications.

Ali, A. & Faris, K.(2021) Assuring enhanced privacy violation detection model for social networks, International Journal of Intelligent Computing and Cybernetics, Vol.14.

Alkahlout, O. H. (2023). The effect of digital HRM practices on human resources performance: The case of Palestine (Master's thesis, Sakarya Üniversitesi).

Al-Maadawi,M.(2018) Protecting the User’s Information Privacy via Social Media Networks, a Comparative Study, Journal of the Faculty of Sharia and Law in Tanta, Al-Azhar University, Volume 33, No. 4, p. 1926,

Almadaawi, A. M. (2018). Information Privacy Protection for Users on Social Networking Sites: A Comparative Study. Journal of Sharia and Law, Tanta University, Volume 33, Issue 4.

Al-Qahtani, M.(2015)Protecting the Personal Privacy of Social Media Users: A Comparative Fundamental Study,(unpublished master’s thesis), Naif Arab Academy for Security Sciences.

Al-Sharif, S.(2014) Digital Data Privacy,” Cairo: Support Center for Information Technology,p. 4.

Ankit Jain et. al.(2021) Online social networks security and privacy: comprehensive review and analysis, Complex & Intelligent Systems 7, , pp 2157-2177.

Ayesha, S. & Umair, A.(2021) Privacy threats on social networking websites, Foundation University Journal of Engineering and Applied Sciences, Vol.2, No.1.

Belassel, Y., & Maqdour, N. (2021). The Right to Digital Privacy. The Future Journal of Legal and Political Studies, Volume 5, Issue 1.

Bouhlel, Y. (2019). Cyber Crimes and Prevention in Algerian Law in Light of the Arab Convention on Combating Information Technology Crimes, Penal Code, Criminal Procedure Law, Special Laws: A Comparative Study. Dar Al-Kotob and Higher Studies.

Brook Auxier , and others ,(2019)Americans and Privacy, Concerned, .1Confused and Feeling Lack Of Control Over Their Personal Information, Pew Research Center.

Eugenia, G. (2021) A Right That Should've Been: Protection of Personal Images on the Internet, The Law Review of the Franklin Pierce Center for Intellectual Property 61 IDEA, Vol.61, No.2.

Gaber, A. (2015). Targeting Internet Users with Commercial Ads and the Right to Privacy Protection. Human Sciences Journal, 9-46.

Galli Federico and others (2022), consent to targeted advertising , European business Law review no 33 , Holland

Habash, M.(2012).The world of Technology. “how-can-facebook-make-money”. Access: 16 February 2024. https://www.tech-wd.com/wd/2012/05/28/how-can-facebook-make-money/

Herwal, & Nabilah Heba. (2018). Protecting Consumer Information Privacy Online.

Hyang, S.(2016) What drives you to check in on Facebook?: Motivations, privacy concerns, and mobile phone involvement for location-based information sharing, Computers in Human Behavior 54, p397.

Ibn Bargouth, L. (2021). Information Privacy on social media in the Face of the Inevitable Trend towards the Virtual Maze: Challenges, Violations, and Reflections. Media and Society Journal, Volume 5, Issue 2.

Jeffrey, C. & Shawn, S.(2016) Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management, Computers in Human Behavior 54, p483

John LK, Kim T, Barasz K (2018) Ads that don’t overstep. Harvard Bus. Rev. 96(1):62–69

Kadwani, Ş. (2022). Controls for protecting the right to privacy via social networking sites - an analytical study, Journal of Media Research, 60(2), 903-948.

Khadija, J. et al. (2018). Protecting consumer information privacy online, Journal of Research in Law and Political Science, Volume (04), Issue 01.

Marie, F.(2008) Les reseaux sociaux en ligne et la vie privée, mémoire, Université Paris II Panthéon-Assas - Master 2 Droit du Multimédia et de l'Informatique , p.33

Office of the United Nations High Commissioner for Human Rights,(2014)The Right to Privacy in the Digital Age (New York: United Nations , p. 6).

Sagee, S. & Devika, R.(2021) Limiting the Social Media's Encroachment into a Person's Right to Privacy, Global Media Journal, Vol.3, Iss.3.

Saleh, M. Z. M. (2016). International Legal Protection of Personal Data Online: Between International Law, Agreements, and National Law. Arab Republic of Egypt: Center for Advanced Studies for Publishing and Distribution.

Shareetah, R. O. (2017). Electronic Advertising: Contemporary Concepts and Strategies. Dar Al-Tarbia Al-Haditha.

Sophie. B. (2021)Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data, Communication Research, Vol.48, Iss.7, p95

Sylvia, K. et. al.(2015) Like us on Facebook!: Analyzing user preferences regarding privacy settings in Germany, 6th International Conference on Applied Human Factors and Ergonomics.

Tawfiq, B., et al.,(2014) Improving Privacy Protection for Social Network Users in the Gaza Strip through Security and Technical Awareness, Al-Azhar University Gaza Journal, Natural Sciences Series, vol. 16, no.p. 69.

Ullah imdad and others,(2022),privacy in tergeted advertising : Asurvey , Naccache : CT-RSA 2001, pp. 408–424 ,C Springer-Verlag Berlin Heidelberg.

Wali, N., & Baghdadi, L. (2021). Legal Protection for Electronic Payment Methods in Algeria. Law and Local Development Laboratory.

Habash, M. (2013) A glimpse of Big Data, the world of technology, access

https://www.tech-wd.com/wd/2013/07/24/what-is-big-data/

Hadi, H., Shnain, A., Hadishahee, S., & Ahmad, D. A. (2014). Big Data and five v's characteristics.

http://www.iraj.in/up_proc/pdf/110141576915829-36.pdf

Beyer, M. (2011). Gartner Says Solving 'big data' challenge involves more than just managing volumes of data, Gartner, Retrieved November 25, 2011, from

https://www.gartner.com/newsroom/id/1731916

Vance, A. (2010). Start-Up Goes After Big Data with Hadoop Helper, New York Times,

https://bits.blogs.nytimes.com/2010/04/22/start-up-goes-after-big-data-with-hadoop-helper/

Mckinsey & Company (2011). Big Data: The next frontier for innovation, competition and productivity,

https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-

Douglas, L. (2012). "The Importance of 'Big Data': A definition". Gartner,

https://www.gartner.com/doc/2057415/importance-big-data-definition

Prashad, L. (2011, November 28). Social impact through satellite remote sensing: Visualizing acute Page 16 of 16

Bouillet, E. Kothari, R., Kumar, V., Mignet, L., Nathan, S., Ranganathan, A., Turaga, D., Udrea, O. & Verscheure, O. (2012). Processing 6 billion CDRs/day: from research to production (experience report) pp. 264-67 in Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems, (pp. 264-267).

https://www.researchgate.net/publication/241770193_Experience_Report_Processing_6_

Billion CDRsDay_From_Research_to_Production (26/11/2023)