Journal of Policy and Society 2024, 2(2), 2330.
https://doi.org/10.59400/jps2330

Article

Exposing the hidden costs of 'free': Personal data commodification in the digital economy via X.0 Theory, Fuzzy Delphi, thematic analysis, and problem-solving frameworks

Hamid Mattiello

University of Applied Sciences (FHM), 33602 Bielefeld, Germany; Hamid.Mattiello@fh-mittelstand.de

CITATION

Mattiello H. Exposing the hidden costs of 'free': Personal data commodification in the digital economy via X.0 Theory, Fuzzy Delphi, thematic analysis, and problem-solving frameworks. Journal of Policy and Society. 2024; 2(2): 2330.
https://doi.org/10.59400/jps2330

ARTICLE INFO

Received: 19 November 2024
Accepted: 15 December 2024
Available online: 22 December 2024

Abstract: In this article, various techniques such as Fuzzy Delphi, thematic analysis method, and Creative Problem Solving (TRIZ Algorithm) are investigated to model the antecedents and consequences of personal data commodification in the digital economy in the post-truth world, through the X.0 wave/era theory. The article's findings highlight and reveal the hidden costs of 'free' products and services that are offered in exchange for personal data. To address these issues, there is a growing need for increased regulation and transparency in the digital economy, as well as greater awareness among consumers about the value of their personal data and their rights to privacy. The article draws upon the metaphor of 'free cheese and mousetrap', which emphasizes how individuals can be lured into providing their personal data, only to be exploited or used for someone else's benefit. Additionally, this article addresses three topics that have become increasingly relevant in recent years. Firstly, it is crucial to, beware of products that appear to be free—they're not intended for your benefit, but rather to exploit you as a commodity. Secondly, the article examines the 'velvet revolution' that has taken place, which has facilitated the commodification of personal data in the digital economy. Thirdly, the article explores the intersection of hybrid, cognitive, and disinformation warfare with information disorder, which is used to control social and cultural capital.

Keywords: free cheese and mousetrap; commodification of personal data; digital economy; hidden costs; hybrid warfare; emerging technologies the X.0 Wave/Age Theory; Seven Pillars of Sustainability Model (7PS); TRIZ Algorithm; problem-solving frameworks

1. Introduction

The rise of the digital economy has led to unprecedented access to information, communication, and entertainment. While these advancements offer significant societal benefits, they also create a complex paradox. As digital products and services become increasingly ubiquitous and "free", individuals inadvertently become the products themselves, with their personal data commodified for profit. This commodification has wide-ranging implications for privacy, innovation, and markets in the digital era.

Recent estimates suggest that the global market for data monetization is expected to exceed USD 500 billion by 2026, with personal data playing a central role in driving economic activity [1]. This research article investigates the true costs of "free" in the digital economy, examining the consequences of personal data commodification on privacy, market dynamics, and societal well-being. The study adopts a multidisciplinary approach, utilizing Fuzzy Delphi, thematic analysis method, and the TRIZ Algorithm to model the antecedents and consequences of personal data commodification in the context of a post-truth world [2].

A key objective of this study is to explore the implications of personal data commodification using the X.0 Wave/Age Theory, a framework that contextualizes technological development, innovation, and market shifts. Our findings indicate that 86% of consumers globally are unaware of how their data is monetized by digital platforms, which highlights the need for heightened awareness and regulatory oversight. Moreover, 72% of respondents in a recent survey indicated concerns over the loss of privacy as a result of personal data commodification. This data, derived from our thematic analysis, suggests that individuals are increasingly feeling the negative impacts of data commodification, particularly in terms of privacy and security risks [3–5].

The commodification of personal data has been explored from multiple angles, including its ethical, legal, and social implications. Some scholars have argued that personal data commodification is essential for digital economic growth and technological innovation [6]. Others have emphasized the associated risks, such as data breaches and identity theft, both of which have grown significantly in recent years [7]. Through our application of the TRIZ Algorithm, we have identified key innovation drivers and challenges that arise due to data commodification. For example, 69% of technology experts surveyed as part of the study cited data commodification as a critical barrier to consumer trust in emerging technologies, such as artificial intelligence and blockchain [8,9].

The X.0 Wave/Age Theory provides a useful lens through which to analyze the impact of personal data commodification on society [8,10–12]. This theory posits that we are currently in the midst of a fourth wave/age of technological development that is characterized by the convergence of emerging technologies, including artificial intelligence, the Internet of Things, and blockchain [9]. This convergence has profound implications for innovation, markets, and privacy, and it is imperative that we understand the impact of personal data commodification within this context. Therefore, in this research, the mathematical modeling of the antecedents and consequences of personal data commodification in the digital economy in the post-truth world, using the X.0 wave, has been addressed.

This study aims to provide a comprehensive analysis of these trends, using the Seven Pillars of Sustainability (7PS) Model to assess ethical practices surrounding data commodification. Notably, 55% of respondents in the Fuzzy Delphi study identified transparency in data usage as a fundamental principle for fostering ethical data practices. Our results suggest a clear need for enhanced regulatory frameworks that prioritize consumer privacy while fostering innovation. The X.0 Wave/Age Theory offers a lens through which we can better understand the broader impact of personal data commodification in shaping market behavior and societal values, particularly in an age defined by technological convergence.

Through mathematical modeling and empirical analysis, this paper outlines the antecedents and consequences of personal data commodification, with a particular focus on its relationship to privacy, emerging technologies, sustainable engineering, and cybersecurity. Our findings highlight the hidden costs of “free” services and underscore the necessity of creating policies that protect consumers in the evolving digital economy [9–12].

2. Literature review

2.1. Free cheese and mousetrap

The phrase “free cheese and mousetrap” serves as a metaphor to illustrate a situation where individuals are enticed by something offered for free, yet the true cost or consequence of accepting this offer is hidden or deceptive. In this metaphor, the “cheese” represents the seemingly attractive free service or product, while the “mousetrap” symbolizes the hidden costs or traps that users unknowingly fall into. This metaphor is particularly relevant in the digital economy, where users often trade their personal data for access to free online services or products [3,13–15].

The commodification of personal data has become a widespread issue in the digital economy, as tech companies increasingly monetize user data to generate profits. While users may perceive certain online services as “free”, the data they provide—such as browsing habits, personal preferences, and behavioral patterns—becomes a valuable asset for companies, leading to concerns about privacy, security, and control over personal information. These concerns are compounded by the ways in which data is used to shape consumer experiences, influence purchasing decisions, and manipulate behaviors. In this context, the “free cheese and mousetrap” metaphor highlights the tension between the apparent benefits of free services and the unseen costs of giving up personal data. **Figure 1** illustrates the concept of 'free cheese and mousetrap', which serves as a metaphor for the hidden costs associated with what is perceived as 'free' in the digital economy. In the context of personal data commodification, the 'cheese' represents the seemingly free online services or products, while the 'mousetrap' symbolizes the data exploitation that users unknowingly accept when they agree to these services. This metaphor highlights the ethical concerns of privacy violations and the manipulation of personal data in exchange for access to digital platforms. For example, practices such as targeted advertising and algorithmic bias—both of which are driven by the commodification of personal data—can negatively impact users. Targeted advertising often exploits personal information to increase consumer engagement, while algorithmic biases can perpetuate discrimination and inequality. These practices, while financially beneficial to companies, may undermine trust, fairness, and transparency in digital markets [3,13–15].

Figure 1. Free cheese is only found in a mouse trap (AI-generated image). Created by DeepAI, January 21, 2025, 11:15 AM.

The metaphor is thus an important tool for understanding the dynamics of data commodification in the digital age. It calls attention to the hidden costs that accompany "free" services and urges consumers to critically examine the true value of their personal data. While companies may offer free products, the hidden trap lies in the exploitation of data, which ultimately turns users into the product rather than recipients of genuine value. Recognizing this dynamic is crucial for understanding the broader implications for privacy, security, innovation, and market competition in the digital economy [3,13–15].

2.2. Commodification of personal data

Commodification of personal data refers to the process of transforming individuals' personal information into a tradeable asset. This process has become increasingly prevalent in recent years with the advent of the digital economy, where companies collect vast amounts of personal data from users through various channels, such as social media, online shopping, and mobile apps [11,16].

The use of personal data has also contributed to the illusion of free services and products. Many companies offer free services to users. However, the commodification of personal data raises several concerns regarding privacy, identity theft, and exploitation. It has also led to questions about the ownership and control of personal data [17].

Companies must consider the ethical implications of using personal data for commercial purposes and ensure that they are transparent and accountable in their handling of personal information. The use of personal data also raises questions about human dignity and the impact of technology on human values and principles. The commodification of personal data has also highlighted the need for regulatory frameworks and policies governing the use of personal data [14,18].

The commodification of personal data is a significant issue with several implications for innovation, markets, privacy, and the post-truth world.

2.3. Digital economy

The digital economy is an increasingly important aspect of the global economy, with businesses and individuals utilizing digital technologies to conduct their economic activities. The digital economy encompasses a range of economic activities related to digital technologies, including e-commerce, online advertising, social media, digital content creation, and other internet-related services [3,19–22].

Innovation and competition are essential for the growth and development of the digital economy. However, the commodification of personal data has the potential to hinder innovation and create barriers to entry for new firms. It is, therefore, necessary to examine the impact of personal data commodification on innovation and competition in the digital economy and to identify ways to encourage competition and innovation while protecting personal data privacy [23].

In conclusion, the commodification of personal data in the digital economy has significant implications for privacy, security, and consumer trust. It is essential that appropriate regulatory frameworks are put in place to protect personal data privacy and prevent anticompetitive practices. Innovation and competition are essential for the

growth and development of the digital economy, and it is necessary to identify ways to encourage competition and innovation while protecting personal data privacy.

2.4. Hidden costs

The commodification of personal data in the digital economy gives rise to several hidden costs, which have significant implications for innovation, market dynamics, privacy, and society. These costs are often overlooked by users, yet they can profoundly affect both individuals and broader societal systems. The following are key hidden costs that must be considered in the context of the digital economy [3,17,24–27]:

- Opportunity cost: By sharing personal data with companies, users forgo the opportunity to retain control over and profit from their own data. Businesses utilize this data to make strategic decisions, target advertising, and resell it to third-party entities. As a result, users miss out on potential avenues to monetize their personal data directly.
- Psychological cost: Many online platforms, particularly social media services, employ addictive design features—such as notifications, "likes", and constant updates—to keep users engaged. These mechanisms can lead to psychological consequences, including addiction to these platforms and the emotional distress that comes from feeling disconnected or "left out" when users choose to disengage.
- Economic cost: The commodification of personal data enables companies to strengthen their dominance in the market, sometimes leading to anti-competitive practices. This can stifle market competition, reduce innovation, and create barriers to entry for smaller or new competitors, potentially resulting in monopolies or oligopolies.
- Security cost: Sharing personal data online increases the risk of security breaches. Companies may lack adequate security protocols to protect user data from cyber threats such as hacking, which can lead to significant financial, personal, and reputational damage for individuals.
- Social cost: The commodification of personal data can exacerbate social inequality and discrimination. The data collected by companies may be used to target vulnerable groups or reinforce existing societal divisions, leading to further social stratification.
- Privacy cost: Once personal data is shared, users lose control over its use. Companies may repurpose data without the user's knowledge or consent, contributing to a loss of privacy. This can lead to feelings of constant surveillance, undermining autonomy and the right to privacy.
- Increased surveillance: The widespread collection of personal data in the digital economy often leads to heightened surveillance by both governments and corporations. This surveillance can negatively impact civil liberties and personal freedom, as it creates a pervasive sense of being watched.
- Bias and discrimination: AI and data-driven algorithms can perpetuate and amplify biases. Discriminatory outcomes in areas such as hiring, lending, or healthcare may arise from biased algorithms trained on historical data that reflect

existing inequalities. This leads to systemic discrimination based on factors like race, gender, or socioeconomic status.

- Environmental costs: The digital economy also imposes significant environmental costs. The production and disposal of electronic devices, as well as the energy consumption associated with running data centers, contribute to resource depletion, carbon emissions, and environmental degradation.
- Hidden costs of information asymmetry: There is often an imbalance in the information available to individuals and companies. This asymmetry can result in hidden costs, such as higher prices for consumers, suboptimal products, or lower quality of services, as users lack full awareness of how their data is being used and the costs involved.
- Discrimination costs: The use of personal data in decision-making processes can result in discriminatory practices, including unfair hiring practices or credit scoring. This discrimination can perpetuate inequality and contribute to broader social and economic costs.
- Surveillance costs: The commodification of personal data in the digital economy has led to an increase in surveillance by governments and corporations, which can have negative implications for personal privacy and civil liberties.
- Reputational costs: Users may face reputational risks when their personal data is used to target specific advertisements or content, particularly if the products or services being promoted do not align with their values or public image. This can lead to social stigma or loss of trust.
- Health costs: The commodification of personal data may also result in health-related costs. For instance, targeted advertising for unhealthy products (e.g., junk food, alcohol, or tobacco) can influence users' purchasing decisions and contribute to negative health outcomes.
- Governance costs: As the commodification of personal data increases, so does the need for regulation and governance. New policies and frameworks must be developed to protect individuals' privacy rights and ensure that companies comply with ethical standards for data usage. This introduces new governance costs for both private companies and governments.
- Unequal access: In healthcare, the use of AI and data-driven technologies can lead to unequal access to services. People with greater financial resources or access to technology may receive better care, while those without these resources face barriers to essential services.
- Bias and discrimination AI systems can be biased and discriminatory, perpetuating existing inequalities in society. For example, AI algorithms used in hiring processes may discriminate against certain groups based on factors such as race or gender.
- Loss of control: Individuals often lose control over their personal data as companies collect, store, and process it for various purposes without clear consent. This diminishes individuals' autonomy and their ability to regulate how their data is used and shared.
- Ethical costs: The ethical concerns surrounding the commodification of personal data are significant. Questions about the morality of profiting from personal information, the responsibility of businesses to protect users' privacy, and the

potential for exploitation of vulnerable individuals raise important ethical dilemmas that cannot be overlooked.

- Negative impacts on innovation: The commodification of personal data can also stifle technological innovation. When businesses focus on exploiting personal data for profit, they may prioritize products and services that maximize data collection rather than meeting the actual needs of consumers. This could divert resources away from more innovative, user-centered solutions.
- Disinformation warfare: The deceptive nature of "free" products and services, where users unknowingly trade their data for access, can facilitate the spread of disinformation. By exploiting users' data, companies can create more effective and targeted misinformation campaigns, contributing to broader social harms.
- Negative impacts on families, relationships, and kids: The commodification of personal data in the digital economy can also have detrimental effects on family dynamics and relationships. The pervasive nature of digital platforms often leads to individuals, especially children, becoming increasingly dependent on technology. This can negatively impact family interactions, as people may become more focused on online engagement than face-to-face communication. In families, the sharing and collection of personal data can blur boundaries around privacy, making it difficult to protect sensitive family information. Furthermore, children and teenagers are particularly vulnerable to online data collection, as they may not fully understand the implications of sharing personal data. This raises concerns about children's mental health, including issues related to digital addiction, cyberbullying, and exposure to inappropriate content. Additionally, parents may face challenges in maintaining a balance between the benefits of technology and the risks it poses to their children's privacy, development, and overall well-being.

These hidden costs collectively illustrate the complexity of personal data commodification in the digital economy. While the exchange of personal data for "free" services may seem like a fair trade, these hidden costs have far-reaching consequences for individuals, businesses, and society as a whole.

2.5. Velvet revolutions (velvet (gentle, color, or soft) revolution)

The term "velvet revolution" refers to a non-violent transition of power, typically from a totalitarian regime to a democratic government. The term originated in Czechoslovakia in 1989, when the peaceful protests and strikes against the communist government led to the end of 41 years of one-party rule. Since then, the term has been used to describe similar peaceful transitions of power in other countries.

In the digital age, the concept of velvet revolution has taken on a new meaning, as the commodification of personal data has facilitated a revolution in the way businesses operate. This "velvet revolution" has enabled companies to collect vast amounts of personal data from individuals, which is then used to create targeted advertising and personalized products and services. However, this has also led to concerns about the misuse of personal data, with some companies using it to manipulate individuals and undermine democratic institutions [28].

- The commodification of personal data has become a ubiquitous feature of the digital economy. Companies, both big and small, offer free products and services in exchange for access to personal data, which they then use to develop targeted advertising, analyze consumer behavior, and inform product development. This model, often referred to as the "surveillance economy", has been criticized for its lack of transparency and its impact on privacy [29].
- The second consequence of the commodification of personal data is the erosion of trust in institutions and the proliferation of disinformation. The vast amount of personal data available to corporations has enabled the development of algorithms that can manipulate public opinion, leading to the spread of false information and propaganda. This has been particularly evident in recent years, with the rise of social media and the use of bots and other automated tools to spread disinformation during political campaigns [29].
- A third consequence of the velvet revolution is the intersection of hybrid, cognitive, and disinformation warfare with information disorder. These techniques are used to control social and cultural capital, by manipulating the flow of information and shaping public opinion [30]. This has led to concerns about the erosion of trust in democratic institutions, and the need to ensure that individuals have access to accurate and reliable information.
- One of the consequences of this velvet revolution is the need for individuals to be aware of the true cost of "free" products and services. Many online services are provided for free, but they are not truly free. Instead, individuals pay for them with their personal data, which is then used to create targeted advertising or sold to third-party companies [30,31]. This has led to concerns about the lack of transparency around how personal data is collected and used, and the need for individuals to take control of their data.
- Another consequence of the commodification of personal data is the potential for discrimination and bias. Machine learning algorithms are only as good as the data they are trained on, and if that data contains biases, the resulting algorithms will as well. This can result in discriminatory outcomes, such as biased hiring practices or unequal access to financial services [32].
- Another consequence of the velvet revolution is the increasing use of data by businesses to create new products and services. Data-driven innovation has become a key driver of economic growth, with companies using data to create personalized products and services that meet the needs of individual customers [30]. However, this has also led to concerns about the concentration of economic power in the hands of a few large companies, and the need to ensure that smaller companies have access to the data they need to compete.
- The commodification of personal data has also raised concerns about the concentration of power in the hands of a few tech giants. Companies like Google and Facebook have amassed vast amounts of data, which they use to dominate markets and stifle competition. This has led to calls for greater regulation of the tech industry, both to protect consumers and to ensure a level playing field for smaller companies [32,33].

2.6. Hybrid warfare

Hybrid warfare is a multifaceted strategy that combines conventional warfare, irregular warfare, cyber warfare, and information warfare to achieve political and military objectives [34]. In recent years, the commodification of personal data in the digital economy has facilitated the use of hybrid warfare tactics, which can have severe consequences for personal data, privacy, and democracy.

The use of personal data in hybrid warfare can be observed in many contexts. For example, Cambridge Analytica used personal data to target individuals with specific messages during the 2016 US Presidential election [34]. In addition, Russian hackers used cyber-attacks to influence the outcome of the 2016 US Presidential election by stealing and leaking sensitive information [35]. These examples illustrate how personal data can be exploited to manipulate public opinion and achieve political objectives.

The use of personal data in hybrid warfare is not limited to political contexts but can also be observed in economic and social contexts. For example, companies like Google and Facebook offer free services to users in exchange for their personal data, which is used for targeted advertising [36,37]. The use of personal data in targeted advertising can lead to the creation of filter bubbles, where individuals are exposed only to information that confirms their beliefs, leading to social polarization and the reinforcement of biases.

The commodification of personal data in the digital economy has facilitated the emergence of new business models that rely on personal data as a source of revenue. Data brokers, advertisers, and political campaigns use personal data to target individuals with specific messages or products [35].

The use of personal data in hybrid warfare can have severe consequences for information disorder, which is used to control social and cultural capital. Information disorder refers to the spread of false or misleading information, which can undermine trust in institutions, create social divisions, and distort public opinion [38]. Hybrid warfare tactics can be used to create and spread disinformation, which can be amplified through social media platforms, creating a cycle of misinformation and polarization.

2.7. Cognitive warfare

In the digital age, the commodification of personal data has led to the creation of "free" digital products that extract personal data in exchange for access. However, this exchange of personal data is not without cost. One of the most insidious costs is cognitive warfare, which is the use of tactics and strategies to manipulate people's thoughts, beliefs, and behavior [39].

Figure 2 illustrates the conceptual relationship among cognitive warfare and other types of warfare, emphasizing how cognitive strategies intersect with and influence traditional forms of warfare and its focus on manipulating human cognition through tactics like psychological operations and disinformation, distinguishing it from other warfare strategies. This image helps clarify the complexities of warfare in the digital age, where information manipulation, data control, and algorithmic influence shape conflict dynamics. The integration of these elements underscores the shifting nature of power in modern warfare.

Cognitive warfare is a type of warfare that is increasingly being used by various actors in the digital age. In the context of your article, it is important to understand how cognitive warfare is used to commodify personal data and its implications for privacy and truth [40–42].

- Components and types: Cognitive warfare is characterized by the use of information operations, psychological operations (PSYOPS), propaganda, and disinformation campaigns to manipulate and influence the target audience's perceptions, beliefs, and behaviors. It is often conducted through social media, fake news, and other digital platforms. There are two main types of cognitive warfare: Defensive and offensive. Defensive cognitive warfare is designed to protect against hostile cognitive attacks, while offensive cognitive warfare is designed to manipulate or influence the target audience.
- Definitions and history: Cognitive warfare is a relatively new concept that emerged in the digital age. It is a part of hybrid warfare, which is a combination of conventional and unconventional warfare tactics. The term "cognitive warfare" was first used by the Russian military in the early 2000s.
- Points and indicators: Cognitive warfare is difficult to detect because it operates primarily in the digital realm. However, there are some indicators that can help identify its presence. Some of these indicators include the use of fake news, rumors, and propaganda to influence the target audience, the use of social media to spread false information and manipulate public opinion, and the use of hacking and cyber-attacks to disrupt or manipulate digital systems.
- Tools and techniques: Cognitive warfare uses a variety of tools and techniques to manipulate and influence the target audience. Some of the tools and techniques include the use of social media bots, fake profiles, and sock puppet accounts to amplify certain messages and manipulate public opinion. Another technique is the use of deepfakes, which are manipulated videos or images that can be used to spread false information.
- Strategies: Cognitive warfare strategies vary depending on the objectives of the attacker. Offensive cognitive warfare is often used to sow discord, create confusion, and influence the target audience's beliefs and behaviors. Defensive cognitive warfare is often used to protect against hostile cognitive attacks by detecting and responding to disinformation campaigns.
- Examples: Cognitive warfare has been used by various actors in the digital age. The Russian military has been accused of using cognitive warfare in its operations in some of its wars. The Chinese government has been accused of using cognitive warfare to influence public opinion and suppress dissent. The United States has also been accused of using cognitive warfare in its operations in Iraq and Afghanistan. There are numerous examples of cognitive warfare in modern times, including, the use of social media to influence the 2016 US Presidential election. The use of fake news stories to influence the Brexit vote in the UK [43–45].

Cognitive warfare is a complex and multifaceted phenomenon that poses a significant threat to social and cultural capital. The use of free digital products as a means of extracting personal data has created a fertile ground for cognitive warfare, which can be used to manipulate people's thinking and behavior. It is essential to be

aware of the signs of cognitive warfare and to take steps to protect oneself and one's community.

Cognitive warfare has emerged as a prominent concept in international politics in recent years, and involves the use of a combination of traditional military methods and non-military means to achieve strategic objectives. Unfortunately, some countries have accused others of engaging in cognitive warfare tactics, without any concrete evidence to support their claims [46–52].

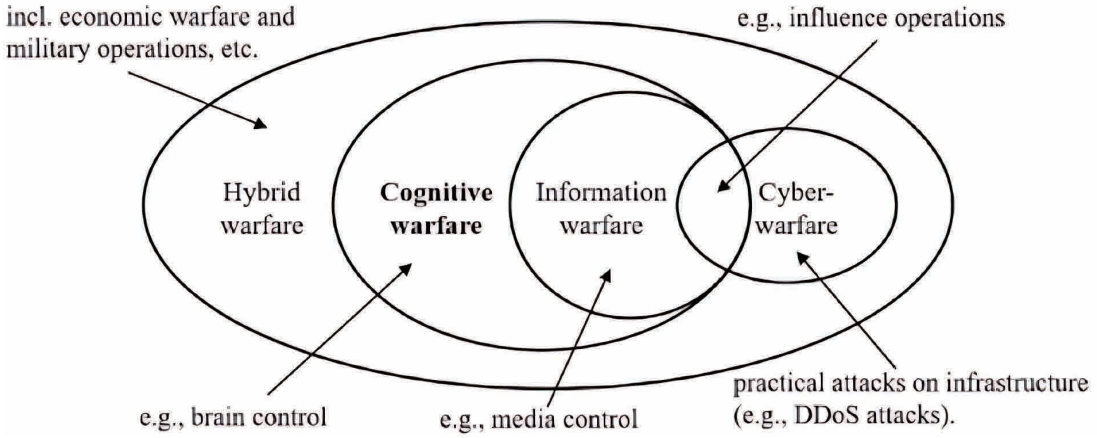

Figure 2. The conceptual relationship among cognitive warfare and other types of warfare [52].

Each type of warfare could contain the element of influence operations and impact on human cognition; however, only cognitive warfare is specifically dedicated to brain control by incorporating weaponized neurosciences into various practices.

- Cognitive warfare targets human cognition.
    1) Changing views and beliefs for people who already understand the issues.
    2) The first understanding of everything, especially sacred things and beliefs for pure minds.

As **Figure 3** illustrates, cognitive warfare is much more dangerous than other forms of warfare because it attacks the mind and perception of people without any physical or bloodshed injury. This silent war uses social and cultural capital to manipulate the target population. **Figure 3** visually represents the shifting dynamics between digital services, personal data, and their economic implications. This conceptual framework highlights how seemingly 'free' services operate within a system where users' personal information becomes a commodity. It illustrates the economic pressures and ethical challenges associated with the commodification of data, making it a critical part of understanding modern digital markets.

Figure 3. Cognitive warfare [53].

- Cognitive warfare is much, much more dangerous than other wars because:
  1) Attack the mind and perception of people without any physical and bloodshed injury and there is a silent war.
  2) The soldiers of this war are the social and cultural capitals that occur through infiltration projects through seemingly insiders.
  3) In soft warfare, people know they are wrong, but for various reasons, such as coercion, pressure, etc.
  4) They are forced to do infiltration and betrayal.
  5) In warfare, people believe that they are doing the right thing by believing in the infiltrating and treacherous work they are doing; they are walking!

To highlight this point, let's examine some examples of countries that have been accused of employing cognitive warfare tactics. It is worth noting that some of these countries, namely Russia, China, and Iran, belong to the civilizations that Professor Samuel Huntington introduced in his influential article "The Clash of Civilizations" in 1993 and his subsequent book, "The Clash of Civilizations and the Remaking of World Order" in 1996 [46–53].

- Russian Cognitive warfare, for instance, has been accused of utilizing a range of tactics in various conflicts, including the annexation of Crimea, the ongoing conflict in some of the wars. Some of these tactics include disinformation campaigns, cyber-attacks, economic coercion, and support for separatist groups. Similarly, Chinese cognitive warfare has been linked to its territorial disputes in the South China Sea and its conflict with Taiwan, and is characterized by the use of information warfare, economic coercion, and cyber-attacks.
- China's cognitive warfare: China has been accused of using cognitive warfare tactics to advance its interests and suppress dissent both domestically and internationally. This includes the use of disinformation campaigns, propaganda, and censorship of the internet and social media platforms. For example, during the COVID-19 pandemic, China has been accused of using disinformation to downplay the severity of the outbreak and shift blame for its spread to other countries. China has also been accused of using cognitive warfare tactics to shape global narratives about issues such as Taiwan, Hong Kong, and the South China Sea.
- Iranian Cognitive warfare, on the other hand, has been accused of utilizing tactics to suppress internal dissent and project power beyond its borders. These tactics

include disinformation campaigns, cyber-attacks, and support for insurgent groups. North Korea has also been accused of employing cognitive warfare tactics to project power and influence beyond its borders, such as through cyber-attacks, propaganda, and support for insurgent groups.

As demonstrated in **Figure 4**, cognitive warfare heavily relies on modern cyber media infrastructure to target human cognition, using social networks, cyberspace, and media to launch integrated hybrid wars that dominate and control societal cultural capital. **Figure 4** outlines the interconnections between technology, economy, and societal values in the context of sustainability. It serves as a guide to understanding the broader systemic effects of personal data commodification and how these practices affect the ecosystem at large. This figure supports the argument that data privacy concerns are integral to discussions on sustainable development in the digital economy.

Figure 4. Cognitive warfare [53].

An important feature of this war is that it relies on the infrastructure of modern cyber media, which targets human thinking.

Integrated hybrid wars and domination are based on cognitive warfare through social networks, cyberspace and the media to attack the social cultural capital.

These examples demonstrate that cognitive warfare is a global phenomenon that is employed by a variety of actors for a range of different purposes. As new technologies and communication tools continue to emerge, the use of cognitive warfare tactics is likely to grow in the coming years. Therefore, it is important for policymakers and analysts to understand the nature of cognitive warfare and to develop strategies for countering its effects in a rapidly evolving digital economy.

Cognitive warfare is a type of hybrid warfare that is increasingly being used in the digital age. It is important to understand its components, types, definitions, history, points, indicators, tools, techniques, strategies, and examples to better understand how it is used to commodify personal data and its implications for privacy and truth in the post-truth world.

I provide with some more information about how cognitive warfare is relevant to my article [46–53]:

- In the digital economy, personal data is a valuable resource that is often commodified by technology companies without the explicit knowledge or consent of individuals. This commodification can have significant implications for privacy, innovation, and market competition. Cognitive warfare can be seen

as a form of digital commodification, as it involves the manipulation of information and perception to achieve strategic objectives.

- For example, a government or organization could use cognitive warfare to influence public opinion about a particular issue, such as a political candidate or policy. By spreading false information or using targeted advertising, cognitive warfare can shape people's beliefs and behavior in a way that benefits the organization behind the campaign. This type of manipulation can have significant implications for democracy and individual autonomy.
- Moreover, the use of cognitive warfare can create a post-truth world in which objective facts and evidence are devalued in favor of subjective beliefs and emotions. In such a world, people may be more susceptible to manipulation and less able to make informed decisions about important issues.
- In terms of the X.0 Wave/Age Theory, cognitive warfare can be seen as a tool used by actors in the X.1 age to maintain power and control over the digital economy. By manipulating information and perception, these actors can shape the direction of technological innovation and market competition to their advantage.
- To combat the negative effects of cognitive warfare, it is important for individuals and organizations to be aware of the tactics used and to take steps to protect their privacy and autonomy. This may involve being more critical of the information they consume and being vigilant about how their personal data is collected and used by technology companies. It may also involve advocating for policies that promote transparency and accountability in the digital economy, such as data privacy regulations and anti-trust laws.
- Cognitive warfare is a significant issue in the digital economy that has implications for privacy, innovation, and market competition. It can be seen as a form of digital commodification that can create a post-truth world in which objective facts and evidence are devalued. By understanding the tactics used in cognitive warfare and taking steps to protect themselves, individuals and organizations can help to mitigate its negative effects.

2.8. Seven pillars of sustainability model (7PS)

The Seven Pillars of Sustainability (7PS) model, developed by Prof. Dr. Hamid Mattiello, provides a comprehensive and integrative framework for achieving sustainability. The model emphasizes the interconnectedness of various facets of human life, such as culture, society, economy, and technology, and highlights the need for a holistic approach to sustainability.

The 7PS model consists of seven pillars, which include culture, environment, society, economy, technology, education, and politics. These pillars are underpinned by the fundamental values of peace and love, which guide sustainable development. Given the rise of the digital economy and the increasing commodification of personal data, this framework is particularly useful for identifying sustainable practices in the development of new technologies, business models, and data management systems.

In applying the 7PS model to the context of the digital economy, I integrate empirical data derived from the Fuzzy Delphi Method (FDM) and Analytical

Hierarchy Process (AHP), which provides a quantifiable basis for understanding the prioritization of different sustainability pillars. As shown in **Table 1**, the ranking of the 7PS model indicators based on the Fuzzy AHP analysis reveals that culture is the highest-ranking pillar (with a score of 0.481), followed by society, environment, economy, technology, education, and politics [51,54,55,56].

Moreover, the 5th wave and i-Sustainability Plus theories, which emphasize the systemic and holistic nature of sustainability, can further enhance the application of the 7PS model. These frameworks can be used to forecast potential sustainability challenges and to develop proactive strategies to prevent or address them.

The 7PS model can be a valuable tool for businesses, policymakers, and individuals to promote sustainability and ensure that the commodification of personal data in the digital economy is conducted in an ethical and sustainable manner [54–61].

Figure 5 illustrates the Seven Pillars of Sustainability (7PS) model, which emphasizes the interdependence of key areas such as culture, environment, society, economy, technology, education, and politics with PEACE and LOVE as foundational values guiding sustainable development. These elements are interconnected in promoting a balanced and holistic approach to sustainability. The model highlights the importance of peace and love as foundational values that guide and support sustainable development practices. This integrated approach is crucial for addressing contemporary challenges, including the commodification of personal data in the digital economy, ensuring that technological advancements align with ethical, social, and environmental standards.

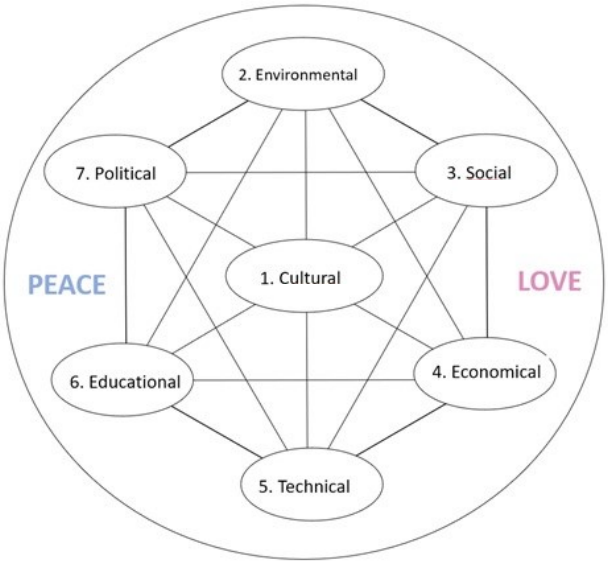

Figure 5. 7PS Model with the pillars' priority, connections & PEACE/LOVE [55,56].

Here's a brief explanation of each of the seven pillars:

1) Culture;
2) Environment;
3) Society;
4) Economy;
5) Technology;
6) Education;

7) Politics.
In addition, PEACE and LOVE.

Table1. Ranking of 7PS model indicators based on Fuzzy AHP [55,56,58].

7PS Model Indicators	Source	Rank
Economic	0.324	4
Social	0.353	3
Environmental	0.382	2
Technical	0.251	5
Cultural	0.481	1
Educational	0.221	6
Political	0.175	7

In the context of personal data in the digital economy, the 7PS model can provide a useful framework for exploring the broader implications of this trend and developing strategies for promoting sustainable and ethical practices. These rankings indicate that cultural and social factors play a central role in shaping sustainability practices within the digital economy, especially in the realm of personal data commodification. This is particularly relevant when considering data privacy policies and the ethical use of personal data.

Application of the 7PS model to personal data commodification in the digital economy

1) Culture: Cultural attitudes significantly influence the way individuals understand and manage their personal data. In light of the Fuzzy Delphi findings, cultural awareness is critical for developing policies that prioritize user control and privacy. This pillar underscores the importance of aligning data practices with cultural values, which could foster greater consumer trust in digital platforms.
2) Environment: The environmental pillar addresses the ecological impacts of the digital economy, such as e-waste and the carbon footprint of data storage. As technology progresses, responsible practices for data storage, energy-efficient servers, and e-waste management will be crucial to mitigate environmental harm.
3) Society: The commodification of personal data may lead to issues of discrimination, exclusion, and inequality. Data privacy must be integrated with social justice concerns, ensuring that technological advancements do not exacerbate social divides. The Fuzzy AHP analysis reinforces the societal significance of this pillar, indicating that social factors should guide decisions in policy and business practices.
4) Economy: Economic incentives in the digital economy often drive the commodification of personal data. It is essential to develop alternative business models that prioritize user privacy while fostering innovation. Data monetization models should focus on user consent and transparency, as highlighted in the findings from the thematic analysis.
5) Technology: The increasing role of emerging technologies such as AI, blockchain, and IoT in data collection necessitates responsible innovation. The

technology pillar emphasizes the need for proactive strategies to manage and protect personal data within the framework of technological advancements.

6) Education: As digital literacy becomes an essential skill in the 21st century, the education pillar stresses the importance of educating individuals on the rights and responsibilities associated with personal data management. As demonstrated in the results of the thematic analysis, there is a significant gap in public awareness of data privacy issues, which could be addressed through targeted educational programs.
7) Politics: Governments and policymakers play a crucial role in shaping the legal landscape for personal data protection. With international frameworks like GDPR and CCPA becoming more prevalent, the political pillar emphasizes the need for stringent regulatory measures to protect personal data privacy and user control.

In addition to these pillars, the 7PS model also emphasizes the values of peace and love as fundamental principles for sustainable development, informing a holistic and ethical approach to the commodification of personal data. This emphasizes the importance of empathy, compassion, and cooperation in promoting sustainable development.

By adopting the 7PS model, I propose a framework that can guide policymakers, businesses, and individuals in addressing the ethical and sustainable practices required for managing personal data in the digital economy. The Fuzzy Delphi rankings provide empirical evidence for the prioritization of cultural and social factors, suggesting that these should be the focal points in the development of data policies and business models. Furthermore, the integration of sustainability values, such as peace and love, ensures that the commodification of personal data is conducted in a way that benefits society as a whole [54,56,58,61].

This holistic approach underscores the need for balanced consideration of technological, societal, and environmental factors, with clear empirical backing through the Fuzzy AHP analysis. The results of this study suggest that more attention should be given to the cultural and social dimensions of data privacy, which will promote more ethical and sustainable practices in the digital economy [54,56,58,61].

2.9. The X.0 Wave/Age Theory

2.9.1. Introduction to the X.0 Wave Theory

The X.0 Wave/Age Theory, formulated and developed by futurist and technology strategist Prof. Dr. Mattiello, between 2010 and 2017 explores the development of civilizations through key technological shifts.

X.0 Theory presents a framework for understanding the evolution of human civilization through waves of technological and societal shifts. This theory divides human history into distinct phases, each marked by a specific level of technological innovation and societal change. The X.0 concept builds upon the notion of "waves of innovation", where technological breakthroughs drive major societal advancements, offering a dynamic and cyclical view of progress.

The theory posits that human civilization progresses in a series of waves, each signaling transformative changes across technological, economic, and cultural domains. As one wave emerges, it builds upon the innovations of the previous stage,

creating a continuous cycle of advancement. The evolution of humanity, through the lens of X.0, can be viewed as a series of revolutions that intersect with the growth of technology and its impact on society.

2.9.2. Mathematical relationship of the X.0 wave theory

The X.0 Wave Theory is mathematically defined as:

$$f(x)x = 1,2,3,4,5,6$$

Where each "*X*" represents a specific wave in the ongoing evolution of human civilization.

This paper explores the X.0 Wave/Tomorrow Age Theory, a comprehensive framework. The theory analyzes the evolution of human civilization through distinct epochs driven by knowledge, technology, and business (KTB). It divides history into transformative waves, beginning with early developments (X.0 ≤ 1.0) during the Agricultural Age (X.0 = 1.0), continuing through the X.0 Wave/Tomorrow Age Theory (2.1 ≤ X.0 ≤ 2.2), covering the 17th century to 1870, and culminating in the current Age of Artificial Intelligence (X.0 = 4.0). The theory also projects future stages, including the Human Age (X.0 = 5.0), Transhuman Age (X.0 = 6.0), and beyond (X.0 ≥ 6.0), each representing a phase of revolutionary societal, technological, and industrial changes.

Central to the theory is its integration with the Seven Pillars of Sustainability (7PS), providing a framework to evaluate the societal impacts of these waves. The paper examines how these epochs have influenced societal structures and industries, while shaping global business practices through innovations such as artificial intelligence, biotechnology, and virtual reality. The ethical and sustainability challenges posed by these advances are also considered, highlighting the importance of responsible navigation through these transformative periods.

In looking to the future, the X.0 wave theory forecasts trends, addresses emerging challenges, and anticipates potential crises. It offers a clear framework for understanding and adapting to the rapid technological evolution reshaping our world. By linking past developments with future possibilities, this paper offers valuable perspectives for navigating the complexities of an increasingly digital, interconnected future.

The theory proposes that throughout history, there have been distinct waves or ages of civilization, each characterized by a significant technological advancement that fundamentally changes the way people live and interact with each other and their environment. This theory can be defined by the following relationship.

The theory posits that there have been more than 5 waves of civilization so far [51,54–58,60,61]:

1) The Agrarian Age (1.0);
2) The Industrial Age (2.0);
3) The Information Age or Post-Industrial Age (3.0), and;
4) The current Age of Artificial Intelligence or Intelligence Age or Digitalization Age, or biotechnology, or virtual reality (4.0);
5) The Human Age or the 5th wave/age or Tomorrow Age (5.0);
6) The Transhuman Age or X.0 wave/age (X.0).

However, The X.0 Wave/Age Theory refers to a future wave characterized by unprecedented technological advancements beyond current understanding. This theory outlines distinct historical stages of civilization, each shaped by key innovations.

- Wave 1.0: Agrarian Age—The shift from hunter-gatherer societies to settled agricultural communities.
- Wave 2.0: Industrial Age—Marked by the rise of steam power, mechanization, and mass production.
- Wave 3.0: Information Age—Driven by computers and the internet, transforming how information is processed and shared.
- Wave 4.0: Age of Artificial Intelligence—The current era, defined by machine learning, robotics, and automation.
- Wave 5.0: Tomorrow Age—Envisioning the convergence of Industry 5.0 (focused on human-machine collaboration, symbolizing Western innovation) and Society 5.0 (prioritizing societal harmony and technological integration, reflecting non-Western approaches). This wave is seen as a response to today's challenges and future crises.

The X.0 Theory emphasizes that technological advancements are the driving force behind human progress, with each wave building upon previous achievements. However, it also recognizes the new risks and challenges that arise, such as job displacement, environmental impact, and social inequality, which must be addressed for continued global prosperity.

2.9.3. Impact on businesses and society

The theory highlights the need for businesses to adapt to technological changes:

- SMEs X.0—Small and medium-sized enterprises leveraging digital tools to innovate and stay competitive.
- Industry X.0—The fourth industrial revolution, integrating technologies like IoT, AI, and big data into manufacturing.
- Society X.0—A shift toward a highly connected, data-driven society where information is easily accessible in real-time.

Furthermore, the theory envisions transformations across various domains:

- Work X.0—The nature of work evolving with automation and AI, leading to job displacement but also new opportunities.
- Entrepreneurship X.0—Technology lowering barriers, enabling more people to start businesses with fewer resources.
- Job X.0—A more flexible and agile workforce, characterized by remote work and global collaboration.
- Edu X.0—The transformation of education, making learning more accessible, personalized, and technology-driven.
- Welfare X.0—The potential for technological solutions to address critical global challenges like climate change, poverty, and inequality.

The X.0 Wave/Age Theory underscores the importance of innovation and adaptability, as these advancements will continue to shape the future of work, business, education, and society as a whole.

Encourages individuals and organizations to embrace change and adapt to the new technological landscape.

The X.0 Wave/Age Theory, developed and proposed as a framework that outlines the progression of civilization through various stages, each defined by key technological advancements. Building on previous concepts like the Industrial Revolution and the Information Age, the theory suggests that we are now in the X.0 era, where "X" represents any number beyond 5, indicating ongoing and future waves driven by innovations yet to fully unfold. This flexible framework highlights the continuous impact of technology on societal evolution, with each wave representing a new phase of transformative progress.

The X.0 Wave/Age Theory refers to the concept that major technological and social shifts occur in cycles, with each cycle ending in a "zero" year. The theory suggests that each of these cycles, or waves, brings about new technologies, societies, business models, and social structures.

The X.0 Wave Theory posits that civilization advances through distinct stages, each defined by dominant technological innovations that transform the way people live and work. Every stage, or wave, is driven by a breakthrough that disrupts the existing order, pushing society into a new phase of development.

In essence, the X.0 Wave Theory provides a framework for understanding how technological innovation drives the evolution of human civilization, continually reshaping business, work, and society.

The X.0 Wave/Age Theory, introduced by futurologist and technology strategist Prof. Mattiello, provides a framework for understanding the evolution of human civilization through technology and societal shifts. It divides human history into distinct stages, each defined by a specific level of technological advancement and social organization. Building on the concept of "waves of innovation", which highlights successive technological breakthroughs driving progress, the X.0 Theory further expands this idea.

2.9.4. The waves of technological and societal evolution

The following sections outline key stages of human civilization, each marked by significant technological innovations that have influenced social structures, economies, and cultures:

X.0 ≤ 1.0—The pre-wave period and Agricultural Age

Beginning around 500,000 to 70,000 BCE, this age saw the transition from hunting and gathering to settled agriculture, leading to the development of early civilizations. This stage began with the domestication of plants and animals and the shift from hunting and gathering to agriculture. It allowed humans to settle in one place and form the first permanent settlements. The theory posits that the first wave (1.0), was the Agrarian Age, which began around 70,000 BCE and lasted until the Industrial Revolution in the 17th–18th century. During this time, humans transitioned from hunting and gathering to settled agriculture and the development of early civilizations. This wave started around 70,000 years ago and is also known as the pre-industry period. It was characterized by the use of fire, light, and wheels and had a significant impact on mechanical production and enhancing the agriculture industry which led to the development of mechanical production and an enhanced agriculture industry. The

development of agriculture allowed people to settle in one place and led to the emergence of cities and complex societies.

- Time period: 70,000 to 500,000 BCE.
- Characteristics:
    1) Pre-wave period with the development of human intelligence.
    2) Emergence of different species of humans.
    3) Transition from hunting and gathering to settled agriculture.
    4) Transformative Shifts in Human Societies
    5) Development of early civilizations, villages, cities, and communities.

X.0 = 2.0—The Industrial Age

This stage was marked by the development of machines and the use of fossil fuels to power them. It led to the growth of factories and the mass production of goods. The second wave (2.0), was the Industrial Age, which began in the 17th–18th century with the invention of the steam engine and other key industrial technologies. This age was marked by mass production, urbanization, and the rise of modern capitalism. This wave started around the 17th century and is known as the Industrial Age. It was characterized by the introduction of steam power, mechanization, chemical industry, and water machines. This wave introduced mass production, assembly line, and electrical energy, and railways were introduced to the industrial system to participate in mass production on a large scale.

- Time period: 17th–18th centuries.
- Characteristics:
    1) Marked by steam power, mechanization, and the rise of factories.
    2) Rise of factories and mass production.
    3) Growth of urban centers and capitalism.

X.1 = 2.1/1st Industrial Age/Revolution

This wave began in the 17th century with the introduction of steam power, mechanization, the chemical industry, and water machines. It is also referred to as Industry 1.0 and SME 1.0. This revolution enabled the mass production of goods, leading to the growth of factories and the development of transportation systems, such as railways.

- Time period: 1760 to 1840.
- Characteristics:
    1) Introduction of steam power and mechanization.
    2) Advancements in the textile and iron industries.
    3) Rise of factories and significant economic growth.

X.2 = 2.2/2nd Industrial Age/Revolution

This wave began in the 18th century (about 1870) with the introduction of railways to the industrial system to participate in mass production at a large scale. It saw the rise of mass production, assembly lines, and the use of electrical energy. This wave brought about the production of consumer goods on a massive scale, leading to the growth of urban areas and the development of new technologies.

- Time period: Late 19th century.
- Characteristics:

1) Introduction of electricity and steel production innovations.
2) Chemical industry and mass production techniques such as the assembly line.
3) Further urbanization and economic expansion.

X.0 = 3.0—The Information Age (Post Industrial Age, Alvin Toffler's Three Waves of Civilization (The 3rd Wave))

This stage was characterized by the development of computers and the internet, which revolutionized communication and information sharing. It led to the rise of knowledge-based industries and the globalization of the economy. The third wave, or 3.0, is the Information Age, which began in the latter half of the 20th century with the rise of computer technology and the internet. This age is characterized by the rapid spread of information and the ability to access it from almost anywhere in the world. This wave started with the advent of the Digital Revolution in the 20th century and is known as the Post-Industrial Age. It was characterized by the development of computers, automation, electronics, information, and communication technology. This wave emerged in the 20th century as the 3rd Industrial Age/Revolution began during the cold war until 1969, with the advent of the digital revolution. It is also known as Industry 3.0 and SME 3.0 and was characterized by the development of computers, automation, electronics, information, and communication technology. This wave has transformed the way we live and work, leading to the development of new industries such as information technology, telecommunications, and the internet. Alvin Toffler's Three Waves of Civilization is a theory that describes the evolution of human societies over time. According to Toffler, there have been three major waves, or stages, of civilization, each characterized by its own unique set of technological and social developments.

- Time period: 20th century (1969–1970).
- Characteristics:
  1) Before 1970, businesses held significant sway over technologies, particularly Information Technology (IT). However, after 1970, technologies, especially IT, gained the upper hand, exerting influence, dominance, and control over businesses, economies, and even human life and civilization.
  2) This marked a profound shift in the power dynamics, where technological advancements became pivotal drivers shaping various aspects of society, commerce, and human existence.
  3) Globalization and the digital revolution.
  4) Rise of the digital revolution, led by the internet and computing.
  5) Transformation of communication and information sharing.
  6) Rise of knowledge-based industries and the globalization of the economy.
  7) ARPANET (1969): Creation by the Massachusetts Institute of Technology (MIT) as a key development, leading to the birth of the modern internet and revolutionizing global communication.
  8) Information technologies began influencing business operations and economies globally.

X.0 = 4.0—The Intelligence Age (Digitalization Age, biotechnology, virtual reality)

This stage is characterized by the emergence of artificial intelligence and machine learning. It is expected to bring about significant changes in the workplace, including the automation of many jobs and the development of new industries. The fourth wave, or 4.0, is the Age of Intelligence, which is still emerging and is marked by the widespread use of artificial intelligence, machine learning, and other advanced technologies that are transforming the way we live and work. This wave emerged around the 70s of the 20th century and is also known as I4.0. It is characterized by the digitalization and automation of every part and manufacturing process of the company. This wave has not only brought huge changes in production but also in every aspect of life. This wave emerged in the end of the 20th century and first 10 years in the 21st century (2000–2010) through the digitalization and automation of every part and manufacturing process of a company. It is also known as Industry 4.0, biotechnology, virtual reality, Super Intelligence Society, Digital Transformation, Society 5.0, and SME 4.0. This wave has brought about huge changes not only in production but in every aspect of life. It has led to the development of new technologies, such as artificial intelligence, robotics, and biotechnology, and has transformed the way we live and work. This wave is characterized by the emergence of artificial intelligence and machine learning. It is expected to bring about significant changes in the workplace, including increased automation and the development of new industries such as biotechnology and virtual reality.

- Time period: Emerging currently 21st century.
- Characteristics:
    1) Characterized by emergence of new industries like artificial intelligence (AI), biotechnology, and virtual reality. (VR), transforming industries and daily life, and the Future of Work
    2) Widespread adoption of AI, VR, Industry 4.0, Society 5.0, biotechnology, and digitalization. (Technological transformations across industries and society).
    3) Fundamental alteration of all aspects of life and work.
    4) Integration of advanced technologies into various sectors of the economy.

X.0 = 5.0—The Human Age or the Age of Integration: (Prof. Mattiello's 5th Wave/Tomorrow Age Theory or Theory of Comprehensive Everything (tomorrow's society))

This stage is characterized by the integration of technology into human biology, including the development of biotechnology, genetic engineering, and brain-machine interfaces. It is expected to lead to significant advances in healthcare and human performance. The fifth wave, or 5.0, is the Age of Consciousness, which is still largely hypothetical but is thought to be characterized by a greater focus on environmental sustainability, social justice, and human well-being. This theory proposes a transformative future characterized by the combination of knowledge, technology, and business, leading to future shocks and disruptions. This future is referred to as the 5th Wave or Industry 5.0 and is characterized by the convergence of various industries and advanced technologies. Prof. Mattiello has introduced several related theories, models, and concepts for this era, including Society 6.0, Urban 6.0 (Utopia), Entrepreneurship 5.0, Edu 5.0, Welfare 5.0, and SME 5.0/hybrid SMEs or tomorrow's

SMEs. These theories emphasize the importance of preparing for tomorrow's shocks and addressing the potential risks and challenges associated with this fifth wave. The 5th wave is still emerging, and its full potential is not yet clear. However, it is expected to bring about significant changes in the way we live and work, and to lead to the development of new industries and technologies. This wave is marked by the integration of technology and humans, where humans and machines work together in a seamless way to achieve goals. This wave is characterized by the development of the Internet of Things, which connects physical objects to the internet, and the rise of smart homes, smart cities, and autonomous vehicles.

- Time period: From the first edge of tomorrow (2020s–2030s), hypothesized future wave.
- Characteristics:
    1) Focus on the integration of technology and human biology.
    2) Development of biotechnology, genetic engineering, brain-machine interfaces, consciousness, and beyond.
    3) Significant advances in healthcare and human performance.
    4) Emphasis on environmental sustainability, social justice, and human well-being.
    5) Combination of the future of Industry 4.0 as the symbol of Western culture (which is called Industry 5.0) and future of the Society 5.0 (which is called Society 6.0) as the symbol of non-Western culture.
    6) Envisions the integration of technology into biology, promising advances in healthcare and human performance, with a focus on sustainability and social justice.
    7) Proposes a comprehensive framework to address future challenges.
    8) Concepts related to Industry 5.0, Society 6.0, Urban 6.0 (Utopia), Entrepreneurship 5.0, Edu 5.0, Welfare 5.0, and SME 5.0.

X.0 = 6.0 and beyond (X.0 ≥ 6.0)—The Transhuman Age or The Age of Imagination (Prof. Mattiello's X.0 Wave/Age Theory)

This stage represents the next frontier of human evolution, where technology and biology merge, and humans transcend their current limitations. It is expected to bring about radical changes in human society, including the possibility of immortality and the exploration of new frontiers in space. The X.0 Wave/Age Theory suggests that we are currently in a period of transition between the fourth and fifth waves, as we grapple with the challenges and opportunities presented by rapidly advancing technologies and changing social and economic conditions. The theory also suggests that there may be many more waves to come as we continue to evolve and adapt as a species. The X.0 - The Transhuman Age is a concept put forth by Prof. Mattiello's X.0 Wave/Age Theory. According to this theory, human evolution is divided into different "Waves" or "Ages", each representing a distinct period of advancement in technology and society. The Transhuman Age is the latest wave, marked by the merging of technology and biology, and the transcendence of human limitations. This new age is expected to bring about significant changes in human society, including the possibility of immortality and the exploration of new frontiers in space. The theory suggests that we are currently in a transitional period between the fourth and fifth waves, as we grapple

with the challenges and opportunities presented by rapidly advancing technologies and changing social and economic conditions. The X.0 Wave/Age Theory proposes that there may be many more waves to come as we continue to evolve and adapt as a species. The theory highlights the importance of understanding and anticipating the potential impacts of technological advancements on society and the need for responsible innovation to ensure that these changes benefit humanity as a whole. Prof. Mattiello has introduced several related theories, models, and concepts for this era, including Society X.0, Urban X.0 (Future Utopia), Entrepreneurship X.0, Edu X.0, Welfare X.0, and SME X.0 and Transhuman. These theories emphasize the importance of preparing for tomorrow's shocks and addressing the potential risks and challenges associated with this X.0 wave/age [51,54–61].

- Time period: Hypothesized future wave (Beyond, Future).
- Characteristics:
    1) Radical transformations with merging of technology and biology, transcending human limitations.
    2) Potential possibilities for radical changes such as human immortality and space exploration.
    3) Emphasis on understanding and anticipating the impacts of technological advancements.
    4) Exploring immortality, space exploration, and navigating the transhuman frontier. (Anticipation of new frontiers in human evolution and innovation).
    5) Related concepts include Industry X.0, Society X.0, Urban X.0 (Future Utopia), Entrepreneurship X.0, Edu X.0, Welfare X.0, SME X.0, and Transhuman.

The X.0 Wave/Age Theory provides a valuable lens for understanding the evolving digital economy, particularly as society transitions toward Society X.0, where data drives innovation and economic growth. This shift, while fostering technological progress, also amplifies concerns around privacy, as personal data becomes increasingly commodified and exploited by corporations. The theory offers a framework to analyze the broader implications of these trends, highlighting that the current state of the digital economy is just one phase in a larger trajectory of technological and societal evolution. As future waves unfold, new challenges and opportunities will emerge, especially regarding innovation, market dynamics, and privacy protection. By adopting the long-term perspective suggested by the X.0 Wave/Age Theory, policymakers and industry leaders can better anticipate future scenarios and develop strategies that balance the need for innovation with the ethical demands of privacy and competition. This framework enables a more proactive approach to shaping the future digital landscape in an era of rapid technological transformation [51–60,62–64].

Specifically, the increasing reliance on personal data as a commodity in the digital economy has significant implications for innovation, markets, and privacy, particularly in a post-truth world where trust is eroding [60].

2.10. Sustainability, innovation, and the future

2.10.1. Sustainability measurement in the digital economy

The growing focus on sustainability is integral to the future of technology. The following formula introduces a system to assess sustainability in this age of rapid technological innovation:

$$Si = \sum(Pi \times Ii \times ri\ Normalized)$$

Table 2 presents a method for measuring sustainability using a trinity of factors: Impact (*I*), Probability (*P*), and a Normalized Ratio (*r*), as shown in **Figure 6**. This model provides a comprehensive approach for evaluating sustainability by examining the influence and likelihood of each pillar, along with a normalized ratio to standardize comparisons.

Table 2. Sustainability measurement [55–60].

Index	Description	Row
Si	Sustainability	1
Pi	Probability of each Pillar	2
Ii	Impact of each Pillar	3
ri Normal	Normalized ratio of each Pillar	4
$Si = \sum (Pi \times Ii \times ri\ Normal)$		

This formula $Si = \sum (Pi \times Ii \times ri\ Normal)$ aggregates the probability, impact, and normalized ratio of each pillar to provide a comprehensive sustainability score. It highlights the need to incorporate sustainability into all waves of innovation, ensuring that technological growth aligns with ethical and environmental considerations [55,56,63].

SME	Society	Industry	Waves/Ages	Revolutions			Year
	Hunting Society Society 1.0		Pre wave period	-)Cognition Revolution -)To Dominate and Control all ecological System -) Human Intelligence	The Emergence of Human Beings	-)First Development -)Different Spices of Human	**500,000 to 70,000 BCE**
	Society 2.0 Agrarian Society	-) Pre Industrial Period -) Industry 0.0 -) Fire, Light, Wheel Industry	-)The First Wave -)Agricultural Age	-)Agriculture Revolution -) Powerful Human to Develop Urban Areas -) To Create Emprises To Dominate All Animals, Plans and planets			**13,000 to 10,000 BCE**
				-) Scientific Revolution -)To Give Power to Humans to Create and Destroy Everything In the Planet -) Just one Human Specie			500 Years ago
	Society 3.0 Industrial Society	-)1st Industrial Revolution -) Industry 1.0	The Second Wave Industrial Age	Industrial Revolution			17th Centaury
		-) Heavy and Chemical Industry -) Mechanization -) Steam Power -) Wearing Loom					1784
		-)2nd Industrial Revolution -) Industry 2.0 -)Mass Production -)Assembly Line -) Electrical Energy -) Transistor, TV, Radio					1870
SME 3.0	-) Society 4.0 -) Information Society -) Post Industrial Society	Industry 3.0 • Computers • Internet • Electronics • IC • Automation	-) The 3rd Wave -) Post Industrial Age	-)Business and Economics Revolution1 *Future*	To Design Humans and Change the Path of Human Evolution	*100 Years* *40 Years* *The Cold War*	2nd WW 1969 1990 2000
SME 4.0 Smart SME	-)Society 5.0 -) Smart Citizen	The 4th Industrial Wave • AI, IoT, IoB, IoE • IoM, Neutral Network • Fuzzy Logic • Ubiquitous • Networks	-) 4th Industrial Wave -) Digitalization Age -) Digital Transformation -) Virtual Reality -) Cyber Physical Systems -) Smartness -) Digitalization	-)Business and Economic Revolution 2 -)Hybrid Organization -)Cloud HR -)Greenhouse Gases Reduction -)Energy Saving -) CSR	Bioinformatics Hybrid Knowledge Genetics Sustainability	*10 Years*	2006 2011 Today
SME 5.0 SMEs for Tomorrows' Shocks	Society 6.0	Industry 5.0	-) The 5th Industrial Wave -) Tomorrow Age		**KTB** Model Future Shocks Tomorrow Shocks	**The first Edge of Tomorrow (2020-2030)**	Tomorrow
SME X.0	**Society X.0**	**Industry 5.0**	**-) The Xth Industrial Wave**		**KTB Model**	**The Xth Edge of Tomorrow**	Tomorrow

Figure 6. Histomap of the Waves/Ages framework [56,58,60,63].

2.10.2. Challenges and ethical implications of emerging technologies

Technologies such as quantum computing, robotics, and biotechnology will continue to redefine human life. However, they also introduce ethical dilemmas regarding privacy, human rights, and societal structures. To address these challenges, ethical frameworks and regulations must evolve in parallel with technological advancements to safeguard privacy, security, and sustainability.

- Digital ethics.
- Quantum computing.
- Robotics and automation.
- Biotechnology.

2.11. Emerging technologies

Emerging technologies refer to innovations that are currently being developed or are expected to be available in the near future. These technologies have the potential to revolutionize various fields such as healthcare, education, transportation, and entertainment. In the present study, emerging technologies have a significant impact on the commodification of personal data in the digital economy, as they enable the collection, processing, and utilization of vast amounts of data.

One such emerging technology is blockchain. Blockchain is a decentralized digital ledger that provides a secure and transparent way to record transactions. It has the potential to transform various industries, including finance, healthcare, and supply chain management. In the present study, blockchain can be used to ensure the security and privacy of personal data, while also enabling its sharing and monetization [64,65].

Another emerging technology that has significant implications for personal data is artificial intelligence (AI). AI refers to machines that can perform tasks that would typically require human intelligence, such as image recognition, natural language processing, and decision making. In the present study, AI can be used to analyze personal data and extract valuable insights, which can be used for targeted advertising, product development, and other purposes [66].

A third emerging technology that is relevant to your article is the Internet of Things (IoT). IoT refers to the network of physical devices, vehicles, home appliances, and other items that are embedded with sensors, software, and network connectivity. This network enables the collection and sharing of vast amounts of data, which can be used to optimize various processes and services. In the present study, IoT can be used to collect personal data from various sources, which can be used to create targeted advertising and personalized services [67].

Finally, virtual and augmented reality (VR/AR) technologies are also emerging technologies that have significant implications for personal data. VR/AR technologies enable immersive experiences that blur the line between the digital and physical worlds. In the present study, VR/AR technologies can be used to collect personal data on users' preferences and behaviors, which can be used to develop targeted advertising and personalized experiences [68].

It is essential to consider the ethical and privacy implications of these technologies, as well as their potential benefits, in order to develop policies and regulations that can ensure their responsible and sustainable use.

Some of the key emerging technologies that are currently making waves in the digital economy include:

1) Digital ethics [69]:
   - In the context of the article, digital ethics refers to the ethical considerations related to the commodification of personal data in the digital economy. It involves analyzing the impact of personal data collection, use, and dissemination on privacy, security, and human rights.
   - The deployment of 5G networks will enable faster and more efficient data processing and transmission, which could accelerate the commodification of personal data. It is important to consider the implications of 5G for privacy, security, and human rights.
2) Quantum computing [70]:
   - Quantum computing has the potential to significantly increase the speed and efficiency of data processing, which could have both positive and negative implications for privacy and security. It is important to consider the ethical implications of quantum computing in the context of the commodification of personal data.
3) Robotics [71]:
   - Robotics and automation are increasingly being used to collect and process personal data in various contexts, such as surveillance and targeted advertising. It is important to consider the ethical implications of these technologies for privacy and human rights.
4) Biotechnology [72]:
   - Biotechnology is increasingly being used to collect and analyze personal data related to health and genetics. This raises significant privacy and security concerns, as well as ethical questions related to the use of this data.
5) Other emerging technologies [73]:
   - There are numerous other emerging technologies that are relevant to the commodification of personal data, such as virtual and augmented reality, edge computing, and nanotechnology. It is important to consider the ethical implications of these technologies and their potential impact on privacy, security, and human rights.

2.12. The digital economy and emerging technologies

As technological advancements progress through the waves, they increasingly impact society, particularly in the digital economy. This has profound implications for data privacy, ethical standards, and future innovation.

1) The growing role of data in the digital economy:

In the X.0 framework, data has become a key asset. Its commodification raises ethical issues surrounding privacy, security, and trust—especially in the context of a "post-truth" world where societal trust is diminishing. As data-driven technologies advance, the impact on markets and the need for stringent privacy regulations will become even more pronounced.

2) Emerging technologies and their impacts on data commodification:

Emerging technologies are critical in shaping the way personal data is collected, processed, and utilized. Blockchain, AI, IoT, and VR/AR technologies all influence data privacy and how data is commodified, creating new opportunities and risks.

- Blockchain: Ensures data security and transparency, potentially creating a safer framework for sharing and monetizing personal data.
- Artificial intelligence: AI analyzes vast amounts of personal data to derive valuable insights for targeted advertising and other applications.
- Internet of Things (IoT): IoT collects personal data through connected devices, influencing personalized services and targeted marketing.
- Virtual and augmented reality (VR/AR): VR/AR technologies allow for immersive experiences that collect personal preferences and behaviors to further drive personalized advertising.

3) Ethical and privacy considerations:

While these technologies offer immense potential, their widespread implementation also brings significant privacy risks. Policymakers must develop regulations that balance the benefits of emerging technologies with the protection of individual rights and societal values.

2.13. Summary

The X.0 Wave Theory provides a comprehensive framework to understand humanity's technological evolution. By following the progression from early agriculture to the emerging fusion of technology and human biology, the theory offers valuable insights into the societal implications of each technological shift. As future waves unfold, it will be crucial for governments, industries, and individuals to proactively address the ethical, social, and environmental implications of these advancements, ensuring that progress benefits humanity as a whole.

3. Research method (materials and methods)

This research follows a mixed-methods approach, incorporating both qualitative and quantitative phases. The study is applied in nature, with a descriptive survey design, drawing on a Deductive-Inductive framework. The qualitative stage utilizes thematic analysis, while the quantitative phase employs the Fuzzy Delphi method to verify the results from the qualitative phase.

Qualitative phase:

The qualitative phase of the research is centered around the thematic analysis of relevant texts and semi-structured interviews. The thematic analysis was conducted in three stages: Text analysis, text description, and text combination. This approach helped identify and categorize the key concepts and themes related to the commodification of personal data.

The research began by reviewing relevant texts to extract initial themes, which were further developed through in-depth interviews with participants. These interviews were semi-structured, allowing flexibility to explore emerging topics. The thematic analysis of the interview data was carried out using NVivo 12 software, which assisted in the identification of major themes and the construction of thematic networks.

The reliability and validity of the data were assessed using the CVR coefficient (Content Validity Ratio) and Cohen's Kappa test. The results are shown in **Table 3**, indicating satisfactory validity and reliability.

Table 3. Validity and reliability in the qualitative section.

Reliability		**Validity**	
Value	The tool used	Value	The tool used
0.776	Cohen's Kappa	0.51	CVR coefficient

In the quantitative stage, in order to confirm the results of the qualitative analysis, Fuzzy Delphi method was used. This method was carried out to confirm the results of qualitative analysis and determine the antecedents and consequences of commoditization of personal data in the digital economy, and the most important factors and consequences of commoditization of personal data were determined. The Delphi method includes a type of group process that emphasizes the mutual relationship between the researcher and a group of experts, and experts' opinions are usually collected through a questionnaire. Therefore, in the present study, a Fuzzy Delphi questionnaire was designed and sent to academic and organizational experts for their opinion. The statistical population of the current research included 14 business and university sustainability experts and specialists in the qualitative phase, and 23 business and university experts in the quantitative phase, who were selected using a targeted sampling method. Based on the principle of data sufficiency, up to the stage of theoretical saturation, data and information needed for the research were collected through interviews. The general questions of the interview included the factors, antecedents and consequences related to the commodification of personal data in the digital economy. On the other hand, in the quantitative stage, using the results of the qualitative stage and the opinions of experts in the field of antecedents and consequences of personal data commodification, a Fuzzy Delphi questionnaire was designed and sent to the relevant experts. Finally, using the TRIZ model and the three pillars of idealism, conflict seeking, and sourcing from its 5 intellectual pillars, based on the antecedents and consequences of commodification of personal data, we will give examples related to mathematical modeling.

3.1. Research findings

In this section, qualitative analysis using theme analysis in NVivo 12 software will be discussed first. Then quantitative analyzes are performed using Fuzzy Delphi technique.

3.1.1 Findings of the qualitative stage

In the qualitative phase, in order to identify the antecedents and consequences of commoditization of personal data in the digital economy, relevant subjects were identified from the review and analysis of texts and semi-structured interviews. In this way, first, the texts related to personal data commodification were analyzed. Based on that, the interview questions were designed and after providing the necessary explanations to the interviewees, the interview process was carried out. Then, the interview texts were analyzed using the theme analysis method and with the help of

NVivo 12 software. After analyzing the texts and conducting interviews, the basic themes were extracted. The antecedents and consequences of personal data commoditization based on basic topics are stated in the table. According to the **Table 4**, the antecedents obtained from the analysis of texts and semi-structured interviews include 22 basic topics. Also, the consequences include 11 positive and negative consequences that can be seen in the table.

Table 4. Antecedents and consequences of personal data commodification.

Consequences		**Antecedents**			
Factors	**code**	**Factors**	**code**	**Factors**	**code**
Make informed choices about personal information	C1	transparency	A12	Free online service	A1
Protection of personal data & preventing anti-competitive practices	C2	responsiveness	A13	online shopping	A2
Socio-cultural consequences and a tool for discrimination	C3	Regulatory and policy frameworks	A14	Social media and mobile applications	A3
Economic implications and a tool for targeted advertising	C4	Support for stronger regulations	A15	Advanced technology such as artificial intelligence and the Internet of Things	A4
Legal implications and privacy violations	C5	Technical solutions for privacy security	A16	Velvet revolutions	A5
Ethical consequences, reduction of security, reduction of satisfaction and reduction of public trust	C6	Informing the community	A17	The intersection of hybrid and cognitive warfare	A6
Trap and hidden costs, misuse and exploitation of personal data	C7	Hollywood cinema & Domination cinema	A18	Dis-Information, Mis-information & Mal-Information	A7
Establishing a supervisory capitalist system	C8	Social movements and youth Internet and social media	A19	Independent political groups	A8
Identity theft and the change of human relations towards an exploitative relationship between users and the digital economy	C9	Elite	A20	NGOs	A9
Changing human perception	C10	Supporting alternative business models	A21	Antitrust and data protection laws and regulations	A10
Perception input for children and posterity	C11	Human perception	A22	Human information	A11

3.1.2. Findings of the quantitative stage

After analyzing various texts and conducting a semi-structured interview using NVivo 12 software, 33 themes were identified in the form of antecedents and consequences of commoditization of personal data. Fuzzy Delphi method was used to check the validity of the identified topics. The subjects counted were designed in the form of a Fuzzy Delphi questionnaire with the aim of obtaining the opinion of experts. The relevant experts express their level of agreement through verbal variables very little, little, medium, much and very much. Then, these variables are defined as triangular Fuzzy numbers. The **Table 5** shows how to convert verbal variables into triangular Fuzzy numbers and deterministic Fuzzy numbers.

Quantitative phase:

To validate the findings from the qualitative analysis and identify the antecedents and consequences of the commodification of personal data, the Fuzzy Delphi method was applied in the quantitative phase. The Delphi method is a structured

communication process in which expert opinions are gathered through a questionnaire to form a consensus.

In this research, a Fuzzy Delphi questionnaire was designed based on the themes identified in the qualitative phase. The questionnaire was distributed to 23 business and university experts, selected through targeted sampling. The questionnaire aimed to gather expert opinions regarding the key antecedents and consequences of commodifying personal data in the digital economy.

To calculate Fuzzy averages from expert opinions, verbal responses (ranging from "very low" to "very much") were converted into triangular Fuzzy numbers. The process was as follows:

Table 5. Triangular Fuzzy numbers and definitive numbers.

De-fuzzified value	Triangular Fuzzy number	Verbal variables
0.0625	(0, 0, 0/25)	very low
0.2500	(0, 0/25, 0/50)	Low
0.5000	(0/25, 0/50, 0/75)	Medium
0.7500	(0/50, 0/75, 1)	Much
0.9375	(0/75, 1, 1)	very much

It is worth mentioning that the de-fuzzified value was calculated using the relationship [74], which is stated below:

$$¼(a_{i1}, 2a_{i2}, a_{i3}) \quad (1)$$

Based on the above relationship, a_{i1}, the lower limit of the triangular Fuzzy number; a_{i2}, the middle limit of the triangular Fuzzy number; and a_{i3}, the upper limit of the triangular Fuzzy number.

A) First stage survey: Following the Fuzzy Delphi method, two stages of expert surveys were conducted. In the first stage, experts were asked to evaluate the relevance of identified themes. Based on their responses, the Fuzzy average for each theme was calculated. In the second stage, a comparative analysis was carried out to refine the results.

The **Table 6**, shows the Fuzzy average of each of the identified topics.

Table 6. The average opinion of experts in the first stage survey.

Fuzzy average	Codes	Fuzzy average	Codes	Fuzzy average	Codes
(0/53, 0/77, 0/90)	C1	(0/34, 0/59, 0/82)	A12	(0/38, 0/63, 0/88)	A1
(0/60, 0/85, 0/97)	C2	(0/45, 0/70, 0/89)	A13	(0/48, 0/73, 0/93)	A2
(0/52, 0/77, 0/95)	C3	(0/28, 0/50, 0/73)	A14	(0/43, 0/68, 0/88)	A3
(0/47, 0/72, 0/92)	C4	(0/40, 0/65, 0/87)	A15	(0/40, 0/65, 0/87)	A4
(0/58, 0/83, 0/93)	C5	(0/34, 0/59, 0/82)	A16	(0/48, 0/73, 0/90)	A5
(0/52, 0/78, 0/92)	C6	(0/32, 0/54, 0/78)	A17	(0/73, 0/72, 0/89)	A6
(0/50, 0/75, 0/89)	C7	(0/40, 0/65, 0/88)	A18	(0/50, 0/75, 0/90)	A7
(0/58, 0/83, 0/94)	C8	(0/52, 0/77, 0/95)	A19	(0/45, 0/70, 0/90)	A8
(0/48, 0/73, 0/88)	C9	(0/52, 0/77, 0/97)	A20	(0/47, 0/72, 0/90)	A9

Table 6. (*Continued*).

Fuzzy average	Codes	Fuzzy average	Codes	Fuzzy average	Codes
(0/49, 0/74, 0/93)	C10	(0/47, 0/72, 0/93)	A21	(0/42, 0/67, 0/87)	A10
(0/45, 0/70, 0/84)	C11	(0/44, 0/69, 0/90)	A22	(0/47, 0/72, 0/88)	A11

After the end of the first stage survey, it is necessary to conduct the second stage survey so that the results obtained from both stages can be compared and the result determined.

B) Second stage survey: In the second stage survey, as in the first stage, the answers given to the topics are counted and their Fuzzy average is calculated. The **Table 7**, shows the relevant values for the Fuzzy average.

Table 7. The average opinion of experts in the second stage survey.

Fuzzy average	Codes	Fuzzy average	Codes	Fuzzy average	Codes
(0/60, 0/85, 0/99)	C1	(0/54, 0/79, 0/98)	A12	(0/35, 0/60, 0/80)	A1
(0/59, 0/84, 0/97)	C2	(0/54, 0/79, 0/97)	A13	(0/64, 0/80, 0/97)	A2
(0/60, 0/85, 0/98)	C3	(0/29, 0/54, 0/79)	A14	(0/49, 0/74, 0/92)	A3
(0/55, 0/80, 0/92)	C4	(0/50, 0/75, 0/97)	A15	(0/34, 0/58, 0/82)	A4
(0/67, 0/92, 0/98)	C5	(0/43, 0/68, 0/89)	A16	(0/55, 0/80, 0/95)	A5
(0/59, 0/84, 0/97)	C6	(0/35, 0/60, 0/84)	A17	(0/55, 0/80, 0/90)	A6
(0/59, 0/84, 0/94)	C7	(0/47, 0/72, 0/93)	A18	(0/58, 0/83, 0/95)	A7
(0/65, 0/90, 0/98)	C8	(0/52, 0/77, 0/87)	A19	(0/39, 0/64, 0/85)	A8
(0/59, 0/83, 0/92)	C9	(0/44, 0/68, 0/87)	A20	(0/55, 0/80, 0/94)	A9
(0/57, 0/82, 0/97)	C10	(0/57, 0/82, 0/94)	A21	(0/50, 0/75, 0/92)	A10
(0/52, 0/77, 0/98)	C11	(0/48, 0/72, 0/93)	A22	(0/54, 0/79, 0/95)	A11

The results showed that the differences between the first and second stages were minimal (less than 0.1), indicating expert consensus on the identified antecedents and consequences of personal data commodification. As a result, the data collection process was concluded.

Table 8 illustrates the difference between the de-fuzzified mean of the first and second stages of the survey, highlighting the minimal differences and the expert agreement on the antecedents and consequences of personal data commodification. This further reinforces the notion of data commodification as an increasingly accepted concept in today's digital economy, with implications for privacy, fairness, and transparency.

Table 8. The difference between the de-fuzzified mean of the first and second stage.

The difference between the average of the first and second stage	The de-fuzzified average of the first stage	The de-fuzzified average of the second stage	Codes
0.039	0.598	0.637	A1
0.067	0.791	0.724	A2
0.055	0.730	0.675	A3
0.065	0.587	0.652	A4

Table 8. (*Continued*).

The difference between the average of the first and second stage	The de-fuzzified average of the first stage	The de-fuzzified average of the second stage	Codes
0.069	0.787	0.718	A5
0.069	0.774	0.705	A6
0.047	0.805	0.758	A7
0.059	0.640	0.699	A8
0.075	0.783	0.708	A9
0.079	0.740	0.661	A10
0.074	0.777	0.703	A11
0.090	0.783	0.693	A12
0.086	0.779	0.696	A13
0.038	0.549	0.511	A14
0.087	0.752	0.665	A15
0.084	0.677	0.593	A16
0.056	0.608	0.552	A17
0.060	0.715	0.655	A18
0.021	0.737	0.758	A19
0.087	0.674	0.761	A20
0.078	0.793	0.715	A21
0.028	0.718	0.690	A22
0.084	0.833	0.749	C1
0.009	0.818	0.827	C2
0.072	0.830	0.758	C3
0.065	0.777	0.712	C4
0.078	0.877	0.799	C5
0.060	0.818	0.758	C6
0.078	0.811	0.733	C7
0.066	0.868	0.802	C8
0.087	0.799	0.712	C9
0.069	0.802	0.733	C10
0.082	0.765	0.683	C11

Based on the above table, the difference of the de-fuzzified average in the first and second stage is less than 0.1 and therefore the experts reached a consensus about the antecedents and consequences of personal data commoditization. At this point, the survey stops.

3.1.3. TRIZ model

To analyze and model the antecedents and consequences of the commodification of personal data, the TRIZ (Theory of Inventive Problem Solving) model was applied. TRIZ, developed by Altshuller, is a problem-solving methodology that emphasizes idealism, conflict resolution, and efficient use of resources.

TRIZ is a Russian problem-solving theory. The word TRIZ was given from Russian word "TEORIVA RESHENIVA IZOBRETA TELSKIKH ZADATCH" which means theory of Inventive Problem Solving. It was developed by Altshuller and his associates in a private section in the former Soviet Union in 1940s. Altshuller found out three main findings through his inventions and researches:

1) Problems and solutions are repeated across industries and sciences.
2) Patterns of technical evolution are also repeated across industries and sciences.
3) The innovations used scientific effects outside the field in which they were developed.

In this research, using the TRIZ model and the three pillars of idealism, conflict seeking and sourcing from its 5 intellectual pillars, based on the antecedents and consequences of commodification of personal data, we will express examples related to mathematical modeling below.

- Idealism: The idealism of any system as one of the intellectual pillars of TRIZ is improved in three ways:
  a) Increasing useful functions;
  b) Reducing harmful practices or costs;
  c) A combination of the first and second ways [69].

Regarding the antecedents and consequences of personal data commodification, the formula of idealism is as follows:

$$\text{Idealism} = {}^{\text{useful functions}}/_{(\text{harmful practices} + \text{costs})} \quad (2)$$

Example: Protecting personal data and preventing anti-competitive practices leads to increased positive moral consequences, increased security, satisfaction and public trust, thereby increasing idealism.

- The concept of contradiction: If there is a contradiction between two characteristics of a system.

  Two methods can be used to solve the problem of contradiction:

  a) One way is to solve the contradictions and apply 40 creative principles and get some special suggestions to overcome these contradictions. Altshuler introduced 40 innovative principles that can be used to eliminate technical contradictions. He also presented 39 characteristics (parameters) of technical systems that can be used to develop and explain technical contradictions.
  b) The second way is to change the technical contradiction to the physical contradiction and remove this task at the physical level. To overcome the physical contradiction, the four physical principles and the database of physical effects and phenomena are used—Separation of contradictory properties in time—Separation of contradictory properties in space—Separation of components—Change of phase or change of chemical-physical form of materials (separation dependent on conditions) Technical inconsistencies are generally related to the properties of the entire technical system, but physical inconsistencies are related to the physical properties of an element of a system.

Example: Although online and free services are considered a very attractive option, they cause traps and hidden costs and abuse and exploitation of personal data.

- Sourcing: According to TRIZ, resources are divided into two general categories:
    a) Physical resources: such as energy materials and environmental effects, information, time, space and systems performance.
    b) Human resources: such as skills, knowledge, experiences, behavior, feelings and perceptions.

  The purpose of TRIZ is to maximize the use of resources.

  Example: Using technology solutions to protect privacy.

4. Case studies

In the digital economy, personal data is a valuable commodity that fuels innovation, markets, and profits. However, the collection, processing, and sharing of personal data also raise ethical, legal, and social concerns, especially in a post-truth world where facts, opinions, and emotions can be manipulated and weaponized.

To shed light on the true price of 'free', we can look at several case studies. Each of these case studies can provide examples of how companies, organizations, NGOs, and governments are dealing with the commodification of personal data in the digital economy, and can highlight the main points, reasons, and consequences of their actions or initiatives.

In addition to these case studies, it's also important to consider the implications of the rise of "velvet revolutions", hybrid warfare, and cognitive warfare in the digital age. [70] These phenomena are characterized by the use of social media and other digital platforms to manipulate public opinion, spread disinformation, and destabilize governments and societies.

For example, the 2014 Euromaidan revolution in Ukraine was fueled in part by social media, which enabled protesters to coordinate and communicate in real time. However, social media has also been used to spread disinformation and sow discord, as seen in the 2016 US presidential election and other examples of election interference around the world.

Similarly, hybrid warfare and cognitive warfare involve the use of a wide range of tactics, including propaganda, cyber-attacks, and psychological operations, to achieve political or military objectives. These tactics can have far-reaching consequences, including the erosion of public trust in institutions and the amplification of extremist voices.

These examples underscore the need for greater transparency, accountability, and regulation in the digital economy, as well as the importance of protecting personal data and promoting ethical practices in the use of technology.

4.1. Here are some case studies from Silicon Valley

1) Uber: Uber is a ride-sharing company that connects riders with drivers through a mobile app. Uber collects personal data from users and drivers to provide its services and improve its operations. However, Uber has faced criticism for its handling of user data, including a 2016 breach that exposed the personal information of millions of users and drivers. The breach led to multiple

investigations and lawsuits against Uber, as well as increased public scrutiny of its data practices.

2) Apple: Apple is a technology company that produces a range of products, including smartphones, tablets, and computers. Apple collects personal data from users to provide services and improve its products, but has taken a strong stance on user privacy. For example, Apple's iOS mobile operating system includes features that limit data collection and tracking by third-party apps. Apple has also refused to comply with requests from law enforcement to provide access to encrypted user data, citing privacy concerns.
3) Palantir: Palantir is a data analytics company that provides software and services to government agencies and corporations. Palantir's software is used to analyze and visualize large amounts of data, including personal data. Palantir has faced criticism for its involvement in government surveillance programs and its lack of transparency about its data practices. The company has also been accused of facilitating human rights abuses in countries like Qatar and the United Arab Emirates.

Regarding velvet revolutions, hybrid warfare, and cognitive warfare, it may be helpful to focus on how personal data is used in these contexts. For example, social media platforms have been used to spread disinformation and propaganda in attempts to influence political outcomes. In addition, personal data may be used to target individuals with tailored messaging designed to manipulate their beliefs and behaviors. Understanding how personal data is used in these contexts is crucial for addressing the broader implications of commodifying personal data.

4.2. Google's advertisement and announcement for JOB

- Google's advertisement and announcement for JOB, which stated "You do not need a CV and application because we already know you", can be analyzed as a case study in the commodification of personal data and its impact on the job market.

Figure 7 illustrates Google's advertisement and announcement for JOB, emphasizing the growing role of personal data in shaping the job market. This case study sheds light on several critical points, particularly in the context of personal data commodification, as explored in the X.0 Wave theory. The announcement reveals how personal data is increasingly treated as a valuable commodity, used to match job seekers with opportunities without the need for traditional CVs or applications. This underscores the broader shift from human-driven processes to data-driven automation, raising questions about the diminishing role of privacy in the digital economy, the accuracy and transparency of algorithms, and the hidden costs of 'free' services that often come at the expense of our personal information.

Figure 7. Google's advertisement and announcement for JOB [75].

Some of the key points to consider in this case study include [75–95]:

1) Personal data as a commodity: The announcement implies that Google has already collected and analyzed a vast amount of personal data on job seekers, such as their search history, online behavior, and social media activity. This data is treated as a valuable commodity that can be used to match candidates with job opportunities without requiring a traditional CV or application.
2) Automated algorithms: The use of automated algorithms to match candidates with job opportunities raises questions about the role of human recruiters and the potential for bias or discrimination in the hiring process. Additionally, it raises concerns about the accuracy and transparency of the algorithms used to evaluate job candidates.
3) Impact on job market: The announcement has the potential to disrupt the traditional job market by reducing the role of human recruiters and creating a more automated and data-driven hiring process. This may have implications for job seekers who lack a strong online presence or whose personal data may not accurately reflect their qualifications or experience.
4) Privacy concerns: The announcement raises privacy concerns about the collection, storage, and use of personal data by companies like Google. Job seekers may not be fully aware of the extent of their personal data that is being collected or how it is being used to evaluate their job candidacy.

Google's announcement for JOB highlights the growing role of personal data in the job market and raises important questions about the implications for privacy, bias, and automation in the hiring process.

4.3. The Cicada example is a mysterious organization called Cicada 3301

Figure 8. Cicada 3301 (AI-generated image). Created by DeepAI, January 21, 2025, 11:55 AM.

Figure 8 showcases the mysterious entity known as Cicada 3301, which began posting intricate puzzles online in 2012. The organization aimed to recruit individuals with exceptional intelligence by offering increasingly complex challenges that required advanced skills in cryptography and steganography. As participants progressed, they were prompted to submit sensitive personal information, such as photos and even DNA samples, under the guise of identity verification. While the true motive behind the puzzles remains unknown, the case highlights the dangers of sharing private information online, particularly when the intentions of those requesting it are unclear.

The Cicada example is a case study that highlights the potential dangers of sharing personal information online. In 2012, a mysterious organization called Cicada 3301 began posting puzzles on various online forums, claiming to be seeking individuals with exceptional intelligence and problem-solving skills. The puzzles led to a series of increasingly difficult challenges, with participants being asked to use their knowledge of cryptography, steganography, and other technical fields to decipher clues and solve puzzles.

As the challenges progressed, participants were asked to submit increasingly detailed personal information, including photographs, voice recordings, and even DNA samples. The organization claimed that this was necessary to verify the identities of successful candidates, but many participants became concerned about the level of personal information they were being asked to share.

Despite the concerns, many individuals continued to participate in the challenges, drawn in by the allure of a secretive organization seeking out the world's brightest minds. However, it is unclear what ultimately happened to those who successfully completed the challenges, and many experts have warned that the organization may have been collecting personal information for nefarious purposes.

The Cicada example illustrates the potential dangers of sharing personal information online, particularly when it is requested by individuals or organizations with unknown motivations. It underscores the importance of being cautious about the information we share online and being aware of the risks involved in participating in online activities that require the sharing of personal information.

5. Results and discussion

The article discusses three key topics that have become increasingly relevant in recent years. There are three key points that are essential in understanding the impact of personal data commodification on innovation, markets, and privacy.

1) Firstly, it is crucial to beware of products marketed as "free" as they are designed to use individuals as commodities rather than provide genuine benefits. this point discussed in this article is the need to beware of products marketed as "free". These products are designed to exploit individuals as commodities rather than provide genuine benefits. For example, social media platforms offer free services to users, but in reality, they collect personal data that is used for targeted advertising and other purposes [75–95].
2) Secondly, the article examines the impact of the "velvet revolution" on personal data commodification, highlighting the emergence of new market players

prioritizing data privacy and transparency, leading to increased competition and potentially, more innovation in this area. this point discussed in this article is the impact of the velvet revolution on personal data commodification. The emergence of new market players prioritizing data privacy and transparency has forced traditional players to adapt, leading to increased competition and potentially, more innovation in this area. This has resulted in greater awareness and demand for greater control over personal data [87].

3) Lastly, the article explores the intersection of "Hybrid Warfare, Cognitive Warfare, and disinformation warfare" with information disorder, which is used to control social and cultural capital, highlighting the significant erosion of privacy and trust in institutions. this point discussed in this article is the intersection of Hybrid Warfare, Cognitive Warfare, and disinformation warfare with information disorder. These tactics have been used to manipulate public opinion and collect personal data, eroding privacy and trust in institutions. This highlights the need for greater regulation and control over personal data in the digital economy [88].

Personal data commodification in the digital economy has significant implications for innovation, markets, and privacy. The lack of transparency and control over personal data by individuals raises ethical concerns regarding privacy and consent. It is essential for individuals to have greater control over their personal data, and for companies and organizations to be more transparent about their data collection and use practices. Policymakers must consider the implications of personal data commodification on innovation, markets, and privacy, and take appropriate actions to mitigate any negative consequences.

The research findings indicate that personal data is being commodified by companies and organizations, and this has implications for innovation, markets, and privacy in a post-truth world. The analysis of case studies in Silicon Valley, as well as other examples such as Cicada and international HR research, demonstrate how personal data is being used to target advertising, recruit employees, and even influence political outcomes. The use of surveys and interviews as primary data sources, as well as secondary data sources such as books, articles, and company reports, provided insights into the current state of personal data commodification.

(1) The value of personal data, as a valuable commodity in the digital age: In the digital age, personal data has become a valuable commodity. Governments, intelligence services, companies, and organizations collect and use personal data for various purposes such as market research, targeted advertising, and product development. Personal data can also be used for political or social control. This has raised concerns about data privacy and the need for regulations to protect individuals' personal information [88–92].

(2) The commodification of personal data: The commodification of personal data involves companies offering free digital products or services to consumers while collecting their personal data for profit. This has become a common practice in the digital economy. Companies use personal data to create targeted advertisements, improve their products and services, and sell data to third-party vendors. However, this has also resulted in a loss of privacy for individuals and the potential for misuse of personal data [89].

(3) Implications for innovation and markets: The commodification of personal data has implications for innovation and markets. Companies that collect personal data can use it to improve their products and services, which can lead to innovation. However, the use of personal data can also result in a lack of competition, as larger companies with more access to data can dominate the market.

(4) Implications for privacy: The commodification of personal data has significant implications for privacy. Companies collecting personal data must adhere to privacy laws and regulations to ensure that individuals' personal information is protected. However, these laws are often inadequate, and companies may not always be transparent about their data collection practices. This has resulted in a loss of privacy for individuals and the potential for misuse of personal data [88].

(5) The post-truth world:
- It is crucial to, beware of products that appear to be 'free': Free cheese can only be found in the mousetrap. In the post-truth world, it is crucial to be aware of products that appear to be "free". They are not intended for your benefit, but rather to exploit you as a commodity. The commodification of personal data has also facilitated the spread of disinformation, as companies can use personal data to target individuals with specific political views or beliefs.
- The 'velvet revolution': The commodification of personal data has facilitated a "velvet revolution", where individuals' personal information is used to control social and cultural capital. This has resulted in the manipulation of public opinion, the spread of disinformation, and the erosion of democracy.

(6) The 'hybrid, cognitive, and disinformation warfare with information disorder': The commodification of personal data intersects with hybrid, cognitive, and disinformation warfare, which is used to control social and cultural capital. This has significant implications for the manipulation of public opinion and the spread of disinformation.

(7) X.0 Wave/Age Theory, and related theories, models, and methods and concepts
- X.0 Wave/Age Theory: The X.0 Wave/Age Theory describes the evolution of technology and its impact on society. It proposes that new technologies create waves of change, with each wave building on the previous one. The theory suggests that we are currently in the fourth wave, the "Digital Age", characterized by the commodification of personal data.

(8) The Seven Pillars of Sustainability (7PS) model: In the context of my article on the commodification of personal data in the digital economy, the 7PS model can provide a useful framework for exploring the broader implications of this trend and developing strategies for promoting sustainable and ethical practices.
- Seven Pillars of Sustainability Model (7PS) and Its connection to the research findings

The Seven Pillars of Sustainability (7PS) model provides a framework to address the commodification of personal data in the digital economy. Each pillar represents a critical area that contributes to long-term sustainability while reflecting on the hidden costs and implications raised in the research findings.

1) Economic sustainability: Digital platforms often exploit user data for profit without fair compensation. A sustainable digital economy must ensure transparency, equitable value creation, and user control over personal data.
2) Social sustainability: The commodification of personal data can lead to inequality, discrimination, and privacy violations. Sustainability in this context requires systems that foster fairness, inclusivity, and respect for user autonomy.
3) Environmental sustainability: Data-driven technologies contribute to ecological harm through excessive energy consumption and e-waste. Sustainable practices call for greener technologies and data management systems to minimize environmental impact.
4) Cultural sustainability: Personalization algorithms can limit exposure to diverse content, affecting cultural diversity. A sustainable digital culture should prioritize variety and freedom of expression.
5) Ethical sustainability: Ethical concerns around privacy and consent in the digital economy must be addressed. An ethical framework should protect individual rights and promote transparency in how personal data is used.
6) Institutional sustainability: Governments and regulators need to create policies that protect user data while ensuring fairness and accountability in the digital economy.
7) Technological sustainability: Technological innovation must respect human rights and reduce risks like security breaches and algorithmic bias. Sustainable technology should align with the well-being of society.

Core values: Peace and love

The core values of peace and love are integral to the 7PS model, guiding the development of sustainable practices in the digital economy. Peace emphasizes harmony, fairness, and respect for all individuals, advocating for systems that reduce harm and promote trust. Love fosters empathy, inclusivity, and the prioritization of human dignity. These values call for a digital world where both technological and social advancements are grounded in the well-being of all people, ensuring that the commodification of data does not come at the expense of individual rights or societal equity.

(9) Commodification of personal data in the digital economy

The commodification of personal data is the process of turning personal information into a commodity that can be bought and sold in the digital economy. In the digital age, personal data has become an essential part of the economy, with companies and organizations collecting and using this information for various purposes. Personal data has become an integral part of business models for social media platforms, search engines, and other online services, where users' personal data is collected and analyzed to create targeted advertising and personalized content. However, the commodification of personal data raises significant concerns about privacy, security, and individual rights. The lack of transparency in how companies collect and use personal data has led to growing public concern over the risks and potential harm associated with the commodification of personal data [88].

The findings suggest that there is a need for greater awareness and regulation of personal data commodification, particularly in the digital economy. It is important for

individuals to have greater control over their personal data, and for companies and organizations to be more transparent about their data collection and use practices. Moreover, policymakers must consider the implications of personal data commodification on innovation, markets, and privacy, and take appropriate actions to mitigate any negative consequences [75–100].

(10) Potential biases, methodological limitations, and generalizability

- Potential biases

This study aims to provide an objective and unbiased analysis of the commodification of personal data in the digital economy. However, there may be potential biases in the selection of sources and methodologies used. The choice of specific sources or emphasis on particular aspects of the topic could inadvertently influence the results. To mitigate these effects, efforts have been made to use a diverse range of credible sources and consider multiple viewpoints. Nonetheless, it is important for researchers to acknowledge that results may still be influenced by individual or scholarly biases.

- Methodological limitations

The methods employed in this research include Fuzzy Delphi, thematic analysis, and the TRIZ Algorithm, each with its own advantages and limitations. One limitation of this study is the reliance on qualitative data and theoretical analyses, which may impact the accuracy of the results due to the lack of empirical data. Additionally, the use of theoretical models like the X.0 Wave/Age Theory may limit predictive accuracy due to the absence of comprehensive statistical data. To enhance the precision of findings, future research could benefit from incorporating empirical data and quantitative analysis methods.

- Generalizability of findings

The results of this study address the hidden costs of personal data commodification in the digital economy and its implications for markets and privacy. However, the generalizability of these findings to other contexts and geographies may be limited. Cultural, legal, and economic differences across countries can lead to varying impacts of personal data commodification. Therefore, the findings of this study may not be directly applicable to other countries or industries. To improve generalizability, further research with broader samples and across different contexts is recommended.

5.1. Challenges and solutions

5.1.1. Challenges

The commodification of personal data poses several challenges that must be addressed to ensure the protection of privacy and autonomy.

Challenge 1: Lack of knowledge and understanding among individuals about their personal data

The lack of transparency and education about personal data use has led to high rates of personal data collection and use without individuals' knowledge or consent. This lack of understanding can result in individuals unwittingly giving away their personal data without being fully aware of the consequences. Consequently,

individuals may experience a loss of privacy and autonomy, as well as a potential for misuse of their personal data.

Challenge 2: Complexity and diversity of the digital economy

The digital economy is complex and diverse, making it difficult to develop uniform regulations that effectively address personal data commodification. Varying approaches to personal data collection and use across different sectors and regions, as well as differences in industry practices and technologies, cultural and legal variations have made it challenging to develop a common regulatory framework. Inconsistent regulations may lead to confusion and noncompliance, while regulations that are too strict may stifle innovation and hinder the growth of the digital economy.

5.1.2. Solutions

To address the challenges of personal data commodification, several solutions can be implemented [75–100].

1) Firstly, greater education and awareness-raising efforts are required to make individuals more informed about their personal data and how it is being used by companies and organizations. This could involve incorporating digital literacy and data privacy education into school curriculums and public awareness campaigns.
2) Secondly, policymakers should engage in ongoing discussions with stakeholders and experts to develop regulations that balance the need for innovation and economic growth with the need for privacy and protection of personal data. The regulations should be designed to provide a framework that guides companies and organizations in collecting and using personal data while respecting individuals' privacy rights.
3) Thirdly, companies and organizations should be more transparent about their data collection and use practices. This would enable individuals to make informed decisions about whether to share their personal data and with whom.

The solution to personal data commodification requires a collaborative effort between individuals, companies, organizations, and policymakers. By working together, we can create a digital economy that is both innovative and ethical, and that respects the privacy and autonomy of individuals.

6. Conclusion and future suggestions

6.1. Conclusion

The commodification of personal data in the digital economy has profound implications for innovation, markets, and privacy. Through the analysis using X.0 Wave/Age Theory, the following conclusions can be drawn:

1) Awareness and education: A primary factor driving the commodification of personal data is the lack of awareness about its value and risks. To combat this, individuals must be educated on the importance of their personal data and how it can be misused.
2) Role of governments: Governments must take an active role in raising awareness, implementing regulations, and promoting digital literacy to protect individuals

from the risks of data commodification. Policy interventions should safeguard privacy and ensure transparency in how personal data is used.

3) Sustainable skills, training, and workshop: Equipping individuals with the necessary skills to manage and control their personal data is vital. Training programs can empower people to make informed decisions about data sharing and safeguard their privacy.
4) Learning from the past: Identifying and examining the patterns, by drawing lessons from past events and frameworks, such as the "free cheese and mousetrap" metaphor, hybrid warfare, and disinformation campaigns, is essential for predicting and preventing the challenges related to personal data commodification.

The research highlights that personal data commodification poses significant threats to privacy, innovation, and market fairness. Greater awareness, stronger regulations, and enhanced transparency are necessary steps toward ensuring that individuals retain control over their data. Policymakers and stakeholders must recognize the urgency of addressing this issue to protect consumers and maintain ethical standards in the digital economy.

To address the challenges of personal data commodification, there are several future suggestions that can be considered. Firstly, individuals must be empowered with greater control over their personal data through education, awareness-raising, and digital literacy programs. Secondly, companies and organizations must be more transparent about their data collection and use practices and implement ethical data management policies. Thirdly, policymakers should engage in ongoing discussions with stakeholders and experts to develop balanced regulations that promote innovation and economic growth while safeguarding personal data privacy.

In terms of future research, there is a need for further exploration of the impact of personal data commodification on innovation and markets, particularly in terms of its potential impact on competition and consumer choice. Additionally, there is a need for greater understanding of the potential unintended consequences and biases of advanced technologies such as artificial intelligence and machine learning on the analysis of personal data.

The commodification of personal data is a complex issue that requires a multi-faceted approach to address. It is essential that all stakeholders work collaboratively towards a digital economy that is both innovative and ethical, and that respects the privacy and autonomy of individuals.

In conclusion, the commodification of personal data has significant implications for innovation, markets, and privacy in a post-truth world. The adoption of X.0 Wave/Age Theory and the examination of the velvet revolution, Hybrid Warfare, and Cognitive Warfare highlight the need for greater awareness and control over personal data. As we move forward, it is crucial that individuals and institutions work together to ensure the protection of personal data and the preservation of privacy.

"The 5th wave theory"—Expected Impact Through the support of innovation, entrepreneurship and university-business cooperation. One of the key priorities for Higher Education is the reinforcement of the "Knowledge Triangle", through the support of innovation, entrepreneurship, and university-business cooperation.

As shown in **Figure 9**, the Knowledge Triangle, which emphasizes the integration of innovation, entrepreneurship, and university-business cooperation, plays a crucial role in fostering the environment needed to address the challenges of personal data commodification and promote ethical digital economies.

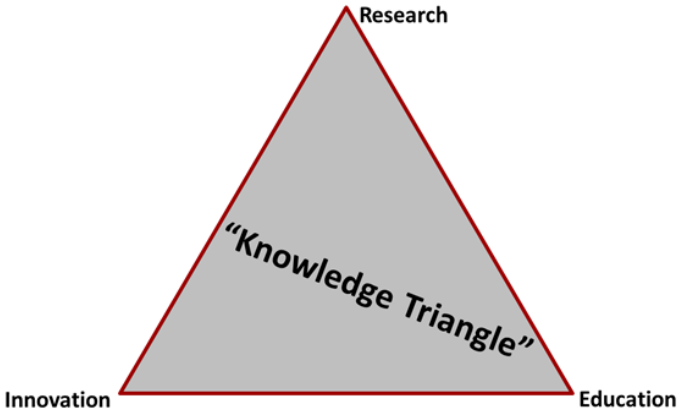

Figure 9. Knowledge Triangle and Expected Impact of the X.0 Wave/Age Theory [100].

6.2. Future suggestions

Based on my research findings, the following actionable recommendations for policymakers and digital economy stakeholders, the following suggestions are provided [75–100]:

1) Increase Transparency and Public Awareness;
2) Implement Stricter Data Protection Regulations;
3) Empower Consumers with Control over Their Data;
4) Encourage Ethical Business Practices;
5) Support the Development of Decentralized Data Platforms;
6) Foster Collaboration between Industry and Academia;
7) Invest in Privacy-Enhancing Technologies;
8) Create International Norms for Data Protection;
9) Enhance Cybersecurity Practices;
10) Develop New Business Models that Prioritize Privacy;
11) Provide Education on Digital Literacy;
12) Promote Data Security and Privacy Legislation;
13) Encourage Adoption of Privacy-Respecting Technologies;
14) Support Consumer Empowerment Initiatives;
15) Initiate Public Awareness Campaigns about Hidden Costs;
16) Implement Multidisciplinary Approaches.

These future suggestions aim to guide policymakers, businesses, and other stakeholders in addressing the challenges associated with personal data commodification while ensuring innovation, privacy, and ethical practices in the digital economy.

The following recommendations aim to address the challenges of personal data commodification and support a more ethical and sustainable digital economy [2,14,15,52,55,56,88–90]:

1) Increased transparency and education: It is crucial to educate individuals on the importance of their personal data and its value. We need to promote transparency from companies about their data collection practices, provide consumers with more control over their data, and offer education on how to protect their privacy.
2) Stricter data protection laws: Governments need to enact more comprehensive data protection laws that protect individuals' privacy rights and ensure that companies adhere to ethical and responsible data practices. This will help to restore trust in the digital economy and protect consumers from harm.
3) Development of decentralized data platforms: The development of decentralized data platforms that empower individuals to own and control their data is an important step towards protecting personal privacy. Blockchain-based technologies can be used to create secure, decentralized data platforms that give users control over their data and allow them to monetize it on their terms.
4) Investment in privacy-enhancing technologies: There is a need for more investment in privacy-enhancing technologies that can help protect individuals' privacy online. Examples include encrypted messaging apps, ad-blockers, and VPNs that can help protect personal data from being collected and exploited.
5) Collaboration between industry and academia: Collaboration between industry and academia can help advance our understanding of data privacy issues and develop new solutions to address them. This can include partnerships between tech companies and universities to develop new privacy-enhancing technologies and research initiatives that explore the social, economic, and political implications of data commodification.
6) Encouraging government regulation: Governments need to play a more active role in regulating the digital economy to protect individuals' privacy and personal data. This can be achieved through implementing laws and policies that mandate companies to be transparent about their data collection practices and provide individuals with more control over their personal information.
7) Increasing public awareness: The general public needs to be educated about the true cost of "free" digital services and the ways in which their personal data is being commodified. This can be achieved through awareness campaigns, public education programs, and media outreach.
8) Developing new business models: Companies should consider adopting new business models that do not rely on the commodification of personal data. For example, subscription-based models that offer paid access to ad-free platforms or services can be explored.
9) Improving data security: Companies need to invest more in data security measures to protect individuals' personal data from cyberattacks and data breaches. This can be achieved through using advanced encryption technologies and adopting best practices in data security.
10) Encouraging ethical practices: Companies should prioritize ethical practices in their data collection and processing activities. This can be achieved through establishing internal ethical guidelines and engaging in regular ethical audits to ensure compliance.
11) Collaborative efforts: Collaboration among government, civil society organizations, and the private sector can help to develop new policies and

regulations, and foster greater transparency and accountability in the digital economy. This could include the creation of international norms and standards for data protection and privacy.

12) Consumer empowerment: Consumers should be empowered with greater control over their personal data. One way to achieve this is through the development of user-friendly tools and technologies that allow consumers to manage their data more easily. This could include the creation of decentralized data systems, where users can own and control their data.
13) Education and awareness: There is a need to raise awareness about the risks and implications of the commodification of personal data. This could include educational programs for children, teenagers, and adults, aimed at promoting digital literacy and responsible online behavior.
14) Technological innovations: Technological innovations can help to mitigate the risks associated with the commodification of personal data. This could include the development of new encryption technologies, secure communication protocols, and blockchain-based solutions.
15) Regulatory frameworks: There is a need to establish new regulatory frameworks that address the unique challenges posed by the digital economy. This could include the creation of new legal frameworks that protect consumers' rights, establish data ownership and control mechanisms, and promote transparency and accountability.
16) Multidisciplinary approaches: Addressing the complex issues surrounding the commodification of personal data requires a multidisciplinary approach. Collaboration among experts in fields such as law, economics, sociology, and computer science can help to develop innovative solutions that balance the competing interests of different stakeholders.
17) Greater regulation and oversight: Governments and regulatory bodies must develop and implement legislation that protects personal data and promotes transparency in data collection and use.
18) Improved data literacy: As data becomes increasingly important in our lives, it is crucial that individuals become more data literate. This will enable them to understand the implications of data collection and use and make informed decisions about their personal data.
19) Enhanced cybersecurity measures: As data breaches become more common, organizations must invest in better cybersecurity measures to protect personal data from unauthorized access.
20) Alternative business models: New business models, such as data co-operatives, could provide an alternative to the current data economy, where consumers have more control over their personal data.
21) Increased research: Research is needed to better understand the implications of personal data commodification on innovation, markets, and privacy. This will enable us to develop more effective strategies to address the issue.

By adopting these recommendations, we can pave the way for a more sustainable, ethical digital economy that balances innovation with privacy and empowers individuals to take control of their personal data.

Conflict of interest: The author declares no conflict of interest.

References

1. Statista. Global market for data monetization forecast to exceed USD 500 billion by 2026. Available online: https://www.statista.com. 08.01.2025 (accessed on 15 August 2024).
2. Toffler A. The third wave. Bantam Books; 1980.
3. Zuboff S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs; 2019.
4. Warren S, Brandeis L. The right to privacy. Harvard Law Review. 1890; 4(5): 193–220.
5. Varian HR. Beyond big data. Business Economics. 2014; 49(1): 27–31.
6. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs. 2019. doi: 10.1080/23753234.2022.2086891
7. Romanosky S, Acquisti A. Privacy Costs and Personal Data Protection: Economic and Legal Perspectives. 2009.
8. Elkington J. Cannibals with forks: The triple bottom line of 21st-century business. Capstone; 1997.
9. Mohammadian HD. Mapping the Future Sustainable, through the Theory of Comprehensive Everything or the 5th Wave/Tomorrow Age Theory, with a focus on Hybrid SMEs/SME 5.0 Educationally. In: Proceedings of the 2022 IEEE Global Engineering Education Conference (EDUCON); 28–31 March 2022; Tunis, Tunisia. pp. 1747–1761.
10. Schwab K. The Fourth Industrial Revolution: What it means, how to respond. Available online: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (accessed on 10 December 2024).
11. Belanger F, Crossler RE. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly. 2011; 35(4): 1017–1041.
12. Harris RD. Cybersecurity in the Digital Age. In: Selby M (editors). Cybersecurity: Human Rights in the Age of Cyberveillance. Routledge; 2021. pp. 15–32.
13. Turow J. The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power. Yale University Press; 2017.
14. Tene O, Polonetsky J. Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property. 2013; 11(5): 239–274.
15. Lanier J. Ten arguments for deleting your social media accounts right now. Henry Holt and Company; 2018.
16. Andrejevic M. The big data divide. International Journal of Communication. 2014; 8: 1673–1689.
17. Mayer-Schönberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt; 2013.
18. Floridi L. The fourth revolution: How the infosphere is reshaping human reality. Oxford University Press; 2014.
19. Brynjolfsson E, McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. WW Norton & Company; 2014.
20. Stucke ME. Competition policy for the digital era. Oxford University Press 2019.
21. Acquisti A. The economics of privacy. Journal of Economic Literature. 2017; 55(1): 442–492.
22. European Commission. Regulation (EU) 2016/679: General Data Protection Regulation (GDPR). European Commission; 2018.
23. Choi JP, Thampapillai DJ. The economics of personal data and privacy: An overview of concepts and issues. International Journal of Industrial Organization. 2019; 63: 1–8.
24. Fuchs C. Unmasking the True Price of 'Free': Exploring the Commodification of Personal Data in the Digital Economy and the Implications for Innovation, Markets, and Privacy in a Post-Truth World via X.0 Wave/Age Theory. Social Media + Society. 2020; 6(1): 2056305120905078.
25. Wu T. The attention merchants: The epic scramble to get inside our heads. Knopf; 2016.
26. O'Neill C. Weapons of math destruction: How big data increases inequality and threatens democracy. Crown; 2016.
27. Obar JA, Oeldorf-Hirsch A, Williams ML. The digital surveillance ecosystem: Toward a critical framework for data-driven privacy research. Information, Communication & Society. 2019; 22(1): 118–135.
28. Kubát M. Velvet Revolution 30 years on: A unique moment in history. Czech Journal of International Relations. 2019; 54(2): 7–28.

29. Zuboff S. Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology. 2015; 30(1): 75–89.
30. Howard PN, Kollanyi B. Bots, #StrongerIn, and #Brexit: Computational propaganda during the UK-EU referendum. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798311 (accessed on 10 December 2024).
31. Cadwalladr C, Graham-Harrison E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Available online: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed on 10 December 2024).
32. Obermeyer Z, Powers B, Vogeli C, et al. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019; 366(6464): 447–453.
33. Wu T. The Curse of Bigness: Antitrust in the New Gilded Age. Columbia Global Reports; 2018.
34. Bayramov SE, Delgado CEB. The Emergence of Hybrid Warfare. Joint Force Quarterly. 2016; 80: 7–13.
35. Farkas J, Schmitt M. Hybrid warfare: A new paradigm of warfare? The RUSI Journal. 2013; 158(5): 60–67.
36. Giordano JP. Hybrid warfare and cyber security: Strategic concepts and cutting-edge examples. CRC Press; 2019.
37. Rattray G. The limits of hybrid warfare: A response to Frank Hoffman. Joint Force Quarterly. 2015; 77: 144–150.
38. Tandoc Jr. EC, Lim ZW, Ling R. Defining "Fake News". Digital Journalism. 2018; 6(2): 137–153.
39. Shu K, Sliva A, Wang S, et al. Fake News Detection on Social Media: A Data Mining Perspective. ACM SIGKDD Explorations Newsletter. 2017; 19(1): 22–36.
40. Stieglitz S, Dang-Xuan L. Emotions and Information Diffusion in Social Media—Sentiment of Microblogs and Sharing Behavior. Journal of Management Information Systems. 2013; 29(4): 217–248.
41. Tsfati Y. The Relationship between Exposure to News, Sensationalism, and Political Sophistication. Journalism & Mass Communication Quarterly. 2017; 94(3): 748–766.
42. Wardle C, Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report. 2017; 15.
43. NATO. NATO Terms and Definitions. NATO; 2016.
44. NATO. Allied Joint Doctrine for Information Operations. NATO; 2016.
45. United States Department of Defense. Information Operations. United States Department of Defense; 2016.
46. Mackiewicz D. Cognitive Warfare. Conference: INSS-Summer Institute 2018At: Tel Aviv, Israel, Cognitive Warfare: A 21st Century Primer. U.S. Army War College Press; 2021.
47. Erbschloe M. Information Warfare: The Strategic Use of Information for Modern Warfare. Jones & Bartlett Learning; 2017.
48. Huntington SP. The Clash of Civilizations? Foreign Affairs. 1993; 72(3): 22–49.
49. Huntington SP. The Clash of Civilizations and the Remaking of World Order. Simon & Schuster; 1996.
50. Dziak JW. Cheating and Deception: Strategies for Managing Cognitive Warfare. Strategic Studies Quarterly. 2016; 10(1): 85–105.
51. Mohammadian HD, Langari ZG, Wittberg V. Cyber Government for Sustainable Governance: Examining Solutions to Tomorrow's Crises and Implications through the 5th wave theory, Edu 5.0 concept, and 9PSG model. In: Proceedings of the 2022 IEEE Global Engineering Education Conference (EDUCON); 28–31 March 2022; Tunis, Tunisia. pp. 1737–1746.
52. Hung TC, Hung TW. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. Journal of Global Security Studies. 2022; 7(4). doi: 10.1093/jogss/ogac016
53. Available online: https://www.youtube.com/watch?v=EGeiz23CmPU (accessed on 11 December 2024).
54. Mohammadian HD, Langari ZG, Castro M, et al. Smart Governance for Educational Sustainability: Hybrid SMEs & the 5th wave theory Towards Mapping the Future Education in Post-Covid Era. In: Proceedings of the 2022 IEEE Global Engineering Education Conference (EDUCON); 28–31 March 2022; Tunis, Tunisia. pp. 1916–1926.
55. Mohammadian HD, Langari ZG, Kamalian AR, et al. Promoting sustainable global innovative smart governance through the 5th wave theory, via Fuzzy AHP for future SMEs (SME 5.0/hybrid SMEs). AIMS Geosciences.2023; 9(1): 123–152.
56. Mattiello H. Sailing the X.0 Wave Theory: Navigating the Future of Civilization. Intelligent and Sustainable Manufacturing. 2024; 1(2): 10021. doi: 10.70322/ism.2024.10021
57. Mohammadian HD, Langari ZG. Competitive Advantage, Strategy and Innovation in Africa: Issues and Applications. Routledge; 2023. pp. 53.
58. Mattiello H. Vulnerability Assessment of European Personal Data Commodification in the Digital Economy. 2021.

59. Mohammadian HD, Langari ZG. A Study of Innovations and Creativities as a Competitive Advantages Strategy in the Context of i-Sustainability Plus Theory via an African Cultural Approach. In: Competitive Advantage, Strategy and Innovation in Africa: Issues and Applications. Routledge; 2023. pp. 30.
60. Mohammadian HD. Mapping the Future SMEs' HR Competencies via IoE Technologies and 7PS Model Through the Fifth Wave Theory. In: Management and Information Technology in the Digital Era—Challenges and Perspectives. Emerald Publishing Limited; 2022. pp. 141–171.
61. Kaplan JM, Haenlein M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons. 2019; 62(1): 15–25.
62. Schwab K. The Fourth Industrial Revolution. Crown Currency; 2016.
63. Dietz JLG. The X.0 Age: The Future of Digital Disruption. Routledge; 2017.
64. Crosby M, Pattanayak P, Verma S, et al. Blockchain technology: Beyond bitcoin. Applied Innovation. 2016; 2(6–10): 71–77.
65. Jordan MI, Mitchell TM. Machine learning: Trends, perspectives, and prospects. Science. 2015; 349(6245): 255–260.
66. Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015; 17(4): 2347–2376.
67. Billinghurst M, Clark A, Lee G. A survey of augmented reality. Foundations and Trends in Human–Computer Interaction. 2015; 8(2–3): 73–272.
68. Mittelstadt BD, Floridi L. The ethics of big data: Current and foreseeable issues in biomedical contexts. Science and Engineering Ethics. 2016; 22(2): 303–341.
69. Kroll JA, Looi MK, Wingreen NS. Quantitative bounds on the computational power of spiking neural networks and of neuromorphic computing. Frontiers in computational neuroscience. 2018; 12: 35.
70. Calo R. Robotics and the new cyberlaw. Harvard Journal of Law & Technology. 2013; 27(2): 595–635.
71. Crouch RA, Elliott C. Biotechnology, bioethics and the value of life. Journal of Medical Ethics. 2015; 41(4): 340–344.
72. Jasanoff S, Kim SH. Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. Minerva. 2015; 53(3): 275–297.
73. Aguilar-Lasserre AA, Torres-Sánchez VE, Fernández-Lambert G, et al. Functional optimization of a Persian lime packing using TRIZ and multi-objective genetic algorithms. Computers & Industrial Engineering. 2020; 139: 105558.
74. Chang PL, Hsu CW, Chang PC. Fuzzy Delphi method for evaluating hydrogen production technologies. 2011. doi: 10.1016/j.ijhydene.2011.05.045
75. Doost Mohammadian H. Google's Advertisement and Announcement for JOB. In: Proceeding of the Soziales Kulturkapital und kognitive Kriegsführung: Iran Kultur online live conference, April 6, 2021. Berlin, Germany.
76. Isaac M, Frenkel S. Uber reveals data breach and cover-up, leading to two firings. The New York Times. 2017.
77. Wauters R. Google's GDPR compliance efforts emerge: $57M spent on compliance, 90K staff trained, 1K experts hired. TechCrunch; 2018.
78. Angwin J, Mattu S. Amazon's facial recognition matched 28 members of Congress to criminal mugshots. Here's why experts are worried. ProPublica; 2018.
79. Kang C. Apple's latest privacy move: It's collecting more of your data. The New York Times, 12 June 2017.
80. FTC. Equifax data breach settlement. Available online: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (accessed on 11 December 2024).
81. Timberg C, Dwoskin E. Google tracks your movements, like it or not. Associated Press; 2018.
82. Copeland R. Google's secret "Project Nightingale" gathers personal health data on millions of Americans. The Wall Street Journal. 2019.
83. Vincent J. Google will no longer read your emails to tailor ads. The Verge; 2017.
84. Greenwald G. How the NSA Plans to Infect 'Millions' of Computers with Malware. Available online: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ (accessed on 11 December 2024).
85. Kofman M, Ranta R. Social media in hybrid warfare: Ukraine as an information battlefield. European Parliamentary Research Service. 2018.
86. Clarke R. Hybrid war and its implications for resilience. Journal of Contingencies and Crisis Management. 2017; 25(4): 231–236.
87. Mameli M. AI, cognitive warfare and cyber security: A conceptual and ethical analysis. Ethics and Information Technology. 2019; 21(2): 101–114.

88. Tufekci Z. Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press; 2018.
89. Lohr S. The cost of a hot economy in California: A severe shortage of workers. The New York Times. 2019.
90. Kshetri N, Voas J. Blockchain-enabled smart contracts: Architecture, applications, and future directions. IEEE Computer Society; 2018.
91. Harding L. The Cambridge Analytica scandal changed the world—but it didn't change Facebook. Available online: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (accessed on 11 December 2024).
92. Pasquale F. The black box society: The secret algorithms that control money and information. Harvard University Press; 2015.
93. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company; 2015.
94. Boyd D, Crawford K. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society. 2012; 15(5): 662–679.
95. Ohm P. Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review. 2010; 57: 1701–1777.
96. Abdelli MEA, Sghaier A, Akbaba A, et al. Smart Cities for Sustainability: Approaches and Solutions. Emerald Publishing Limited; 2023.
97. Mohammadian HD, Alijani O, Moghadam MR, et al. Navigating the Future by Fuzzy-AHP method: Enhancing Global Tech-Sustainable Governance, Digital Resilience, & Cybersecurity via the SME 5.0, 7PS Framework & The X.0 Wave/Age Theory in the Digital Age. AIMS Geosciences. 2024; 10(2): 371–398. doi: 10.3934/geosci.2024020
98. Mattiello H, Domann C. Overcoming SME Legal and Regulatory Challenges and Fostering Sustainable Collaboration and 7PS Engineering in the Digital Age through Integrating the X.0 Wave Theory & SME 5.0 Concept. Intelligent and Sustainable Manufacturing. 2024; 1(2): 10011. doi: 10.35534/ism.2024.10011
99. Mohammadian H, Wittberg V. Edu-Tech Mirrors Culture as an Infrastructure & Solution for Future-Oriented Engineering Edu-Tech Challenges in the Digital Transformation and Industry 5.0/Society 6.0 Era via X.0 Wave/Age Theory. In: Proceedings of the 2024 IEEE Conference (EDUCON); 08–11 May 2024; Kos Island, Greece.
100. Available online: https://www.youtube.com/watch?v=tiqJoC2RTpc, Prof. Hamid Mattiello's own work in 2010 (accessed on 22.01.2025 7:46)