Chapter 9

Trust, Privacy and Cybersecurity in E-Commerce

Nazlı Pehlivan Yirci[1]

Abstract

As digital technologies rapidly spread, e-commerce has become one of the fastest growing areas keeping pace with this speed in global trade. The remarkable development of e-commerce, which has changed the way businesses interact with consumers, has brought with it the need for concepts such as security and privacy, especially on the consumer side. While physical contact and face-to-face interaction in traditional methods instill trust in consumers, this situation creates cognitive and emotional difficulties in digital environments. In digital environments, the concepts of the business's competence and proficiency, honesty, positive feelings towards the business, commitment and felt loyalty are important for the consumer, and businesses can instill confidence in the consumer through the sensitivity they show in these matters. It is now as important for consumers that the security of issues such as personal data and payment information is ensured as it is for the products offered by businesses to meet consumer expectations. Ensuring standards of trust, privacy, and cybersecurity, which directly influence consumers' decisions when conducting transactions in online environments, has become a strategic element for digital businesses to increase their interaction with consumers and gain a competitive advantage. This situation is also a necessity for e-commerce to be sustainable. This is because consumer trust is not only a factor that increases sales, but also provides businesses with sustainable customer relationships and brand loyalty in the long term.

This part of the study covers the concept of consumer trust, the importance of establishing consumer trust in digital businesses, regulations regarding data protection and privacy, cyber attacks and measures that can be taken to reduce these attacks

1 Dr., Hitit University, Osmancık Ömer Derindere Vocational School
https://orcid.org/0000-0001-9641-415X, nazlipehlivan@hitit.edu.tr

https://doi.org/10.58830/ozgur.pub943.c3953

1. Introduction

Internet technologies have changed the ways businesses share information with their partners, communicate, and buy and sell (Damanpour & Damanpour, 2001:16). As with many other areas, business-consumer interaction has also undergone a transformation, particularly with digitalization. In this transformation, the security of personal data and payment information in digital environments has become important for consumers. According to Laudon & Traver (2021), the development of e-commerce, which is growing rapidly in global trade with the spread of digital technologies, has also brought with it many requirements in areas such as privacy, security, and user trust (Laudon & Traver, 2021).

Consumers want businesses to meet their expectations for the products they offer. However, today's consumers also want the security of their personal data and payment information in digital environments. According to Gefen et al (2003), the secure protection of consumers' personal data and payment information has become a fundamental requirement for the sustainability of e-commerce (Gefen et al, 2003). Indeed, e-commerce, which is conducted without physical observation and control, is based on mutual trust, and the most important measure of e-commerce development is the security of information sent over the internet. Furthermore, the risk of consumers' credit card and other information falling into the hands of third parties when providing such information for e-commerce, eliminating this risk, or ensuring the security of personal information is important for the development of e-commerce (Elibol & Kesici, 2004; Söylemez, 2006).

Regulations regarding the protection and confidentiality of consumer data aim to ensure that consumers can shop safely in e-commerce. This is because user identity information, addresses, credit card details, and behavioral data are processed on e-commerce platforms, and the confidentiality of this data requires legal and ethical responsibility (Solove, 2006).

Advancing technologies and the widespread use of the internet have changed many of our habits, such as communication, shopping, and banking transactions, while also introducing the concept of cybercrime into our lives and exposing businesses trying to adapt to changing technologies to cyber threats (Eroğlu, 2023). While advancing digital technologies enable businesses to communicate with consumers more interactively and directly, and to effectively operate their marketing strategies and online platforms, they also make their systems vulnerable to cyber attacks (Gündüzyeli, 2025:4). As technology advances, the number of consumers using electronic platforms is increasing, and malicious attackers' attempts at illegal access are

also rapidly multiplying (Gülmüş, 2010), and security breaches on these platforms are putting consumers' financial and personal information at risk (Suh & Han, 2003).

This part of the study covers important concepts in e-commerce, such as consumer trust, regulations on consumer data protection and privacy, cyber threats, and risk mitigation strategies.

2. Building Consumer Trust in Digital Businesses

Digital marketing, which encompasses the communication activities carried out by businesses using their online communication channels and assets (Şengül, 2017), has become a profitable and critical sector for almost every business in recent years (Kumar, 2022). To create an internet-based marketing platform, a secure, reliable, and privacy-sensitive system must first be established (Belanger, 2002:247).

Trust, an important factor in influencing consumer behavior, has gained even greater importance in an uncertain environment such as e-commerce (Chellappa & Pavlou, 2002). In this context, with the increase in online services, building trust among consumers has become a strategic element that provides a competitive advantage for businesses (Gefen et al., 2003). Consumer trust is defined as the consumer's belief that the products offered by businesses will meet their expectations, that their personal information will be kept secure, and that the process will run smoothly (McKnight et al., 2002). In other words, it goes beyond the consumer's satisfaction with the product's features and functional performance and consists of a sense of security that will meet the consumer's expectations (Tong & Su, 2018: 524). Trust, which has an economic meaning in the buyer-seller relationship (Sahay, 2003:556), is a fundamental factor in establishing long-term relationships with consumers and maintaining these relationships (Sharma, 2000:471).

Trust, reliability, and privacy, which are also important in traditional marketing approaches, have become even more important in digital marketing. Furnell (1999) lists the reasons why this is so important in digital marketing as follows (Furnell, 1999:373):

- Because there is never complete control over the transfer of data or products to the buyer, the buyer selects the product they want to purchase online and places their order using certain technological devices. The existence of data control systems that ensure all stages of data or information transfer are carried out securely is important.

- Because the other party may be unknown, i.e., no information about the other party may be available other than their website address, it is important that at least one of the parties is a recognized and trustworthy person/institution to resolve this issue.
- One of the parties may be located in a different and unknown physical location and therefore be subject to different laws and rules. Therefore, it is important that there are rules or laws that each party will accept.

Consumers fear and suspect fraud when doing business with unfamiliar companies on online platforms, and the reliability of the website is crucial to overcoming this (Constantinides, 2004: 114). Furthermore, if consumers have privacy concerns, this also reduces trust. The issue of privacy directly affects users and raises many concerns, such as the security of information obtained from consumers, payment details, whether payment details will be misused, and identity theft (Niranjanamurthy et al., 2013: 2361).

On e-commerce platforms, website features, third-party certifications, situational factors, consumer trust tendencies, and perceived risk affect consumer trust (Connolly & Bannister, 2008). The existence of security vulnerabilities on a shopping site and the perception that rules may be violated in critical processes such as payment transactions and personal data protection can undermine consumer trust, which may cause consumers to avoid using the shopping site (Akçacı & Kurt, 2020). Payment methods such as credit cards, debit cards, and prepaid cards, especially those used in digital marketing systems, raise concerns about security vulnerabilities and cybercrime. In such cases, customers' security concerns may increase, or real risks may arise (Martin et al., 2017). This is because the payment methods mentioned are the most common payment methods used for online transactions, and this situation also increases the incidence of fraud (Akdemir & Yenal, 2020).

In digital businesses, consumer trust is influenced by the quality of the website and user experience, security and privacy policies, social proof, customer reviews, brand image, and reputation. Features such as user-friendly interfaces, easy navigation, fast loading times, and mobile compatibility (Flavián, Guinalíu & Gurrea, 2006), data security such as SSL certificates, and transparent privacy policies (Yenisey et al., 2005), user reviews and ratings that include the experiences of other consumers, especially for new customers (Ba & Pavlou, 2002), and a well-structured digital brand image (Kim et al., 2008) are critical for consumer trust. If the security of consumer data cannot be adequately ensured, brand reputation may be damaged due to increased security concerns among customers, making it crucial to provide

an environment that inspires consumer confidence (Gündüzyeli, 2025: 3). Therefore, businesses must prioritize privacy and security factors to increase their transaction volumes (Kim et al., 2008: 557).

Trust issues in e-commerce are a problem encountered in every sector, and trust can be established by developing appropriate strategies for these problems. For example, in the financial services sector, problems such as phishing, fraud, and data leaks may occur. To address this, behavioral analysis and multi-factor authentication strategies can be developed (Kaur & Arora, 2021). In healthcare and pharmacy, the confidentiality of electronic health data can be an issue. To address this, strategies such as role-based access control and cloud-based encryption can be developed (Ozair et al., 2015). Furthermore, in the food and service delivery sector, strategies such as end-to-end data encryption and user permission control systems can be developed to combat issues such as location data breaches and fake applications (Zhang et al., 2021). In the fashion and retail sector, strategies such as using artificial intelligence applications to detect fraud and 3D Secure payments can be developed against security issues such as credit card theft, social media-related threats, or fake websites (Chatterjee & Kar, 2020). In the tourism and hospitality sector, there may be reservation fraud and breaches of customer data. To address this, strategies such as verification codes and user email identity detection can be developed to build consumer trust (Law et al., 2019).

3. Data Protection and Privacy Regulations

The concept of personal data, which is defined similarly in the European Convention on Human Rights and the decisions of the European Court of Human Rights, and which is defined in Article 3/1 of the Personal Data Protection Law No. 6698 as "any information relating to an identified or identifiable natural person" (Başalp, 2004: 22), is defined in Article 4/1 of the General Data Protection Regulation (GDPR) Article 4/1 as "any information relating to an identified or identifiable natural person (data subject)" (GDPR, 2016). Şimşek (2008) and Sert (2016) state that personal information includes official identity information, education and health data, personal expenses, social media information, images and photographs, and special categories of data such as political and religious beliefs (Şimşek, 2008: 121; Sert, 2016: 276-278).

Personal data, which is any information that makes individuals identifiable (Kılınç, 2012: 1095), vary from country to country, such as convictions in the UK, trade union membership in Poland, genetic information, skin color

in Iceland, sexual behavior, alcohol and drug use data, sexual preferences and social welfare assistance data in Finland (Kaya, 2011: 319).

The process of collecting and using data consists of the processes of collecting personal data, combining and storing the collected data, analyzing and transferring the data, and finally compiling, storing, and analyzing the collected information (Şahbaz et al., 2014: 4-5) concerns both government agencies and private sector organizations (Bainbridge, 1997: 17).

In this regard, consumers are concerned about issues such as the unauthorized sharing, use for advertising purposes, or leakage of their data, and these concerns can also influence their shopping behavior. (Beldad, De Jong & Steehouder, 2010). In this context, the importance of privacy becomes apparent. Privacy, a fundamental human right, is one of the most difficult concepts to define among all human rights, and this right was initiated in 1890 by two lawyers (Bennett, 2009). Kokolakis (2017) expresses privacy in three dimensions: territorial privacy (privacy related to a person's physical space), personal privacy (unnecessary interference with an individual's physical presence, such as physical searches), and information privacy (control over the collection, storage, or processing/distribution of personal data) (Kokolakis, 2017). Privacy, as a fundamental human right, has become important in e-commerce in terms of the security of personal data. Ersoy (2006) stated that one of the threats to the security of personal data is the illegal acquisition and use of information in e-commerce through electronic programs and methods (Ersoy, 2006). Necessary regulations have been made both globally and in our country within the scope of these threats.

In the international arena, within the scope of personal data protection; in the United States, the Freedom of Information Act (1966) and the Privacy Act (1974) (Kaya, 2011: 321), the "Guidelines for the Protection of Privacy and Transborder Flows of Personal Data" prepared by the Organization for Economic Cooperation and Development (OECD) and adopted in 1981 (Ünver & Kim, 2016: 6), the "Guidelines for the Protection of Privacy and Transborder Flows of Personal Data" adopted by the United Nations General Assembly in 1990 "Guidelines Concerning Computerized Personal Data Files" (Kılınç, 2012: 1097) and the Council of Europe, influenced by developments in information technology since the 1960s, have adopted various texts on the protection of personal data (Warner, 2005: 79). Furthermore, in 1953, the Council of Europe enacted the European Convention for the Protection of Human Rights and Fundamental Freedoms, which can be considered the basis for the misuse of personal data (İmre, 1974: 150-151). In 1970, the first data protection law in Europe was

enacted in the German state of Hesse (Tortop, 2000: 2-3). In 1978, France enacted the "Law Concerning Data Processing, Files, and Liberty" to protect individuals' private lives. In Turkey, a commission was established in 1989 to draft legislation on the protection of personal data, but the commission was unable to complete its work (Nebil, 2016). In 2000, a second commission was formed and drafted a bill on the protection of personal data. After a long process, Law No. 6698 on the Protection of Personal Data was passed by the Turkish Grand National Assembly on March 24, 2016, and became law (Sert, 2016: 277).

To increase individuals' control over their data and define the responsibilities of businesses, various legal regulations developed by governments and international organizations (Solove, 2006) include the European Union's General Data Protection Regulation (GDPR) and the United States' California Consumer Privacy Act (CCPA) are among the most important regulations in this area. The GDPR is user-focused and includes provisions such as data portability, the right to be forgotten, and explicit consent. The CCPA, on the other hand, is a regulation that protects data privacy by granting users the right to prevent the sharing of their data and to have their data deleted. In Turkey, the legal regulation in this area, the KVKK, regulates the personal data processing procedures of businesses. The fundamental principles of the General Data Protection Regulation (GDPR) (GDPR, 2016) are as follows:

- Compliance with the law, transparency
- Accuracy
- Integrity and confidentiality
- Purpose limitation
- Storage limitation
- Data minimization
- Accountability have been determined. These principles form the basis of the regulation's data protection and confidentiality. The first principle of the regulation, legality and transparency, states that businesses collecting data must be transparent about why they are collecting the data and for what purpose they will use it. Under the principle of accuracy, organizations have an obligation to organize individuals' information and correct it at the individual's request in case of error or omission. The principle of integrity and confidentiality requires organizations to protect personal data and ensure the

necessary level of security. The principle of limitation does not specify a clear time period for data retention by organizations, but states that data should not be retained longer than necessary, except in certain scientific and exceptional cases. The principle of data minimization requires organizations to store only the minimum amount of data necessary for their purposes. The principle of accountability requires organizations to take responsibility for the data they hold and process.

The prominent rights in the General Data Protection Regulation (GDPR) are (GDPR, 2016):

- Right of access
- Right to erasure (right to be forgotten)
- Right to rectification
- Right to object to automated processing
- Right to data portability.

The GDPR covers European Union citizens. In contrast, the CCPA, which came into force in 2020, aims to protect the data privacy of individuals living in the state of California (Greenleaf, 2020) and features such as the right to be informed, the right to erasure, the right to opt out of sales, and the prohibition of discrimination against consumers who exercise their rights (Solove & Schwartz, 2021). The KVKK is highly compatible with the GDPR and has fundamental features such as explicit consent, the obligation to provide information, and data security principles (Çalışkan & Özer, 2020).

4. Cyber Treats and Risk Mitigation Strategies

With the spread of the internet and advancing technologies, people's habits such as shopping, communication, and banking transactions have also changed, and businesses trying to adapt to this change have faced cyber threats (Eroğlu, 2023). Cyberattacks are activities carried out with the aim of exploiting, corrupting, or altering information in the cyber environment, or blocking access to or damaging systems (Çiftçi, 2013). With the increasing frequency and scope of cyberattacks, every area of economic activity is being affected, putting industry and businesses at risk (Aiman et al., 2021). Accordingly, ensuring the security of personal information and accounts has become imperative to protect against cybercrime (Kumar, 2022).

Cyber threats carried out through various digital channels include the theft of data and sensitive information in the field of marketing, malware

infection, DDoS attacks, browser hijacking, identity theft, fake news dissemination, and WordPress malware. Unfortunately, the vast majority of digital marketing professionals are unaware of all these threats and are caught unprepared for these attacks (Kumar, 2022).

In the digital age, cyber threats are a reality that every business must face (Akhtar et al., 2021). Businesses should develop digital marketing strategies that create a defense mechanism against cyber threats (Şenyapar, 2024). The principles known as the CIA triangle, namely confidentiality, integrity, and availability, form the fundamental elements required to ensure information security. These principles, which also constitute the most important functions of cybersecurity, are of great importance for businesses to continue their activities on digital platforms (Stallings & Brown, 2008). These principles, which are critical for the secure operation of digital marketing strategies, are expressed as follows (Gündüzyeli, 2025: 7):

1. *The principle of confidentiality: This ensures that user data is accessible only to authorized individuals.*
2. *The principle of integrity: This ensures that data is protected accurately and without corruption.*
3. *The principle of accessibility: This ensures that users can access accurate information at all times.*

Cyberattacks targeting marketing systems cause interruptions in business services and jeopardize the security of brands on online platforms. In today's world, where implementing cybersecurity measures is of great importance, secure systems are needed to protect businesses' personal data and trade secrets from the threat of theft (Buhas et al., 2021).

Obitovich & Utkirovna (2023) emphasize the necessity of cybersecurity measures to increase the effectiveness of digital marketing strategies and state that the measures taken will also positively affect the return on investment (Obitovich & Utkirovna, 2023). At this point, it may be necessary to briefly mention the types of cyberattacks targeting digital marketing processes and the measures that can be taken against them.

Table 1: Types of Cyber Attacks

Types of Cyber Attacks	Explanation
Viruses	Malicious software that replicates itself and spreads to other systems.
Worms	Malicious programs that replicate themselves and spread over a network.
Trojan Horses	Malicious software that secretly infiltrates systems and compromises security.
Logic Bombs	They aim to delete or modify data by embedding malicious code in a specific program.
Unsolicited Electronic Mail	Spam emails; usually for advertising purposes.
Keyloggers	Record user keystrokes and send them to unauthorized individuals.
Spyware	Malicious software that copies and transfers data without the user's knowledge.
DDoS Attacks	Intense data transmission that blocks network communication and prevents access to services.
Social Engineering	A technique that manipulates human errors to gain access to confidential information.
Other Types of Attacks	New threats are constantly emerging, showing diversity and continuous development.

Source: Gündüzyeli, 2025: 11.

Trojan horses and spyware, which are types of cyber attacks targeting digital marketing processes, are hidden malicious software that can compromise security by obtaining consumers' private information. Viruses and worms, which can spread by replicating themselves, steal consumer data and disrupt system operations. Unsolicited emails, or spam emails, can send advertising emails to consumers without their request. DDoS attacks can block access to businesses' e-commerce pages, hindering marketing activities.

Table 2: Cyber Attack Prevention Methods

Prevention Methods	Explanation
Encryption	Encrypts plain text, allowing access only to authorized personnel.
Antivirus Software	Detects and prevents viruses, protecting systems.
Firewall	Controls network traffic, enforcing security policies.
Digital Signature	Verifies the sender and recipient of electronic documents and increases the reliability of the documents.
Virtual Private Networks (VPN)	Provides secure communication over the Internet by encrypting and protecting data.
Proxy Servers	Increases security by providing indirect access between two networks.
Intrusion Detection Systems	Detects security vulnerabilities by analyzing system activities and triggers an alarm.
Vulnerability Scanning Tools	Identifies and analyzes security vulnerabilities in systems and networks.

Source: Gündüzyeli, 2025: 12.

Businesses engaged in digital marketing activities must develop defense strategies by taking preventive measures to ensure cybersecurity. According to Kumar (2022), cybersecurity investments strengthen businesses' image, protect customers' personal information, and provide robust cybersecurity (Kumar, 2022). Effective protection against cyber threats can be achieved through measures such as up-to-date antivirus software, strong encryption, firewalls, the use of virtual private networks (VPNs), sender and recipient verification systems, and regular system updates.

5. Conclusion

Technological developments are rapidly increasing the speed of shopping in virtual environments. This increase has led businesses to develop new strategies in competition. In particular, making shopping in online environments easy and secure in line with consumer needs and demands has become important. Building consumer trust is a sales-boosting factor for digital businesses, but it is also important for long-term customer relationships and brand loyalty.

Given the importance of consumer trust for long-term customer relationships and brand loyalty, businesses must ensure standards of trust, security, privacy, and cybersecurity, along with price competition and product

variety, to be successful in e-commerce. For this reason, it can be stated that consumer trust, privacy, and cybersecurity concepts are among the concepts that are important for the success of business strategies in e-commerce today. This is because sustainable e-commerce is not possible without building consumer trust (Kim, Ferrin & Rao, 2008). Therefore, businesses need to build environments where consumers can comfortably conduct transactions in digital environments.

Today, digital businesses not only sell goods and services on e-commerce platforms but also gain a competitive advantage by ensuring data security and using data in accordance with laws and ethical rules. The privacy and protection of consumer data is a fundamental right and is regulated by legal frameworks such as the KVKK, GDPR, CCPA, and similar regulations. The aim is to increase control over data and ensure a sustainable digital ecosystem.

In today's world, where technology is gaining momentum day by day, the legal frameworks implemented for data protection and privacy need to be continuously expanded and updated. Apart from data security and privacy, cyber threats, which are one of the important issues in e-commerce, are constantly evolving today. For this reason, the concept of cybersecurity needs to be approached with a layered, dynamic, and holistic perspective. Cyber security measures should include both technical and organizational precautions. To ensure cyber security, businesses must not only be prepared for cyber attacks but also be able to manage crises during cyber attacks, focusing on continuous training, awareness, and corporate risk management for their personnel. According to Ilyas et al (2021), an effectively developed cybersecurity strategy not only prevents financial losses and unauthorized access to or loss of sensitive data in digital marketing, but also ensures customer trust and loyalty.

Particularly in the digital age, products that provide competitive advantages through security can achieve longer-term advantages. Various encryption technologies are available to ensure this by establishing secure infrastructure and certification systems. This ensures data transfer security. It appears that trust seals can be incorporated into spending to mitigate the loss of consumer trust. Furthermore, policies such as obtaining explicit consent and responding to data access requests can be presented transparently to users. Content on the website or app can be presented in a way that informs about data privacy and confidentiality rights, or it can lead to a fragmented understanding of consumers. Businesses can prevent potential leaks by conducting regular security scans for potential risks. Fast and effective

response plans can be developed for potential attacks. Data backup and recovery processes can be regularly audited. Transparent, fast, and reliable communication methods (such as live support, chatbots, customer service) can be offered to customers, and updates can be made based on customer feedback. This can increase customer trust, support the digital branding process, and create a sustainable structure against cyber threats.

References

Aiman, A. H., Ahmad Tajuddin, S. N. A., Bahari, K. A., Manan, K. A., & Abd Mubin, N. N. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. *Asian Culture and History, 13*(2), 20.

Akçacı, T., & Kurt, F. B. (2020). Consumer trust factor in online supermarket shopping. *Dicle University Journal of Faculty of Economics and Administrative Sciences, 10*(20), 414–433.

Akdemir, N., & Yenal, S. (2020). Card-not-present fraud victimization: A routine activities approach to understand the risk factors. *Güvenlik Bilimleri Dergisi, 9*(1), 243–268.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243–268.

Bainbridge, D. I. (1997). Processing personal data and the Data Protection Directive. *Journal of Information & Communications Technology Law, 6*(1), 17–40.

Başalp, N. (2004). *Protection and storage of personal data.* Yetkin Publishing.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3–4), 245–270.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857–869.

Bennett, L. (2009). Reflections on privacy, identity and consent in online services. *Information Security Technical Report, 14*(3), 119–123. https://doi.org/10.1016/j.istr.2009.10.003

Buhas, V., Ponomarenko, I., Bugas, V., Ramskyi, A., & Sokolov, V. (2021). Using machine learning techniques to increase the effectiveness of cybersecurity. *Cybersecurity Providing in Information and Telecommunication Systems II, 3188*(2), 273–281.

Chatterjee, S., & Kar, A. K. (2020). Why do small and medium enterprises use social media marketing and what is the impact: Empirical insights from India. *International Journal of Information Management, 53*, 102103.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5–6), 358–368.

Connolly, R., & Bannister, F. (2008). Factors influencing Irish consumers' trust in internet shopping. *Management Research News, 31*(5), 339–358.

Constantinides, E. (2004). Influencing the online consumer's behavior: The web experience. *Internet Research, 14*(2), 111–126.

Çalışkan, A., & Özer, A. (2020). Personal data protection law: A comparison between Turkey and the European Union. *Istanbul Law Review, 78*(2), 245–268.

Çiftçi, H. (2013). *Cyberwar in all its aspects.* TÜBİTAK.

Damanpour, F., & Damanpour, J. A. (2001). E-business e-commerce evolution: Perspective and strategy. *Managerial Finance, 27*(7), 16–33.

Elibol, H., & Kesici, B. (2004). Electronic commerce from the perspective of modern business management. *Journal of Social Sciences Institute, Selçuk University, 11*, 303.

Ersoy, E. (2006, February 9–11). Privacy, individual rights, and protection of personal data. Paper presented at the *4th Academic Informatics Congress on Information Technologies*, Telecommunications Authority, Turkey.

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management, 43*(1), 1–14.

Furnell, S. M., & Karnewi, T. (1999). Security implications of electronic commerce: A survey of consumer and business. *Internet Research, 9*(5), 372–382.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

GDPR. (2016, May 4). *General Data Protection Regulation*.

Gülmüş, M. (2010). *Corporate information security management systems and security* (Master's thesis). Yıldız Technical University, Institute of Science, Istanbul, Turkey.

Gündüzyeli, B. (2025). The role and importance of cybersecurity in digital marketing systems. *Journal of Research in Entrepreneurship, Innovation and Marketing, 9*(17), 1–18.

İlyas, G. B., Munir, A. R., Tamsah, H., Mustafa, H., & Yusriadi, Y. (2021). The influence of digital marketing and customer perceived value through customer satisfaction on customer loyalty. *Journal of Legal, Ethical & Regulatory Issues, 24*(1).

İmre, Z. (1974). Issues concerning the protection of personal rights, private life, and privacy. *Istanbul University Journal of Faculty of Law, 39*(1–4), 146–168.

Kaya, C. (2011). Sensitive (personal) data and its processing within the framework of the European Union Data Protection Directive. *Istanbul University Journal of Faculty of Law, 69*(1–2), 317–334.

Kaur, G., & Arora, A. (2021). GDPR's implication on financial institutions: Challenges and opportunities. *Journal of Banking and Finance Technology, 5*(2), 87–101.

Kılınç, D. (2012). Protection of personal data as a constitutional right. *Ankara University Journal of Faculty of Law, 61*(3), 1089–1169.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kumar, S., Pallathadka, H., & Pallathadka, L. K. (2022). An analysis of cybersecurity threats in digital marketing. *Journal of Critical Reviews, 9*(3), 85–94.

Laudon, K. C., & Traver, C. G. (2021). *E-commerce 2021: Business, technology, society* (16th ed.). Pearson.

Law, R., Buhalis, D., & Cobanoglu, C. (2019). Progress on information and communication technologies in hospitality and tourism. *International Journal of Contemporary Hospitality Management, 31*(1), 414–433.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.

Nebil, F. S. (2016). *History and analysis of the Personal Data Protection Law – II.*

Niranjanamurthy, M., Kavyashree, N., Jagannath, S., & Chahar, D. (2013). Analysis of e-commerce and m-commerce: Advantages, limitations and security issues. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(6), 2360–2370.

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research, 6*(2), 73–76.

Sahay, B. S. (2003). Understanding trust in supply chain relationships. *Industrial Management and Data Systems, 103*(8), 553–563.

Sert, S. (2016). The issue of evaluating personal data obtained via the internet among general grounds for divorce. *TBB Journal, 116*, 275–292.

Sharma, N., & Patterson, P. G. (2000). Switching cost, alternative attractiveness and experience as moderators of relationship commitment in professional consumer services. *International Journal of Service Industry Management, 11*(5), 470–490.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Solove, D. J., & Schwartz, P. M. (2021). ALI data privacy: Overview and black letter text. *UCLA Law Review, 68*, 1252.

Söylemez, F. (2006). *An evaluation of the status of business-to-business (B2B) electronic commerce and suggestions for the top 1,000 enterprises in Turkey* (Master's thesis). Çukurova University, Institute of Science, Adana, Turkey.

Stallings, W., & Brown, L. (2008). *Computer security: Principles and practices* (2nd ed.). Pearson.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*(3), 135–161.

Şahbaz, U., Alpaslan, İ. B., & Sökmen, A. (2014). Opportunities brought by the data-driven economy and the economic analysis of personal data protection. In *Legal and economic analysis of personal data protection in Turkey* (pp. 2–38). Istanbul Bilgi University & TEPAV.

Şengül, O. (2017). *Digital marketing from A to Z in 2 hours.* CERES Publishing.

Şenyapar, H. N. D. (2024). Digital marketing in the age of cyber threats: A comprehensive guide to cybersecurity practices. *The Journal of Social Science, 8*(15), 1–10.

Şimşek, O. (2008). *Protection of personal data in constitutional law.* Beta Publishing.

Tong, X., & Su, J. (2018). Exploring young consumers' trust and purchase intention of organic cotton apparel. *Journal of Consumer Marketing, 35*(5), 522–532.

Tortop, N. (2000). An important issue of our time: The problem of personal information security. *Amme İdaresi Dergisi, 33*(3), 1–14.

Ünver, H. A., & Kim, G. (2016). Data privacy and surveillance in Turkey: An evaluation of the Personal Data Protection Law draft. *Center for Economic and Foreign Policy Research.*

Warner, J. (2005). The right to oblivion: Data retention from Canada to Europe in three backward steps. *University of Ottawa Law & Technology Journal, 2*(1), 75–104.

Yenisey, M. M., Özok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology, 24*(4), 259–274.

Zhang, Y., Ren, J., Zhang, C., & Shen, J. (2021). Security and privacy in smart delivery services: Challenges and opportunities. *IEEE Internet of Things Journal, 8*(4), 2902–2915.

Dr. Nazlı PEHLİVAN YİRCİ works as a lecturer at Hitit University's Osmancık Ömer Derindere Vocational School. She completed her undergraduate studies in the Department of Business Administration at the Çorum Faculty of Economics and Administrative Sciences at Gazi University in 2008. She began her master's and doctoral studies at the same university, completing her master's thesis titled "State Accounting System and Movable Goods Regulation Application in Annexed Budget Institutions" in 2012 and her doctoral thesis titled "A Field Study to Determine the Factors Affecting Consumers' Purchase Intentions for Metaverse Products" in 2024. She has numerous publications, including articles and book chapters, in the field of marketing.