6th International Scientific Conference ITEMA 2022 – Proceedings
DOI: https://doi.org/10.31410/ITEMA.2022.113

Payment Security Issues and User Data in Online Commerce

Nadezda Dimova[1]

Received: November 19, 2022
Accepted: February 7, 2023
Published: June 12, 2023

Keywords:
Online commerce;
User;
Security;
Payment;
Data

Abstract: *In recent years, there has been increased development of information and telecommunication technologies, which have a significant impact on the economic and social sphere on a global scale and, in particular, at the national level. In parallel, there are many challenges to the integration and use of digital technologies and the resulting issues of payment and data security in online commerce.*

This research is dedicated to revealing the nature of data privacy, the relationship between the regulator, consumers and retailers, and presenting the features of payment and data security in online commerce.

1. INTRODUCTION

Dynamic changes in the global aspect of the economy and changes in consumer tastes and preferences are only part of the factors for the creation and integration of new modern technologies. However, their implementation is a prerequisite for solving many specific problems, in particular the problems related to data security and payments in online commerce.

To examine the security of payments in online retail, we should first specify the role of data privacy. From there, let's emphasize the connection between this privacy and the security of payments specifically in online retail.

The purpose of the report is to highlight the security issues of payments and user data in online commerce.

2. DATA PRIVACY IN RETAIL

The study of data privacy in online retailing is closely related to the interrelationship between consumers, retailers, and law enforcement. In the conditions of digitization and technological improvement, they are undergoing significant transformations and, in parallel, they must manage to ensure the privacy of their data and improve the analysis of this data.

Retailers themselves process a large amount of data and many studies prove that they are always ready to increase their spending on new technologies and their personalization to track individual consumers and their location, recognize their faces, track their emotions and encode voices.

This leads to major problems in terms of the feeling of vulnerability on the part of the users (Martin et al., 2017).

[1] New Bulgarian University, 21 Montevideo Str., Sofia, Bulgaria

It is precisely this sense of vulnerability that is particularly important in conditions of challenges of a different economic and social nature (Brough & Martin, 2021).

Stakeholders and their interests in data privacy can be an essential part of big databases and privacy, creating both notable risks and threats to privacy and, in parallel, great potential for retailers.

Stakeholders themselves are looking for various ways to protect and expand user privacy, but these actions are entirely based on cooperation between them rather than contradictions and conflicts.

Researcher Martin and colleagues identify three emerging themes that are channeling collaboration and the increasing convergence between consumers, retailers and regulators regarding the collection and use of consumer data in retail. Primarily, these researchers justify the role of big data as a driver of customer relationships and customer performance because, according to them, it improves customer perceptions.

Next, they highlight the profound impact of regulation in shaping consumer-retailer interactions.

Third, but not least, they advance the idea of the potential of privacy protection as a proactive retail strategy that can provide an innovative source of competitive advantage to retailers.

All these studies and ideas are supported by quantitative and qualitative methods (Martin et al, 2017).

The conclusions reached by the researchers are that the regulatory body shapes the interaction between the consumer and the retailer. On the other hand, retailers must adhere to privacy regulations in dealing with consumers.

Next, they reach many conclusions that relate to the global perspective on data privacy. It is strongly emphasized that most studies focus on a single country or a specific company, depending on the empirical data. In parallel, privacy perspectives are determined by a country's culture, so the views of consumers, regulators and retailers on data privacy are inevitably influenced by their cultural country.

Furthermore, the cross-country and company emphasis is on demonstrating the specific case studies of retailers or regulatory approaches to data privacy and consumer response, which also establishes some frameworks for key tensions in global privacy perspectives to inform retail marketers to expand market share.

The term "privacy" itself is largely applied in specific contexts to consumers and regulators. Through the lens of the issue research, three themes emerged that involved consumers, regulators and retailers.

Researchers in this scientific field are proving that for users, large databases support increasing personalization. Bleier and Eisenbeis prove that online personalized ads improve click-throughs, especially in the early stages of purchasing decisions, but this over-personalization is only possible if customer preferences are volatile or change over time (Bleier & Eisenbeiss, 2015).

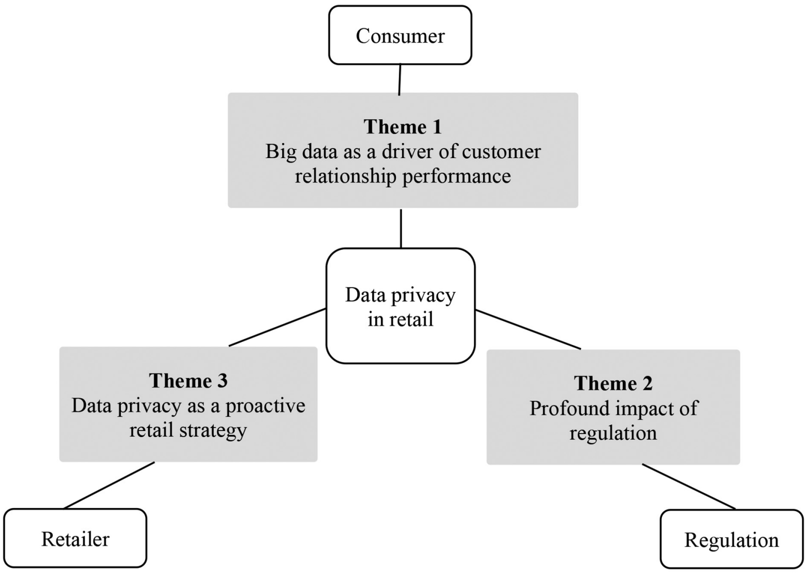
Consumer
Theme 1
Big data as a driver of customer relationship performance
Data privacy in retail
Theme 3
Data privacy as a proactive retail strategy
Theme 2
Profound impact of regulation
Retailer
Regulation

Figure 1

Source: Martin et al., 2017.

Another point of view is given by researchers Chung et al. (2016) who focus in their studies on adaptive personalization using social networks, or Tirunillai and Tellis on online communications and brand positioning (2014).

The very interaction between users and retailers depends on privacy rules. Such privacy policies can be a good proxy for the degree of transparency and control that businesses provide to their customers by notifying them then that they are providing this information (Martin et al., 2017). Along with this, stricter privacy policies can reduce the effect of the negative sides that are caused by a breach of data security, which is caused by competitors (Martin et al., 2018).

Given the purpose of the article, the security of payments in online commerce should also be analyzed.

3. SECURITY OF PAYMENTS IN ONLINE COMMERCE

In general, the targets of hacker attacks and theft of personal information and banking data are different: from the local supermarket to online shopping and providing personal data. Many companies and individuals believe that if they have antivirus software purchased and installed, they are sufficiently protected. In reality, this is not the case at all. Antivirus software is only one possible side of this problem and addresses only one threat or only one possible approach to information theft and destruction. For complete information security, additional actions of active and proactive protection are required.

When a means of payment is created, the responsibility for its protection is most often guaranteed by the one who issues it, but gradually, and especially these days, the commitment to maintaining security becomes shared and includes the entire set of participants in the payment process. Thus, in addition to the operator of the payment system, all bound users of the payment system can join the mechanism of countermeasures against attempts at malicious actions and better protection.

The problems related to the protection against fraud in electronic payments in online commerce are increasing. It is an indisputable fact that the evolution of payment systems and the technological innovations that accompany them are the basis of the improved conditions for commercial exchange and its migration to a digital environment. A new step in the present and in the functioning of online commerce is the use of artificial intelligence, which allows positives to be drawn also in terms of protection against sales fraud. In fact, its integration enables real-time intelligent and automated analytical systems to monitor user activity and implement corrective actions if new and unknown schemes of abuse in commerce and payments are detected.

No less important are three important problems of public information about the real dimensions of crime in electronic payments in commerce. The first is related to the fact that a significant part of the frauds committed in digital payments remains unreported or unregistered by the victims. The second is that the proportion of fraud is sometimes left out of official reporting because the contingently unrealized pecuniary damage is significant. The third problem is related to the evolution of organized crime, which is outpacing the development of defense systems. A prerequisite for this is mainly the limited resource provision for the implementation of various improvements. This would help us summarize that the new reality requires alternative methods of countermeasures and security, leading to the emergence of a new class of electronic services related to the protection of information in digital payments (Stoyanov, 2019).

4. CONCLUSION

In conclusion, to achieve consumer satisfaction and to keep all stakeholders in online commerce satisfied, the security of payments and consumer data is paramount. However, this process is two-way and efforts should be made on both sides – companies and consumers. Only the future will tell what level of security will be required in online commerce and who, how and in what manner will process user data both globally and nationally.

References

Bleier, A., & Eisenbeiss, M. (2015). Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where. *Marketing Science, 34(5)*, 669–688. http://www.jstor.org/stable/24544741

Brough, A. R., & Martin, K. D. (2021). Consumer Privacy During (and After) the COVID-19 Pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108–110. https://doi.org/10.1177/0743915620929999

Chung, T. S., Wedel, M., & Roland T. R. (2016), Adaptive Personalization Using Social Networks, *Journal of the Academy of Marketing Science, 44 (1),* 66–87. DOI: 10.1007/s11747-015-0441-x

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing, 81(1)*, 36–58. https://doi.org/10.1509/jm.15.0497

Martin, K. D., Palmatier, R. W., & Borah, A. (2018), "A Strong Privacy Policy Can Save Your Company Millions", *Harvard Business Review.*

Stoyanov, M. (2019). Protection Against Fraud In Electronic Trade Payments, *Economics 21, issue 1, year 20*, 48-66.

Tirunillai, S., & Tellis, G. J. (2014). Mining Marketing Meaning from Online Chatter: Strategic Brand Analysis of Big Data Using Latent Dirichlet Allocation. *Journal of Marketing Research*, *51*(4), 463–479. https://doi.org/10.1509/jmr.12.0106