Consumers' security and trust for online shopping after GDPR: Examples from Poland and Ukraine

Journal:	*Digital Policy, Regulation and Governance*
Manuscript ID	DPRG-06-2019-0044.R1
Manuscript Type:	Original Article
Keywords:	e-commerce, GDPR, Trust, Security, Online shopping

SCHOLARONE™
Manuscripts

Consumers' security and trust for online shopping after GDPR: Examples from Poland and Ukraine

Artur Strzelecki, Mariia Rizun

Department of Informatics, University of Economics in Katowice
1 Maja 50, 40-287, Katowice, Poland

Abstract

Purpose: This paper considers the question of changes brought to consumers' trust and security issues by the implementation of GDPR in electronic commerce.

Design: Online shopping policies in Poland and Ukraine are compared from the perspective of four factors: application of terms of service and privacy policy, usage of online payment systems, presence in price comparison engines, and grade of SSL security certificates. Comparison is conducted within the framework of three research questions (complemented by eight hypotheses), set to reveal whether: policies of personal data protection and server security for online stores in both countries are the same; all online stores in both countries obey the existing e-commerce rules; e-commerce policies in the two countries differ significantly. The sample for analysis contains 40 Polish and 40 Ukrainian online stores, representing four industries: electronics, entertainment, fashion, and goods for children.

Findings: The research allowed to reveal major differences in the privacy policy of the two countries, caused, mainly, by the absence of GDPR in Ukraine. It also disclosed much stronger cooperation of online stores and price comparison engines in Poland compared to Ukraine. At the same time, research results allow to state that server security in both countries is on the same rather high level and that online stores use transparent and safe methods of online payment.

Limitations: This research opens a way to other, expanded observations which will include more countries and larger scopes of data. Its main limitation is that GDPR influence is only studied in two countries, not in all countries where it is implemented.

Originality: This research contributes from security and trust perspectives by analyzing the situation in two countries: the EU member (Poland) and a non-EU country (Ukraine). The value of exploring the situation of Ukrainian e-commerce consists in understanding how online stores function without implementing the GDPR. Observation of shopbots application allows drawing an important conclusion of the necessity for online stores to cooperate with such services. It was also revealed that consumers' trust in both countries depends a lot on the payment methods applied by an online store, as well as on the ease of use of these methods.

Keywords: e-commerce, trust, security, online shopping, GDPR

1 Introduction

For our today's society Internet is no longer just a means of communicating with relatives and friends. The world wide web has covered all spheres of our life, facilitating our everyday routine in many ways. The "brick-and-mortar" shopping we all were used to has been altered or, for many spheres, even replaced by the possibility to shop online, sitting at home on the favorite couch with a laptop or a smartphone. Online stores are developing every day to keep up with the pace of the market, stay competitive, and attractive for consumers. New products are being introduced, various versions of discounts are suggested, the fastest delivery services are used. However, no matter what goods the stores have in their offer, they all are supposed to follow the same simple rule – provide consumers with the possibility to feel secure while shopping online. Regardless of the quality of products and services, e-commerce would not exist without trust of the consumers. Yet, the question arises – whether the country of origin makes any difference when analyzing the security policy applied by online stores.

There is no doubt that online shopping has its perks. To make a purchase, consumers do not need to travel a long way to the store, spend time in a crowd of other consumers, or wait in queues to make their payments. To buy something in an online store all a person needs is to be "online" – to have an internet connection and a device like a laptop, a tablet, or a smartphone. Consumers can visit hundreds of stores without leaving their homes or offices, while travelling or eating lunch at a restaurant. Moreover, they can purchase from foreign stores, which would be much more complicated if considering brick-and-mortar shopping. Such tools as price comparison engines have played a significant role in facilitating online shopping: one website (or mobile application) provides a consumer with a list of stores offering the product he/she is interested in, allowing to compare prices and/or other characteristics and choose the optimal item – all in a couple of clicks. Popularity of price comparison engines can be explained by the general information-seeking behavior that internet users display: they feel much more comfortable when usage of a single keyword (or a phrase) in a search engine directs them to one website with all the information they need – without the necessity to waste time on searching through various websites. Additionally, online stores (and comparison engines) invite consumers to leave reviews of the goods and these are very helpful for potential consumers. Online stores also attract consumers with lower prices. This is conditioned by the fact that they have lower costs for storing goods; some of them even do not possess their warehouses (Wan et al., 2018). This list of the benefits provided by online shopping is not complete, yet it allows us to state that this type of shopping is very convenient.

However, like almost any phenomenon, online shopping has its disadvantages. The major problem connected with purchasing online is the consumers' trust and security. Trust is based on two main factors: the attitude of consumers; and product quality. The emotional and cognitive responses of consumers' first visit to an online store can influence their intentions to return and their likelihood to make purchases (Chen and Chou, 2012). Online transactions cannot give the physical assurances that traditional shopping possesses (Grabner-Kraeuter, 2002) and consumers face the risk of receiving goods that are of poor quality (or worse than expected), damaged during delivery, or simply different from the ones presented on the website. According to statistics, 17% of online stores delay their deliveries and 13% of online stores' websites are prone to technical failures (Eurostat, 2018). Thus, ensuring consumers have a positive impression of the website and that they receive only goods of high quality allows online stores to remain competitive in the market. Security is the feeling consumers in online stores experience when they know that their personal data, provided for a store, are protected and will not be obtained by third parties. Online stores can guarantee this, for example, by displaying

privacy policy agreements and cookies policy information. However, these measures alone may not guarantee the safety of consumers' data.

To make sure online stores take proper care of consumer security, in May 2018, the European Parliament (European Parliament, 2016) implemented the General Data Protection Regulation (GDPR), which concerns privacy and individual rights, and applies to all residents of the EU and the European Economic Area (EEA), as well as to any other country that wants to do business with EU/EEA countries. The GDPR is linked to the basic rights of every individual in the digital community, including rights regarding the collection and storage of any type of private personal data, especially digital forms (Presthus and Sørum, 2018). To comply with the GDPR, a website must notify consumers of several important aspects, including pre- and post-contractual information; withdrawal period; usage of cookies; and data protection. To gather consumer information (via registration forms, contact forms, or in the ordering process), online stores must notify consumers that their personal data are being recorded (and why). Additionally, consumers need to be aware of the tools they may use to access their data and modify or delete it if needed.

This research is dedicated to the comparison of two neighbor countries – Poland and Ukraine, on the issue of electronic commerce security policy. These countries were chosen for being neighbors, conducting trade with each other, having a lot in common from the point of view of mentality, and, on the other hand, being separated by the border of the European Union. While the whole EU has been applying the General Data Protection Regulation (GDPR) since May 2018, forcing all online stores to work on their data protection policy significantly, these changes did not affect Ukraine. Ukrainian electronic commerce, acting on the local level, is controlled by the laws adopted by the Government of Ukraine. The rules of GDPR, for now, have only influenced Ukrainian online platforms conducting international transactions, or foreign online stores possessing Ukrainian domains (eg. answear.ua, bonprix.ua). This fact makes the comparison of these particular countries interesting for the authors.

The authors' interest in comparing Polish and Ukrainian e-commerce markets has been enhanced by the research of Woźniak (2015). The paper compares online shopping expenses of consumers and their trust in online stores in the two countries. An opinion poll was conducted (with 126 Ukrainian and 100 Polish respondents) and it was revealed that: the assortment of purchased products differs very little; in both countries consumers did not consider online shopping to be risky from the point of view of data protection; the most frequent payment methods are electronic bank transfer and credit card (slightly more popular in Poland); the level of trust towards unknown online stores (as for quality of goods and terms of delivery) is higher in Ukraine than in Poland.

This paper is organized as follows. Section 2 contains a review of the relevant literature on online shopping and its security issues. In section 3 the authors describe the current situation in the online shopping market as for the security of consumers' personal data. The description leads to the development of 8 hypotheses. Section 4 contains characteristics of the sample of online shops selected by the authors for analysis, as well as results of the conducted examination. In section 5 the authors highlight the contribution of the research and suggest possible implications of results, analyze current limitations of the research, draw conclusions on (dis)confirmed hypotheses, and present ideas for their future research on online shopping. The appendix contains the list of online shops analyzed in the research.

2 Literature Review

This section contains a literature review, dedicated to five aspects of e-commerce: trust, GDPR, payments, shopbots, and security in online shopping.

2.1 Trust in online shopping

A lot of works has been written regarding trust and security in online shopping. The topic of trust has been well researched by (Gefen et al., 2003; Grabner-Kraeuter, 2002). In these works, the model of TAM and trust in the e-vendor was introduced and it was proved that at the beginning of online shopping development consumers did not want to provide any of their personal data (Hoffman et al., 1999). Van der Heiden et al. (2003) asked 226 potential online shoppers what their technology and trust attitudes were. The research allowed the authors to find out that these factors directly influence the attitude towards purchasing online. A similar study about trust was provided by Hongyoun Hahn and Kim (2009) on 261 students and brought the same results. Al-Debei et al. (2015) asked 273 online shoppers and it also turned out that consumer attitude toward online shopping is determined by trust and perceived benefits. Trust factor could be strengthened by online consumers' reviews placed in online stores (Lee et al., 2011).

Other research showed that web trust has a significant impact on online shopping, being influenced by web security, availability, and experiences, whereas consumer reviews of websites have no impact (Köksal and Penez, 2015). Trust also plays a critical role in forming a psychological state with positive or negative feelings toward e-vendors (Wu, 2013). Kim and Peterson (2017) analyzed 150 empirical studies involving online trust. The study revealed that methodological characteristics such as study design, website type, and type of items used to measure the trust construct moderated certain online trust relationships. Celik (2016) asked 483 customers what their anxieties in online shopping are and the study indicated that anxiety simultaneously exerts negative direct influences in the context of online shopping. Khan et al. (2015) studied 30 papers about the impact of trust on online shopping. It was concluded that trust is the factor to reduce risk and enhance commitment and satisfaction level of both consumers and sellers.

Recent research has given results in a form of the following models: factors affecting consumer attitudes towards online shopping security (Wu and Ke, 2015); integrating personality traits, perceived risk, and technology acceptance security in shopping online (Akroush and Al-Debei, 2015); interrelationship between perceived risk factors, the marketing impacts, and their influence on product and web-vendor consumer trust (Pappas, 2016). Other researchers noticed that trust in online shopping is affecting consumers' loyalty. Al-dweeri et al. (2017) found that consumers' loyalty is influenced by efficiency, privacy, and customer service. Shafiee and Bazargan (2018) indicated that information security and website performance have a direct positive influence on online shopping quality.

Nilashi et al. (2015) focus on security, design, and content factors that influence customers' trust in mobile commerce websites. In their findings, trusted websites can provide mobile commerce with powerful competitive advantages. An experiment was conducted by Tamimi and Sebastianelli (2015), in which participants viewed fictitious online store web pages and indicated the likelihood of purchasing the products displayed, by manipulating four attributes: familiarity with the online store, product type, summary product review, and the number of customer reviews – in order to determine their relative importance on trust and security in online shopping. Results suggest that the summary review star rating of the product and familiarity with the online store are the two most important attributes. However, data breaches may result

in the loss of personal data belonging to customers. The impact of perceived online shopping risk on post-breach online shopping is significantly different than the one before this breach (Chakraborty et al., 2016).

Similar results were obtained by Arora and Muttoo (2018), who found that consumers' online security and privacy concerns are positively correlated with not giving their credit card number to unprotected online shopping stores if they perceive privacy and security concerns to be barriers to online shopping. Consumers are aware of some threats in online shopping. For example, the survey by Kamaladevi and Vanithamani (2016) exploring UAE users' confidence in online shopping revealed that 15% of the sampled consumers did not feel safe when shopping online. Gupta (2018) explored how large-scale data breaches, coupled with sophisticated deep-learning techniques, have created a new class of fraud mechanism: "Identity Theft 2.0." However, some researchers have mistakenly categorized this as data leakage. Preibusch et al. (2016) stated that "leakage" is a situation in which online stores forward data about consumers and purchases to payment systems.

2.2 GDPR in online shopping

There are not many works published on the adaptation of GDPR in e-commerce. Since the new regulation was established in May 2018, there is still more research to be done in this area. What is available now are mainly assumptions, e.g. how aware the consumers are of this new environment and how online stores should be prepared. Presthus and Sørum (2018) in their survey asked Norwegian citizens how they are informed about the incoming GDPR. Results showed that they are highly aware of new rules and it concerns their privacy. Another finding was that consumers are well aware that they give a lot of private data to online stores. Polański (2018) described challenges related to regulating e-commerce in the EU. On the one hand, there are rules of the country of origin and, on the other hand, there is the Electronic Commerce Directive given by the EU.

Pape et al. (2018) outlined the requirements of a privacy-aware online shopping platform and suggested several architectures for building such a platform. They compared them according to four dimensions: privacy threats, transparency, usability, and compatibility with existing business models. Radu et al. (2018) proposed a structured conceptual framework for consumer protection in e-commerce based on the analysis of literature in the field. They analyzed more than 100 papers, with 30 being considered as most relevant. However, all of them were published before GDPR was released. Still, it is a valuable analysis of literature. Collins and Klotz (2018) analyzed the GDPR and its influence on the Brexit. They noticed that half of the selected companies are not well prepared for GDPR. Boban (2017) described digital consumer trends with the regulation overview of consumer protection rights in the Republic of Croatia and in the EU.

2.3 Payments in online shopping

Recent studies on e-commerce have opened discussions on a few interesting issues considering online payment systems applied. For instance, Gao and Waechter (2017) analyzing the market of such systems distinguished mobile payment (m-payment) systems from other options of online payment. Observations show that despite the promising possibilities of m-payment, its adoption remains low. Yan and Yang (2015) state that such low adoption is caused by such reasons as: risk connected with mobile networks being vulnerable to hacker attacks due to their virtuality and lack of control; small screens, low resolution and inconvenient input of mobile gadgets making it difficult for people to operate the information quickly. In the research of Deufel and Kemper (2018), it is highlighted that these days users of online payment systems

are facing a problem of wide choice: while traditional shopping only gives us the options of cash or a card, new digital payments vary much more - like PayPal, mobile ApplePay system or even digital currency like Bitcoin. Yet, no matter the type of the payment system, the question of a risk coming when you pay online remains, making internet security and trust of consumers the issues of major importance for online payment systems developers (Yang et al., 2015).

2.4 Shopbots in online shopping

Another valuable element of the processes conducted in electronic commerce is a shopbot. Such a bot is a shopping system that gives consumers a possibility to compare prices for particular products or services and chose the best suitable offer. The list of online stores is based on the price specified for a product by each store, usually showing the cheapest product on top as the most popular. However, having a very clear value for consumers, shopbots still have a few disadvantages which form limitations in e-commerce. Shopbots only access the stores that have paid a fee to be included in the search. Thus, some online stores, which may have goods of better quality, are excluded from the list the consumers obtain. Ellison and Ellison (2009) proved that internet search in general and shopbots, in particular, affect not only online commerce but also the "brick and mortar" industries like car manufacturers or airlines.

An interesting observation about consumer behavior using shopbots was made by Dulleck et al. (2011). It is stated that consumers tend to make decisions based on the "consider-then-chose" model, developed by Gaskin et al. (2007) and Yee at al. (2007). Due to this model, a consumer first creates a list of features a product should possess, then thoroughly compares several products by these features, and only then comes up with the decision to buy. A psychological aspect of using shopbots is discussed by Fasli (2006). Users are often uncertain about what product to buy and by employing a shopbot they can shift some of the psychological cost of making a decision to this bot. In case the decision turns out to be not a very good one, the consumer can minimize the psychological risk in the purchase decision by blaming the shopbot instead. Tang et al. (2010) conducted research dedicated to the impact of shopbots popularity on the price policy of online stores. Their analysis showed that with more shopbots the power of consumers has grown and in conditions of high competition online stores are adjusting their prices to be more attractive for consumers. Increasing shopbot use by 1% decreases the price level by approximately $0.45.

2.5 Security in online shopping

One more cornerstone of electronic commerce and, particularly, its security, is server authentication – the property which allows online stores to ensure the servers with which they communicate are truly what they say they are. Server authentication is made possible by the globally distributed public key infrastructure, which works in connection with other protocols like transport layer security and secure sockets layer (SSL) - to provide secure communication (Zhang et al., 2014). It is proven that SSL protocol is vulnerable to a variety of security attacks since the technique is not fully autonomous and user awareness still has a remarkable role in controlling and accepting invalid certificates (Tarazan and Bostan, 2016).

McCole et al. (2010) noted that, in the context of B2C relationships, security during online purchase was important for the consumer to accept any risk associated with a transaction. Kim et al. (2010) examined issues related to e-payment security from the viewpoint of customers and found that perceptions of the security of e-payment systems have become a major factor in the evolution of e-commerce in markets. Payment systems are often considered difficult in e-commerce, especially in the context of cross-border online shopping. There are different kinds

of payment systems available for online sellers. These include the credit, debit, and virtual cards, as well as new technologies like e-wallets, e-cash, mobile payment, e-checks, and cash on delivery (Ming-Yen Teoh et al., 2013). On the basis of the literature analysis the authors have come up with the following research questions (RQs):

RQ1: Do online stores in Poland and Ukraine have the same policies as for personal data protection and server security?
By stating the RQ1 the authors are interested in comparing and revealing the differences (if any) between policies in online stores in Poland and Ukraine. Especially those considering personal data protection and server security are in the area of interest.

RQ2: Do all online stores in Poland and Ukraine follow the rules of e-commerce policy?
By stating the RQ2 the authors would like to see and check whether online stores in Poland and Ukraine are respecting and following current rules of e-commerce policy.

RQ3: Is there a significant difference between Polish and Ukrainian e-commerce policy?
Based on the debate above, there are differences in regulations, policies, and other government acts. The authors would like to study to what extent these differences are impacting e-commerce policy in online stores in Poland and Ukraine.

3 Hypotheses Development

This section contains hypotheses development for four factors: terms of service/privacy policy adjusted to GDPR, usage of well-known payment systems, presence in local price comparison engines, and security as SSL certificate and HTTPS encryption. For all of the hypotheses, thorough literature research was conducted.

3.1 Terms of service/privacy policy adjusted to GDPR

Terms of service or privacy policy are documents that inform consumers about how they can use a website and what rights and duties they have. In European legal regulations for e-commerce, there are mandatory elements for e-commerce websites. To obey European legislation on e-commerce a website must notify consumers of a series of important aspects like: pre and post-contractual information; withdrawal period; usage of cookies; data protection. In pre-contractual information, an online store must tell a consumer how order procedures regarding products or services are implemented. A consumer must know about the technical means available to exercise the right to modify, correct, or eliminate information. An online store must be clear about its terms of use – as well as indicate how electronic documents containing information on the vendor, consumer, products, or services are stored. In post-contractual information, an online store must confirm all electronic purchases by notifying the consumer within 24 hours.

These notifications can be delivered electronically or by any other means indicated during the order procedures. The only requirement is that the method chosen must allow the consumer to save the notification. Under the directive on consumer rights (European Parliament, 2011), consumers have 14 calendar days to exercise their right to withdraw from the order if they are not satisfied with the product. The online store must inform the consumer of this right. If the right is not clearly stated, the consumer will have a longer period of 12 months. An online store must have cookies policy informing the consumer that cookies are being used when the website is accessed. Gathering consumers information (via registration, placing orders, or contact forms) is allowed only if consumers are notified about where personal data are being registered and which management tools they may use for future access, modification or cancellation. All

of these policies are designed to offer a higher level of user security for consumers browsing online stores.

In Poland several acts regulate the presence of the above-mentioned documents in an online store. The last national act was established on December 25, 2014, and strictly concerns online stores. It implements the European directive on consumer rights into the Polish legal system. According to these principles, the consumer should be fairly informed about all rights and obligations at the latest when submitting an order. This means that all information required by the act should be included in the content of the online store website. The act introduces a 14-day period for the consumer to submit a statement on withdrawal from the order placed at a distance (so far it was 10 days) together with a ready-to-use model statement of withdrawal from the order.

Until now, there was no such a model, some online stores created it for their needs, others did not include it, limiting themselves only to providing information about the right to withdraw from the contract. An online store is obliged, however, not later than within 14 days of receipt of the declaration on withdrawal from the order, to return the consumer all payments, including the cost of delivering the goods (only the cost of the cheapest standard delivery method). The act imposes an obligation on the online store, at the latest when the consumer wishes to be bound by the order, to obtain the consumer's explicit consent for each additional payment that exceeds the agreed payment for the main order. In 2018 a new General Data Protection Regulation (GDPR) policy was implemented (European Parliament, 2016). Such regulations are directly applicable in an EU-member country, and therefore do not require implementation in its legal system. Based on these policies and regulations the authors state hypothesis 1: Terms of services and privacy policies are updated to the last GDPR in Polish online stores.

As for Ukraine, before 2015 no particular document regulated electronic trade in the country. Only that year the Law on Electronic Commerce (Legislation of Ukraine, 2015) was adopted by the Ukrainian government, specifying the rules of conducting electronic transactions and clarifying the notion of online stores. The buyer-seller relationship in online stores is controlled by the Law on Consumer Rights Protection (Legislation of Ukraine, 1991), while consumer rights are also secured by the Law on Protection of Personal Data (Legislation of Ukraine, 2010). Under the legislation, the conclusion of electronic transaction requires (a necessary minimum) the name of the product or service as well its price to be given on the store web page. Additionally, information about the following terms may be included in the electronic agreement: prepayment, replacement of the ordered goods, ways of buyer-seller communication during the transaction realization, the procedure in case of consumer providing incorrect data. For the electronic agreement, the address of its conclusion is the address of the legal entity (seller’s office) or the seller’s private address (as an individual entrepreneur).

Once a consumer makes his order, he must immediately receive confirmation of its acceptance and must be informed of the precise terms of the agreement. An email letter containing product characteristics, price, and delivery terms is considered as a sufficient confirmation document. The legislation states that, if requested, a document confirming product quality (certificate of conformity, hygienic conclusions, etc.) must be available for a consumer. Under the Law on Consumer Rights Protection, a consumer can return goods to the store without justification, in case he informs the store within a 14-day period from receiving the order. In such a situation the legislation provides for 30 days, within which the product should be received back by the online store and the money should be returned to the consumer. The costs of goods being sent back to the store (in case any delivery service is used) are covered by the store itself. If the

money is not returned within 30 days, for each subsequent day a penalty of 1% of the value of the product is charged from the store. The Law on Protection of Personal Data states that personal data of a consumer can be processed only when he has agreed on it. The Law on Electronic Commerce adds that the moment a consumer registers in an online-shop information system is the moment he agrees on having his personal data gathered and processed. The data is processed transparently and openly, in correspondence to the objective of such data processing. Sharing consumer's personal data with third parties as allowed only in situations, specified by the Law on Protection of Personal Data and only for the needs of national security or human rights. Based on these facts hypothesis 2 is formulated:
Terms of services and privacy policies are updated to the last GDPR in Ukrainian online stores.
Hypotheses 1 and 2 complement RQs 1 and 2.

3.2 Usage of well-known payment systems

PayU, Dotpay, Przelewy24 are Polish online payment operators (Polasik and Fiszeder, 2010). These operators give the option of making payments over the Internet (Sokołowska, 2015). Usually, payments can be sent via credit card, bank transfer, or electronic wallet (Apple pay, Google pay, or Blik). Blik is a Polish mobile payment system launched on the initiative of several banks. For now, it operates only in Poland. Blik payments are known for safety. For each standard transaction a one-time, six-digit code is generated, and it can only be used within two minutes. A consumer also confirms each transaction in the mobile application, seeing the amount and the name of the acceptance point. Based on these common payment solutions hypothesis 3 is stated: In Poland online stores clearly inform clients about secure electronic payment options.

In Ukraine electronic commerce payments are be conducted under the laws on Payment Systems and Funds Transfer (Legislation of Ukraine, 2001), on Financial Services and State Regulation of Financial Service Markets (Legislation of Ukraine, 2002) and under several other laws and regulations of the National Bank of Ukraine. Payments may be done using payment instruments, electronic money, by money transfer or by cash payment (under the legislation on the execution of cash and cashless payments). The methods, terms and procedures of payment are defined in the electronic agreement, within the framework of the above-mentioned (and other) legislations. The Ukrainian hryvnia (UAH) as the monetary unit of Ukraine is the only legal means of payment in Ukraine, accepted by all physical and legal entities without any restrictions throughout the territory of Ukraine for conducting funds transfers. Most transactions in Ukrainian e-commerce are being paid using money transfers directly from one bank account to the other. The major banks presently operating in Ukraine have developed user-friendly mobile applications, which allow them to conduct payments and send money wherever you want in the shortest time. Yet, some specific non-bank online payment systems can be observed in the market. Among them we can distinguish the WebMoney Transfer (10 years in the market; secure payments; each user has his wallet of electronic cards with a currency equivalent to real money), UkrMoney (2 years in the market; cooperates with PrivatBank - the major Ukrainian bank; a user has 3 accounts - in hryvnia, euro, and Russian ruble), Interkassa (can connect any payment system to online store or website; takes a small commission from the payment received for the goods; does not gather personal data from consumers, which guarantees the security of transactions). Based on these common know payment methods hypothesis 4 is formulated: In Ukraine online stores clearly inform clients about secure electronic payment options. Hypotheses 3 and 4 complement RQs 2 and 3.

3.3 Presence in local price comparison engines

In many European countries there exists at least one price comparison engine - the so-called shopbot. Shopbots are services that aggregate offers from online stores about the same product and place them on one page. Order placement is usually conducted according to the price of the product. Shopbots collect fees from online stores for being in their index. This fee could be calculated on a cost per click model or other provision models. Ellison and Ellison (2009) conducted a study where they noticed that shopbots are the key element of online stores environment. Shopbots can help consumers decide what to buy and enhance their shopping experience (Fasli, 2006). Shopbots verify some basic facts about the online store and sign the agreement. It is one form of ensuring customers that an online store can be trusted.

Price comparison engines in Poland are: Ceneo.pl, Skąpiec.pl, Okazje.info.pl, and Nokaut.pl. In Ukraine the most popular comparison engines are: Hotline.ua, Price.ua, and Sravni.ua. Based on the usage of shopbots by online stores, the authors have formulated two hypotheses stating that each online store is at least present in one shopbot (price comparison engine). Hypothesis 5 is: Online stores in Poland are present at least in one leading price comparison engine; and hypothesis 6 is: Online stores in Ukraine are present at least in one leading price comparison engine. Hypotheses 5 and 6 complement RQ 2.

3.4 Security as SSL certificate and HTTPS encryption

Online stores are scanned with the SSL Labs tool [ssllabs.com]. SSL Labs test is a free online service that performs a deep analysis of the SSL configuration of any web server on the public Internet. SSL Labs also issues detailed information about the expiration date of the certificate, the level of trust of the certification authority, and server settings in four categories: certificate, protocol support, key exchange, and cipher strength. Each of these four categories gets its score, between 0 and 100. Then SSL Labs combines the overall grade (from A to F) based on specific categories. Reduction of the grade is based on a series of rules to handle some aspects of server configuration in case the rules encounter unwanted features. Some rules increase the grade (to A+) to reward exceptional configurations.

Nowadays, browsers such as Firefox (v. 64+) and Chrome (v. 71+) alert consumers, if the online store does not use HTTPS encryption (Strzelecki, 2019). In this way, browsers' producers force online stores to provide SSL certification. Online retailers who have an SSL certificate assure consumers that personal data which is needed to be given to the store when placing orders will not be disclosed to third parties. It concerns the data of a person making an order, address of delivery, and information on the selected payment method. Following this forced alert on a lack of use encryption while sending data to an online store, two hypotheses were formulated, stating that online stores are following this global recommendation. Hypothesis 7 is: Online stores in Poland are using SSL certificates, and hypothesis 8 is: Online stores in Ukraine are using SSL certificates. These hypotheses complement RQs 2 and 3.

4 Data

This section presents the analyzed sample of data about online stores. The research, described in the paper, was conducted in January 2019. Forty Polish and forty Ukrainian online stores were included in the study. Websites were visited using a web browser and were checked with benchmarking software.

The study involved 40 online stores registered in Poland and 40 online stores registered in Ukraine. The selected shops operate in four different industries: those selling consumer electronics (mainly computers, smartphones, TVs, home cinema and home appliances);

entertainment sphere (books, music, games, and presents); fashion stores (clothes, shoes, bags, jewelry); and those selling accessories for the newborns, children, and mothers.

The lists of Top 10 Polish and Top 10 Ukrainian online stores were formed based on the information from the Similarweb tool [pro.similarweb.com]. This web analytics service provides information on website global rank, as well as country and category rank. It also allows to see the number of monthly visits at a particular website. The top lists were formed with the help of monthly visits data (for the last three months - October - December 2018). The data allowed to select the most popular online stores representing each of the four industries, distinguishing them from a large variety of stores on the market.

Each of the online stores was analyzed in terms of its compliance with technical requirements facilitating selling goods abroad. The following four criteria were tested: possession of current terms of service according to last GDPR, usage of electronic payments such as credit cards and micropayments, presence in local price comparison engines, safety in the form of HTTPS encryption. The list of the online stores is to be found in the Appendix.

Firstly, the presence of TOS was manually checked by visiting the pages with published TOS. Secondly, the presence of separately published pages with payment methods was manually checked by searching and visiting them. Thirdly, the presence of online stores in shopbots was examined. Every online store was searched for in each of the selected shopbot engines. The last step was checking SSL certificates. SSL Labs was used to check whether online stores are using SSL certificates and what type of security they provide. SSL Labs gave grades from A to F for security settings. Online stores listed in the Appendix are the top 10 shops in four different industry sectors: electronics, entertainment, fashion, and goods for kids.

5 Discussion

The observation was taken in January 2019 and the results are presented further. In Poland 39 stores have terms of service published on the website, one has only the privacy policy document. 32 online stores have the date stamp in TOS. After manually checking TOS without date or with the date older than the period of GDPR implementation (April-May 2018), 5 stores were revealed having TOS not adjusted to GDPR. 33 online stores have a separate URL web page with detailed information about payment options. Remaining seven only have information about payment options in TOS, usually as a chapter. 33 online stores are present in Ceneo shopbot, 17 stores are present in Skąpiec shopbot, 11 stores are present in Okazje shopbot and 10 stores are present in Nokaut shopbot. 39 online stores are using a secure protocol and SSL certificate, whereas 1 online store does not have it. In Ukraine results are similar. 39 online stores have an SSL certificate, whereas 1 online store does not. Checking all websites in SSL Labs tools gave detailed results of security grades for these certificates. The list of grades is presented in Table 1.

Table 1. Evaluation of SSL certificates.

SSL Labs grade	Polish online stores	Ukrainian online stores
A+	6	4
A	28	29
B	2	3
C	2	2
F	1	0

T	0	1
None	1	1

Source: https://www.ssllabs.com/ssltest/

In the observation of Polish online stores, it turned out that the vast majority have TOS, which is very expected by consumers. However, one online store (bonprix.pl) does not have TOS - only the privacy policy page with terms adjusted to GDPR. This means Hypothesis 1 was confirmed. However, it is noticeable that 5 online stores did not have TOS updated to GDPR. It is very surprising, since the information campaign about GDPR across Europe was very clear and eye-catching. The situation for Ukrainian stores differs significantly from the one in Poland. From the 40 online stores analyzed 12 do not place any information on TOS or privacy policy. The minimum these stores give is (in some cases) information on reclamation guarantee for their goods. Yet none of the stores has updated its privacy policy recently. Being a non-EU member, Ukraine does not follow GDPR standards. As it was mentioned before, e-commerce is controlled by local legislation. Thus, Hypothesis 2 for Ukrainian online stores was disconfirmed.

All of the Polish online stores are using well-known payment systems like credit cards, PayPal, micropayment, and mobile payments. 83% publish a separate information page with detailed payment options. Thus Hypothesis 3 for Poland was confirmed. The study of 40 Ukrainian online stores has shown that 100% of them provide information about payment options as a separate web page, which is very easy to find. All of the stores use credit card transactions as the major way of payment; most of them also allow paying in cash when receiving the goods. This conclusion allows to state that Hypothesis 4 for Ukrainian e-commerce was confirmed.

Out of 40 Polish stores, 83% are using price comparison engines. In Poland there are 4 such engines (Ceneo, Skąpiec, Okazje, and Nokaut). The presence of each online store was checked in each shopbot. Cooperation with such services increases credibility of online stores. Three price comparison engines publish landing pages for each online store which is included in such an engine. The landing page usually contains information such as name, owner, address, phone number, email of the online store. The key element of this kind of landing page is the part that contains reviews from consumers, who already purchased goods in this store. Here Hypothesis 5 was confirmed. For the analysis of Ukrainian comparison engines cooperating with the Top 40 online stores, three engines were selected (Hotline.ua, Price.ua, and Sravni.ua). The results have shown that only 45% of the stores can be found in these comparison engines, with 44% of them being found only in one engine and 56% being present in all three engines. Such results allow to state that Hypothesis 6 was disconfirmed. Moreover, unlike Polish comparison engines, Ukrainian ones do not have specific landing pages for online stores - the consumers are directed straight to the store website.

The conducted study shows that not all Polish online stores have and use an SSL security certificate, though it may seem that all online stores should be doing so. Popular internet browsers display information on websites if they do not have the certificate to inform consumers that the connection is not secure - at the point when the consumer is entering details into the order form. Despite this fact, one of the online stores did not use SSL. According to these facts Hypothesis 7 was confirmed. The research on SSL security certificates in Ukrainian online stores has revealed that only 1 of 40 stores has no certificate. Hypothesis 8 was confirmed. Moreover, security grades for these stores are rather high in 90%.

Apart from confirming 6 hypotheses of the 8 formulated, the research has allowed answering the research questions, set in the beginning. It was revealed that online stores both in Poland

and Ukraine have a set of personal data protection rules which they have to follow, yet in Poland they come out of GDPR, while in Ukraine they are set by local legislation system. There is no significant difference found between Polish and Ukrainian server security and online payment systems. However, it turned out that usage of price comparison engines in Polish electronic commerce is far more developed than in Ukrainian one. Calculation of the number of Polish and Ukrainian stores giving information about TOS and privacy policy (although they initially differ due to the legislation) has allowed stating that online stores in both countries in most cases follow the rules of e-commerce policy. Generally, the authors did not observe significant differences between policy on electronic commerce in two countries, however, it can be claimed that privacy policy in Poland is more strict (due to the implementation of GDPR).

6 Conclusions

This section contains contributions, practical implications of the research, as well as limitations and further research description.

6.1 Contribution

This research can contribute to the literature on online shopping behavior from the following perspectives. First, from security and trust perspective. GDPR was established to increase protection of personal data in the online environment. Consumers doing online purchases are expecting their personal data to be secured and not released to third parties. From one point of view, SSL certificates and HTTPS encryptions ensure that data being sent to an online store is protected and cannot be disclosed. From the other point of view, online stores are processing this data only in the ways GDPR allows it. However, it occurs that GDPR is applied only in EEA countries. Online stores in other European countries do not follow it. They apply only national regulations. Second, the shopbots which operate on the local market are extremely used by online stores. Online stores often use not one price comparison engine but are present in all of them on the local market. The results of the study suggest that online stores with higher visibility are using more than one price comparison engine. Third, online stores should give clear information about payment methods. If a consumer is not sure which forms of payment are available, he should be able to find detailed information about them easily. Thus, online stores need to design their websites in a way that shows paths to the most necessary information like payment methods.

6.2 Implications

In recent years, consumer awareness of secure online e-commerce transactions has increased and become an essential part of the e-market. Because of this awareness consumers search for clear identification of the fact that online store is secure and there is no risk in making purchases. Online stores can show to their consumers that they recognize these needs. This study empirically explores the relationship between online stores' perception and consumers' readiness to buy.

There are three practical findings. Firstly, part of online stores does not stay only on regulations demanded by GDPR. A lot of TOS in online stores have signs of further updates after GDPR implementation. Secondly, online stores are securing pages due to recent changes in web browsers. Consumers are willing to see obvious signs of security like SSL certificate and HTTPS encryption. Without them, consumers are warned by their browser that there is a lack of security. Thirdly, online stores often use price comparison engines. However, if there is one leader in the engines market, most of them are present in this leader shopbot. Less than half of online stores are using all of the available price comparison engines. These findings have significant practical implications.

Theoretical, more abstract, implications of this study are the following. First, is from the perspective of consumer-security awareness. Consumers are used to the current process of online shopping. Users expect that the online store is secure. However, this expectation is based mainly on the fact that users have not suffered from a lack of security in online stores. Second, is from the consumer-trust perspective. Consumers generally put trust in online stores. But if an incident happens to one online store and consumers' trust in this particular store is lost, they still have general trust in online shopping.

6.3 Limitations

This study has several limitations. First is that the observation was conducted only in several industries. It does not reflect the whole e-commerce market in the country. Top 10 online stores with the highest visibility representing four industries were the subject of the study, however, this sample size cannot adequately represent these industries. It is not reflecting all lower visibility online stores. To make the conclusions more convincing, data from more industries will be collected in the future.

Second, the observation was conducted only in two countries, Poland and Ukraine. These are two European countries; however, one is a member state of the EU, the other is not. This observation does not reflect online stores in other European countries, especially members of EEA. GDPR was adopted by all the UE members on 25th May 2018 and on 6th July by three of four EFTA States (Iceland, Liechtenstein, and Norway). GDPR has broad influence, not only on members that adopted it. It can be seen when foreign websites are blocking users from the EEA area due to them not conforming GDPR. Data reflecting more European countries will be collected for further investigation of the role of GDPR in online shopping.

Third, although each online store was observed in terms of the same factors, there are still unobservable factors such as brand recognition across online stores, which might influence consumers. Further studies will retrieve more data to address this issue.

6.4 Future research

One direction of the further studies will be investigation of differences observed in various industries. Each of the top 10 online stores has different averages of having updated terms of service, pages clearly informing about payment options, e-commerces being in shopbots, and having an SSL certificate with a good grade. It is observable that online stores with higher visibility care more about those four factors. Less visible online stores sometimes have a lack of these factors. Further studies could analyze the reasons for stores having those four factors.

Another direction of research could be the analysis of consumers' trust changing when a personal data leak from an online store happens. In recent days, one of the analyzed online stores, morele.net, was a victim having personal data of 2.2M polish consumers hijacked. Passwords, email, names, addresses, even completed credit application leaked from this online store after they refused to pay ransom. Further research may compare the actions taken by online stores after such incidents.

Appendix

List of 40 Polish and Ukrainian online stores in four industry sectors (electronics, entertainment, fashion, goods for kids) based on the analysis on similarweb.com. Similarweb collects data about visibility of domains on the Internet. The most 10 visible were chosen from each industry sector for study.

Polish stores		Traffic	Ukrainian stores		Traffic
Electronics					
1	https://www.euro.com.pl	17.15M	1	https://rozetka.com.ua	59.47M
2	https://www.morele.net	10.17M	2	https://allo.ua	11.83M
3	https://www.x-kom.pl	10.01M	3	https://www.citrus.ua	11.09M
4	https://mediamarkt.pl	9.369M	4	https://comfy.ua	7.482M
5	https://www.komputronik.pl	6.060M	5	https://www.foxtrot.com.ua	5.478M
6	https://www.emag.pl	3.799M	6	https://f.ua	4.475M
7	https://www.oleole.pl	3.434M	7	https://www.moyo.ua	3.398M
8	https://www.neonet.pl	2.692M	8	https://eldorado.ua	3.082M
9	https://www.electro.pl	1.590M	9	https://www.mobilluck.com.ua	1.362M
10	https://redcoon.pl	583,532	10	https://tt.ua	204,809
Entertainment					
1	https://www.empik.com	14.14M	1	https://www.yakaboo.ua	1.969M
2	https://www.taniaksiazka.pl	2.485M	2	https://www.bookclub.ua	733,084
3	https://bonito.pl	2.459M	3	https://www.bodo.ua	681,581
4	https://merlin.pl	1.665M	4	https://balka-book.com	171,318
5	https://www.gandalf.com.pl	1.460M	5	https://bukva.ua	162,623
6	https://helion.pl	1.033M	6	https://nashformat.ua	123,704
7	https://ksiegarnia.pwn.pl/	808,115	7	https://www.podaro4ek.com.ua	104,141
8	https://www.ravelo.pl	600,005	8	https://bookzone.com.ua	86,395
9	https://www.inbook.pl	240,267	9	http://www.librabook.com.ua	38,291
10	https://www.matras.pl	210,099	10	http://knigoland.com.ua	37,762
Fashion					
1	https://www.czasnabuty.pl	583.210	1	https://kasta.ua	6.026M
2	https://www.zalando.pl	10.45M	2	https://leboutique.com	2.034M
3	https://www.eobuwie.com.pl	8.955M	3	https://www.lamoda.ua	1.986M
4	https://www.bonprix.pl	5.213M	4	https://www.bonprix.ua	1.126M
5	https://www.decathlon.pl	4.402M	5	https://answear.ua	791,982
6	https://answear.com	2.295M	6	https://clasno.com.ua	209,635
7	https://www.topsecret.pl	1.595M	7	https://alisa.ua	191,449
8	https://50style.pl/	878,65	8	https://modoza.com	174,728
9	https://ebutik.pl/	699,38	9	https://sportsterritory.com.ua	149,451
10	https://www.spartoo.pl	339,663	10	https://depstor.com	61,951
Kids					
1	https://www.smyk.com	4.810M	1	https://panama.ua	1.101M

2	https://www.51015kids.eu	1.544M	2	https://bi.ua	589,711
3	https://pl.coccodrillo.eu/	475,094	3	https://antoshka.ua	506,402
4	https://endo.pl	340,594	4	https://pampik.com	437,886
5	https://www.babyland.pl	223,353	5	https://toys.com.ua	262,536
6	https://dino.sklep.pl	187,609	6	https://spok.ua	135,903
7	https://www.bobowozki.com.pl	180,945	7	https://shop.mamindom.ua	105,238
8	http://www.sklep-tosia.eu	166,998	8	https://karapuzov.com.ua	96,765
9	https://toysrus.pl	118,551	9	https://goodtoys.com.ua	55,923
10	https://www.tomi.pl	101,056	10	https://kapitoshik.ua	53,084

7 References

Akroush, M.N. and Al-Debei, M.M. (2015), "An integrated model of factors affecting consumer attitudes towards online shopping", *Business Process Management Journal*, Emerald Group Publishing Limited, Vol. 21 No. 6, pp. 1353–1376.

Al-Debei, M.M., Akroush, M.N. and Ashouri, M.I. (2015), "Consumer attitudes towards online shopping: The effects of trust, perceived benefits, and perceived web quality", *Internet Research*, Emerald Group Publishing Limited, Vol. 25 No. 5, pp. 707–733.

Al-dweeri, R.M., Obeidat, Z.M., Al-dwiry, M.A., Alshurideh, M.T. and Alhorani, A.M. (2017), "The impact of e-service quality and e-loyalty on online shopping: Moderating effect of e-satisfaction and e-trust", *International Journal of Marketing Studies*, Canadian Center of Science and Education, Vol. 9 No. 2, pp. 92–103.

Arora, R. and Muttoo, S.K. (2018), "Privacy and security concern of customers doing online shopping – an analytical study", *International Journal of Advanced Research in Computer Science*, Vol. 9 No. 1, pp. 122–136.

Boban, M. (2017), "New digital consumer trends and consumer protection rights challenges of Croatia and EU in information economy", in Yongqiang, L., Hunjet, A. and Roncevic, A. (Eds.), *20th International Scientific Conference Economic and Social Development*, pp. 493–500.

Celik, H. (2016), "Customer online shopping anxiety within the Unified Theory of Acceptance and Use Technology (UTAUT) framework", *Asia Pacific Journal of Marketing and Logistics*, Emerald Group Publishing Limited, Vol. 28 No. 2, pp. 278–307.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. and Raghav Rao, H. (2016), "Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults", *Decision Support Systems*, Elsevier Science Publishers B. V., Vol. 83 No. C, pp. 47–56.

Chen, Y. and Chou, T. (2012), "Exploring the continuance intentions of consumers for B2C online shopping", *Online Information Review*, Emerald Group Publishing Limited, Vol. 36 No. 1, pp. 104–125.

Collins, D.A. and Klotz, E. (2018), *GDPR and E-Commerce*, London.

Deufel, P. and Kemper, J. (2018), "Online Payment Method Selection: The Habitual Choice of Deferring Payment", *ICIS 2018 Proceedings*, available at: https://aisel.aisnet.org/icis2018/implement/Presentations/1 (accessed 20 March 2019).

Dulleck, U., Hackl, F., Weiss, B. and Winter-Ebmer, R. (2011), "Buying Online: An Analysis of Shopbot Visitors", *German Economic Review*, John Wiley & Sons, Ltd (10.1111), Vol. 12 No. 4, pp. 395–408.

Ellison, G. and Ellison, S.F. (2009), "Search, Obfuscation, and Price Elasticities on the Internet", *Econometrica*, John Wiley & Sons, Ltd (10.1111), Vol. 77 No. 2, pp. 427–452.
European Parliament. (2011), "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Co", European Parliament, Brussels.
European Parliament. (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da", European Parliament, Brussels, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (accessed 27 January 2019).
Eurostat. (2018), "E-commerce statistics for individuals", available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals (accessed 27 January 2019).
Fasli, M. (2006), "Shopbots: A Syntactic Present, A Semantic Future", *IEEE Internet Computing*, Vol. 10 No. 6, pp. 69–75.
Gao, L. and Waechter, K.A. (2017), "Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation", *Information Systems Frontiers*, available at:https://doi.org/10.1007/s10796-015-9611-0.
Gaskin, S., Evgeniou, T., Bailiff, D. and Hauser, J. (2007), "Two-stage models: Identifying non-compensatory heuristics for the consideration set then adaptive polyhedral methods within the consideration set", *Proceedings of the Sawtooth Software Conference*, Vol. 13, pp. 67–83.
Gefen, D., Karahanna, E. and Straub, D.W. (2003), "Trust and TAM in online shopping: An integrated model", *MIS Quarterly*, Society for Information Management and The Management Information Systems Research Center, Minneapolis, MN, USA, Vol. 27 No. 1, pp. 51–90.
Grabner-Kraeuter, S. (2002), "The role of consumers' rrust in online-shopping", *Journal of Business Ethics*, Kluwer Academic Publishers, Vol. 39 No. 1/2, pp. 43–50.
Gupta, A. (2018), "The evolution of fraud: Ethical implications in the age of large-scale data breaches and widespread artificial", *ICT Discoveries*, Vol. 1 No. 1, pp. 12:1-12:7.
van der Heijden, H., Verhagen, T. and Creemers, M. (2003), "Understanding online purchase intentions: contributions from technology and trust perspectives", *European Journal of Information Systems*, Taylor & Francis, Vol. 12 No. 1, pp. 41–48.
Hoffman, D.L., Novak, T.P. and Peralta, M. (1999), "Building consumer trust online", *Communications of the ACM*, ACM, Vol. 42 No. 4, pp. 80–85.
Hongyoun Hahn, K. and Kim, J. (2009), "The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context", *International Journal of Retail & Distribution Management*, Emerald Group Publishing Limited, Vol. 37 No. 2, pp. 126–141.
Kamaladevi, B. and Vanithamani, M.R. (2016), "The Role of E-Security in the Success of the E- Store With Reference To UAE Customers", *International Journal of Business Administration and Management Research*, Research Plus Journals, Vol. 2 No. 1, pp. 12–16.
Khan, F., Rasli, A.M., Yusoff, R.M. and Isa, K. (2015), "Impact of Trust on Online Shopping: A Systematic Review of Literature", *Journal of Advanced Review on Scientific Research*, Vol. 8 No. 1, pp. 1–8.
Kim, C., Tao, W., Shin, N. and Kim, K.-S. (2010), "An empirical study of customers' perceptions of security and trust in e-payment systems", *Electronic Commerce Research*

and Applications, Elsevier, Vol. 9 No. 1, pp. 84–95.
Kim, Y. and Peterson, R.A. (2017), "A meta-analysis of online trust relationships in e-commerce", *Journal of Interactive Marketing*, Elsevier, Vol. 38, pp. 44–54.
Köksal, Y. and Penez, S. (2015), "An investigation of the important factors influence web trust in online shopping", *Journal of Marketing and Management*, Vol. 6 No. May, pp. 28–40.
Lee, J., Park, D.H. and Han, I. (2011), "The different effects of online consumer reviews on consumers' purchase intentions depending on trust in online shopping malls: An advertising perspective", *Internet Research*, Emerald Group Publishing Limited, Vol. 21 No. 2, pp. 187–206.
Legislation of Ukraine. (1991), "Law of Ukraine on Consumer Rights Protection. Document 1023-XII, valid, revision on January 1, 2019".
Legislation of Ukraine. (2001), "Law of Ukraine on Payment Systems and Funds Transfer. Document 2346-III, valid, revision on November 24, 2018".
Legislation of Ukraine. (2002), "Law of Ukraine on Financial Services and State Regulation of Financial Service Markets. Document 2664-III, valid, revision on October 1, 2018".
Legislation of Ukraine. (2010), "Law of Ukraine on Protection of Personal Data. Document 2297-VI, valid, revision on January 30, 2018".
Legislation of Ukraine. (2015), "Law of Ukraine on Electronic Commerce. Document 675-VIII, valid, revision on April 26, 2017".
McCole, P., Ramsey, E. and Williams, J. (2010), "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns", *Journal of Business Research*, Elsevier, Vol. 63 No. 9–10, pp. 1018–1024.
Ming-Yen Teoh, W., Choy Chong, S., Lin, B. and Wei Chua, J. (2013), "Factors affecting consumers' perception of electronic payment: an empirical analysis", *Internet Research*, Emerald Group Publishing Limited, Vol. 23 No. 4, pp. 465–485.
Nilashi, M., Ibrahim, O., Reza Mirabi, V., Ebrahimi, L. and Zare, M. (2015), "The role of security, design and content factors on customer trust in mobile commerce", *Journal of Retailing and Consumer Services*, Pergamon, Vol. 26, pp. 57–69.
Pape, S., Tasche, D., Bastys, I., Grosz, A., Laessig, J. and Rannenberg, K. (2018), "Towards an Architecture for Pseudonymous E-Commerce - Applying Privacy by Design to Online Shopping", in Langweg, H., Meier, M., Witt, B.C. and Reinhardt, D. (Eds.), *SICHERHEIT 2018*, Gesellschaft für Informatik e.V., Bonn, pp. 17–28.
Pappas, N. (2016), "Marketing strategies, perceived risks, and consumer trust in online buying behaviour", *Journal of Retailing and Consumer Services*, Pergamon, Vol. 29, pp. 92–103.
Polański, P.P. (2018), "Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union", *Computer Law & Security Review*, Elsevier Advanced Technology, Vol. 34 No. 3, pp. 562–581.
Polasik, M. and Fiszeder, P. (2010), "Factors Determining the Acceptance of Payment Methods by Online Shops in Poland", *SSRN Electronic Journal*, available at:https://doi.org/10.2139/ssrn.1541202.
Preibusch, S., Peetz, T., Acar, G. and Berendt, B. (2016), "Shopping for privacy: Purchase details leaked to PayPal", *Electronic Commerce Research and Applications*, Elsevier, Vol. 15, pp. 52–64.
Presthus, W. and Sørum, H. (2018), "Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation", *Procedia Computer Science*, Elsevier, Vol. 138, pp. 603–611.
Radu, M., Popescu, S. and Unguraş, D. (2018), "Consumer Protection In Electronic Commerce A Conceptual Framework Based On Literature Review", *Acta Technica*

Napocensis-Series: Applied Mathematics, Mechanics, And Engineering, Vol. 61, pp. 159–169.

Shafiee, M.M. and Bazargan, N.A. (2018), "Behavioral Customer Loyalty in Online Shopping: The Role of E-Service Quality and E-Recovery", *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 13 No. 1, pp. 26–38.

Sokołowska, E. (2015), "Innovations in the payment card market: The case of Poland", *Electronic Commerce Research and Applications*, Elsevier, Vol. 14 No. 5, pp. 292–304.

Strzelecki, A. (2019), "Key Features of E-Tailer Shops in Adaptation to Cross-Border E-Commerce in the EU", *Sustainability*, Vol. 11 No. 6, p. 1589.

Tamimi, N. and Sebastianelli, R. (2015), "The relative importance of e-tailer website attributes on the likelihood of online purchase", *Internet Research*, Emerald Group Publishing Limited, Vol. 25 No. 2, pp. 169–183.

Tang, Z., Smith, M.D. and Montgomery, A. (2010), "The impact of shopbot use on prices and price dispersion: Evidence from online book retailing", *International Journal of Industrial Organization*, North-Holland, Vol. 28 No. 6, pp. 579–590.

Tarazan, Ş. and Bostan, A. (2016), "Customizing SSL Certificate Extensions to Reduce False-Positive Certificate Error/Warning Messages", *International Journal of Information Security Science*, Vol. 5 No. 2, pp. 21–28.

Wan, Y., Ma, B. and Pan, Y. (2018), "Opinion evolution of online consumer reviews in the e-commerce environment", *Electronic Commerce Research*, Springer US, Vol. 18 No. 2, pp. 291–311.

Woźniak, J. (2015), "Trust and E-Commerce in the Ukraine and Poland in the Eyes of Young Urban Professionals", *Review of International Comparative Management*, Vol. 16 No. 2, pp. 159–177.

Wu, I.L. (2013), "The antecedents of customer satisfaction and its link to complaint intentions in online shopping: An integration of justice, technology, and trust", *International Journal of Information Management*, Pergamon, Vol. 33 No. 1, pp. 166–176.

Wu, W.-Y. and Ke, C.-C. (2015), "An online shopping behavior model integrating personality traits, perceived risk, and technology acceptance", *Social Behavior and Personality: An International Journal*, Vol. 43 No. 1, pp. 85–97.

Yan, H. and Yang, Z. (2015), "Examining mobile payment user adoption from the perspective of trust", *International Journal of U-and e-Service, Science and Technology*, Vol. 8 No. 1, pp. 117–130.

Yang, Q., Pang, C., Liu, L., Yen, D.C. and Tarn, J.M. (2015), "Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation", *Computers in Human Behavior*, Pergamon, Vol. 50, pp. 9–24.

Yee, M., Dahan, E., Hauser, J.R. and Orlin, J. (2007), "Greedoid-Based Noncompensatory Inference", *Marketing Science*, INFORMS, Vol. 26 No. 4, pp. 532–549.

Zhang, L., Choffnes, D., Levin, D., Dumitras, T., Mislove, A., Schulman, A. and Wilson, C. (2014), "Analysis of SSL certificate reissues and revocations in the wake of heartbleed", *Proceedings of the 2014 Conference on Internet Measurement Conference - IMC '14*, ACM, New York, NY, pp. 489–502.