Journal of Law & Social Studies (JLSS)
Volume 5, Issue 1, pp 30-41
www.advancelrf.org

Securing the Cyberspace for E-Commerce Industry of Pakistan: A Consumer Protection Perspective

Basharat Aziz
(Corresponding Author)
LLM Scholar,
Department of Law, Times Institute Multan, Pakistan.
Email: chxan@my.bristol.ac.uk

Shaukat Hussain Bhatti
Assistant Professor,
Times Institute Multan, Pakistan.
Email: shaukathussain78682@gmail.com

Abstract

Online buying and selling, which is known as e-commerce, has become very popular round the globe. It is so convenient that almost anything can be ordered online without physically visiting the market. This article throws light on understanding e-commerce and importance of cyber security to the digitalized set up for sustainability of e-commerce. Like protection of a conventional consumer, an e-consumer should also be protected to build his confidence for e-shopping. The article also enlightens the significance of emerging trends of e-commerce and how the world needs to respond to these trends through taking legal and security measures to protect cyberspace from cyber-attacks. An important conclusion is that the current situation of cyber economy of Pakistan and legal cover to e-commerce to protect online consumers is not up to the mark. Many online consumers, using cyberspace for e-shopping, are vulnerable to multiple threats like cybercrimes, violation of consumer rights through misleading advertisements, deceptive sale techniques, lack of redress system and alternate dispute resolution mechanisms etc. Government of Pakistan needs to take strict legal and technological measures for cyber security and confidence building of e-consumer to promote e-commerce industry in Pakistan.

Keywords: E-Commerce, Consumer Protection, Cyber Security, Cyber Economy.

Introduction

Convenience is naturally accepted by everyone particularly when it is time saving and cost-efficient. The life of every human being is not only getting busier but also becoming generally adaptive to technological change. The new routine life trends, especially in the context of buying and selling are emerging rapidly. An important thing about a person is being a consumer in daily life and it feels not less than a blessing when things are delivered at the doorstep while sitting at home. The grocery and other items are just few clicks away if you have a mobile phone in your hand or other electronic device at your home. It is, indeed, a fact that a traditional consumer has been a king of the conventional market, but technology, time and cost saving choices and convenience have brought

revolutionary changes to the consumers' behaviors. This is the reason that an online consumer has more importance than a tradition one in recent era of market digitalization.

Now, consumers' purchase patterns have gradually shifted to e-commerce and online consumer still maintains his e-commerce market kingship in cyberspace. The shopping patterns have brought revolutionary changes in e-commerce industry and developed countries are devising strategies according to online consumer demands. The information and Communication Technology (ICT) has brought the internet users in a global village.

E-Commerce Worldwide

There is no doubt that e-commerce has gradually attracted so many buyers and sellers but a remarkable increase in e-commerce websites was experienced worldwide after COVID-19 pandemic. The following table not only shows the e-commerce statistics but also explains the significance of e-commerce for a cyber economy.

Year	Increase in Online Stores	Annual Growth (%)
2019	9.2 million	-
2020	9.7 million	5.4%
2021	19.8 million	204%
2022	26.2 million	39%

(Source: www.markinblog.com/e-commerce-statistics/)

The statistics in above table show that the number of online websites has almost doubled in the year 2021 as compared to the year 2020 because of outbreak of COVID-19 pandemic. It requires more attention of concerned e-commerce policy makers who need to understand the significance of new trends of e-commerce for cyber economy of a country. The retail e-commerce transactions in 2021 amounted to approximately 4.9 trillion U.S Dollars worldwide, consisting of more than one fourth (27.6%) of the total population of the world. This is indeed a significant number having a great potential of earning revenue if technological and legal flaws of e-commerce are met effectively.

Taking in view the cyber threats to e-commerce, most of the countries in the world are formulating strategies to combat the issues of cybercrimes generally as a whole and specifically for e-commerce. China has taken initiative of introducing statutory laws not only at state level but also at community level so that the security and stability of the digital infrastructure for e-commerce could be maintained. The Chinese administrative regulations and statutory laws address the matters related to criminalization, content filtering and user monitoring etc. Chinese government has also taken strict legal and regulatory measures through investing on cyber security technology and recruiting cyber police (Xingan, 2015).

India also owns a huge e-commerce industry with an immense number of internet users due to having a gigantic population. Indian government has taken some serious steps towards securing cyberspace

and protecting their online consumers. The Consumer Protection (e-Commerce) Rules, 2020 issued under Indian Consumer Protection Act, 2019 deal with the consumer issues related to unfair trade practices, violation of consumer rights, e-business entities and other important concerns of e-commerce (Neelam et al., 2022).

United Nations Conference on Trade and development (UNCTAD) has issued guidelines on various aspects of e-commerce which include data protection, unfair commercial practices, consumer redress, unfair contract terms, online payment security and cross-border e-commerce transactions. The report has also issued policy measures including proper legislation, enforcement of relevant laws, consumer education, fair business practices and cross-border cooperation (UNCTAD, 2017).

Situation of E-Commerce in Pakistan

According to official website of International Trade Administration, USA, Pakistan is ranked at 46th in the global ranking of e-commerce markets, with considerable revenue of 4.2 billion U.S. Dollars. Most of the local firms and sellers use social media, including face book which consists of 49.2 million users, to promote the products they are selling. The famous online websites include OLX, daraz, Food Panda, Zameen, PakWheels etc.

A lot of online consumers prefer 'cash on delivery' mode of payment which is probably to avoid the risk of theft of financial and other sensitive data in cyberspace. The 'cash on delivery' mode of payment is not convenient for e-businesses due to the increase in their operational costs etc. It undoubtedly increases the cost of doing business in the country. Another factor for preference of 'cash on delivery' mode of payment may be that only small number Pakistanis have bank accounts.

The e-commerce in Pakistan is now gradually experiencing an increase in number of transactions via digital payment system as State Bank of Pakistan has introduced 'Raast' payment system. The mobile banks like jazz cash, easypaisa and Upaisa are also being used for online payments now. The step of State Bank of Pakistan to ensure biometric verification of all account holders has been really very effective in order to secure cyberspace. The specific legislation and further strict cyber security measures are needed for secure online payments so that the e-commerce users may be protected from cyber-attacks.

Literature Review

Online buying, selling, exchanging products & services, transferring information etc. by using information technology i.e electronic devices and internet is referred as electronic commerce or e-commerce (Rezk, Barakat, & Saleh, 2017). The first transaction of e-commerce in cyberspace took place in 1982 and the Boston Computer Exchange was first to launch its first platform for e-commerce (Azamat et al., 2011; Boateng et al., 2008). The rapid economic digitalization and social connections are significant reasons due to which the cyber security, cyber risk and cyber threats are getting much importance persistently.

The concept of cyber risk is based on the key characteristics i.e. source, object and impact caused by cyber risk (Grzegorz, 2021). There is no doubt that e-commerce technologies possess a lot of benefits that enable cost-minimization, high competition and mass customization but recent cybercrime threats to e-commerce leave adverse effects on the users (Richard, 2019). This is the need of the time to review risks and scrutinize more reflexivity because it relates to the modification in people's attitudes towards the risk of cybercriminal victimization. It also requires that the work may be done to differentiate between conventional and cybercrimes (Muhammed, 2020). Human beings act and behave differently while they are online. Cyber victimization and cybercrimes both have their own patterns (Jose, 2012).

E-commerce is an advanced mode of buying and selling in daily life that has been developed rapidly in recent years. But, there are also some serious problems related to the online consumers using cyberspace. These users of cyberspace are not protected as they must face several threats from cyber criminals. There is a need for protecting the consumers especially through perfect legal system (Weiwei, 2017). The satisfaction of consumer is very important in this era of growing e-commerce and intention of consumer to buy online is necessary element to promote and encourage e-businesses in the digital market.

Government can play a pivotal role in order to safeguard the interests of e-commerce stakeholders (Martono, 2022). Consumers seek to buy products and services through a safe, secure and reliable online business website which is certified and abides by the rules and regulations of the government (Alkaabi, 2022; Amoako et al., 2020). To control and monitor online services, China has shown great concern and formulated strict policies to ensure cyber security. The important actions taken by China to state stability and secure cyberspace include activity monitoring, content filtering, recruiting cyber police, investing on security technology, surveillance on cyberspace users and imposition of requirements on e-commerce business entities. China has created an effective network to deter cybercrimes (Xingan, 2015).

Electronic frauds are being committed frequently by cyber criminals for economic interests. The consumer's interest requires to be protected in cyberspace. The fields of vital importance of consumer protection include consumer awareness, easy accessibility to related laws and efficient redress system. The apt and accurate information about products is of primary importance as it helps to gain proper benefits and creates awareness about risks of doing a particular transaction. The online stores often show deceptive and misleading behavior in displaying relevant information. The legal measures should be taken by government to ensure regulation of online stores, resolution of disputes between parties and effective redress system. E-commerce legislation needs to be revised to address emerging issues in cyberspace (Dilshad et al., 2020).

The lesser trust of consumers on online suppliers and service providers has been one of the primary reasons which cause decline in e-sales of products and services. The penetration of Information Technology has encouraged more people to buy and sell online using cyberspace. The consumers are more vulnerable to new types of cyber scams (Neelam et al., 2022). Most of the common frauds being committed by using electronic devices include transferring funds electronically by illegal way, fraudulent and fake investments, advance fee schemes etc. (Miha, 2012).

As a vital part in e-commerce, trust means how much a party is vulnerable to other party's actions; the trusting party, being involved in networking, experiences trust in risk-taking activity form (Helge et al., 2020). The exploitation theory advocates an identical viewpoint to the argument of 'weaker party'. This theory emphasizes two reasons of need for consumer protection. Firstly, the consumers are left with little choices but to buy from on terms & conditions made by very large and strong business entities. Secondly, suppliers often manipulate significant discrepancies related to complexity and knowledge for their own benefit and favor (Cockshott and Dieterich, 2011).

The importance of online buying and selling is vivid from the report of PwC's Global Consumer Insight Survey 2020 that, due to social distancing, more people would prefer to buy and sell online in post-COVID time. The mobile shopping trends got more importance according to this report. A traditional consumer is not different from an electronic consumer theoretically but there is a big difference between the both because the mode of operation and the way of enjoyment of services with respect to mode and nature are totally different. The system of redressing disputes and determination of business place is still not out of question. Due to increase in electronic consumers, a comprehensive legislation is required to address e-commerce issues (Ananya, 2018).

The growth of internet facilities has impacted the e-businesses in both positive and negative way. One of the adverse effects of internet technology is the commission of crime in cyberspace particularly in the transactions related to buying and selling online, which creates change in consumer perceptions. This is the reason that the companies doing business online should develop appropriate and effective strategies to mitigate the risks of loss associated with online transactions (Nashrudin et al., 2018).

Conventional way of shopping has now become inconvenient with lesser choices available for conventional consumers in a physical market. E-commerce has revolutionized the shopping experience with a variety of choices in competitive prices. The shopping in virtual world is so convenient that there is no need to go to the market or wander across the stores physically. But, this virtual world has risks and threats to identity theft and data theft from cyber criminals (Abdulah, 2021).

The consumer purchase intention is affected by different factors that are critically and important for consumers (Wang et al., 2019). An analysis shows that most of the internet users protect themselves from being the victims of online banking fraud. The victims of phishing scam were found with insufficient knowledge about cyber scams and shared sensitive personal and financial information with the cyber criminals. It was difficult for them to know the extent of safety and security to safeguard themselves from cyber scams (Jurjen et al., 2016).

E-commerce is an open platform for individuals, businesses and governments to participate while there are several categories of e-commerce depending on the relationship of the participants. The e-commerce categories include Business to Business (B2B), Business to consumer (B2C), Consumer to Business (C2B) and Consumer to Consumer (C2C). When there is a dispute between any of the above category of participants, it is resolved through commercial arbitration (Barbulescu, 2015).

With the rapid development of e-commerce, consumer safety and security has become essential for cyber economy. All stakeholders of electronic market are equally important as consumer protection is important to secure cyberspace (Nicoleta, 2016). E-commerce is growing very fast and making the changes in markets, society, industries and individual businesses. Several job opportunities have been created in the fields of marketing, management, entrepreneurship and information system with the introduction and rapid development of e-commerce. E-commerce has created ease and convenience for both buyers and sellers by increasing sales and decreasing sale costs thus making products and services available in more competitive prices. As compared to traditional consumers, online consumers can have more choices and can also have detailed information about the products or services they are about to purchase. But, online suppliers of e-commerce items have several threats and they must face a lot of legal and cultural challenges in conducting e-commerce (Shafiyah et al., 2013).

Types of E-Commerce

There are so many e-commerce users in cyberspace that can be categorized depending on the nature of their business relationships and the types of transactions they perform as e-commerce users. The common types of e-commerce are as under;

Business to Consumer (B2C)

In this type of e-commerce, the online stores market and sell their products and services directly to the end users. This is the most popular and widely used type of e-commerce. This type is very straightforward in which an e-commerce user can make and complete a B2C transaction i.e. purchasing food from an online food website. There are five business models that are being used in B2C type of e-commerce, which include fee-based, advertisement-based, community-based, online intermediaries and direct sellers.

Business to Business (B2B)

This type of e-commerce is known as B2B when businesses or companies directly market their products and services to other companies or businesses. The B2B model type companies are emphasizing their focus on e-commerce so that they can fulfill the emerging trends of consumer demands.

Business to Government (B2G)

Marketing of products and services directly to the government or its institutions by a company is referred as Business to Government (B2G) category of e-commerce. Companies are normally required bidding on the contracts when requests for proposals are announced by the government. This type of e-commerce works on slower pace due to longer procedural aspects.

Consumer to Business (C2B)

Freelancing is the best example of consumer to business model of e-commerce in which consumers sell their services to the businesses. In this type, consumers sell their goods and services to the companies.

Consumer to Consumer (C2C)

Consumers sell their goods and services to other consumers directly. A third-party online website is used for consumer to consumer transactions. Such business models not only allow consumer to consumer online activity but also allow them to sell the goods on their own prices.

Threats to Consumers in E-Commerce

As the internet has been equipped with more innovations and technological advancements, several cyber scams are being committed by cyber criminals in cyberspace. Some of the cyber scams related to e-commerce are as under;

Fake Websites: There are numerous fake websites in cyberspace which attract people to purchase fake products and services. The products or services they order are never delivered and they must face financial losses. Once the consumers fall victim of the fake websites they avoid using online websites in future which is, indeed, a loss to virtual world of e-commerce.

Phishing: Phishing is a type of online fraud in which cyber criminals use false e-mails claiming that these are associated with reputed companies or organizations. The cyber criminals steal internet user's personal and financial data through phishing.

Data Theft: There is a threat of data theft when a consumer is making a purchase online. Personal data of consumer is shared with the website and it can be accessed by workers of website without the knowledge of the consumer.

Unfair Business Practices: These practices include false advertisements, tied selling, misrepresentation of goods and services, false gift offers, non-compliant standards and deceptive pricing.

Misleading Advertisements: An advertisement is misleading when there is incomplete, false or deceptive information. If important information about the product or service is left out in the advertisement, it will also be a misleading advertisement.

Low Quality Products: It is a common experience that some online stores deliver the goods or services which are in lower quality than those described in advertisements or product information portion. The risk of delivery of low-quality products or services is also associated while purchasing online.

Improper return Policy: The return policy of an online store can play a vital role in making the business successful or otherwise. Some websites do not display complete information about return policy or make it so complicated that it seems returning the product will be in vain.

No Proper Redress System: Convenient, efficient and proper redress system must be introduced if there is a dispute between the transacting parties. E-commerce users must face difficulties when there is no proper redress system under proper legal cover.

Lack of Strict Legislation: Most of the developing countries do not have up to the mark legislation regarding e-commerce and cyber security. Numerous issues of e-commerce are still left unaddressed due to lack of updated and revised legislation. This is also a threat to the consumer buying online.

Lack of Awareness: Another important thing is that many cyberspace users do not have information about cybercrimes or cyber scams. They are soft targets and more vulnerable to cyber-attacks. The victims of cyber-attacks, sometimes, do not know how and where to report the cyber offence.

United Nations and E-Commerce

As e-commerce has grabbed so many buyers and sellers on a faster pace especially during the COVID-19 pandemic, most of the countries have taken it seriously by making their strategies accordingly.

UN Guidelines on Consumer Protection

The United Nations has issued guidelines for consumer protection in its conference on trade and development held in 2016. United Nations, while addressing the issues of e-commerce in guideline number 63, issued guidelines for member states focusing on consumer confidence through effective and transparent strategies and policies by ensuring electronic consumer protection like a traditional consumer.

The guideline 64 throws light on taking into the consideration new features of e-commerce, laying emphasis on consumer awareness regarding rights and responsibilities of both businesses and the consumers. In guideline 65, issues of international nature like adoption of international standards and cooperation across the borders as discussed in the report of Organization for Economic Co-operation and Development (OECD), February 21, 2018.

Recurrent Issues of Consumer Protection in E-Commerce

According to the United Nations Conference on Trade and Development (UNCTAD) report on consumer protection in 2017, three consumer-business relationship phases can identify the issues of consumer protection in e-commerce. The three stages include pre-purchase, purchase and post-purchase. Following are the challenges which are faced by the consumers during each phase.

Pre-Purchase Phase

In this phase the consumer must face access issues to true information about the products and services and regarding suppliers who are supplying the items. Asymmetric information is vivid in e-commerce because of the nature of information technology services and complicated terms and conditions as the

consumer cannot always have timely access to this information and becomes vulnerable to deceptive and misleading behavior. According to the above mentioned UNCTAD report, pre-purchase phase includes the challenges of information requirements and unfair commercial practices including misleading advertisements.

Purchase Phase

There are several threats ahead when an online consumer is about to start or doing buying activity online. During purchase phase the consumers have to face the risks of unfair terms of contracts, insecure payments online, privacy and protection of sensitive data. This is very critical phase for consumer in cyberspace.

Post-Purchase Phase

This is also an important phase as it is related with the challenges which can be faced by e-commerce users after the completion of purchase phase. This phase includes resolution of disputes between parties, redress system, cross-border e-commerce issues and protection of children in e-commerce.

Building Confidence of Internet Users in E-Commerce

The speedy development of e-commerce has attracted many buyers and sellers particularly after the wave of COVID-19 pandemic. The emerging trends show that it is the time of e-commerce and people prefer to save their time and cost in shopping. It is a reality that online buying, and selling is not only easy and convenient but also gives more choices to the users on competitive prices. There is a dire need of system of policies that can foster and build confidence in internet users to confidently use information technology to buy or sell goods and services online.

Existing Legislation in Pakistan

The legal situation in Pakistan to address e-commerce issues is not up to the mark. The existing laws do not cover numerous issues of online stakeholders of e-commerce. Pakistan has made some major legal efforts related to Information Technology by making following legislation.

- Pakistan Telecommunication (Re-organization) Act, 1996.
- Electronic Transactions Act, 2002.
- Prevention of Electronic Crimes Ordinance, 2007.
- Prevention of electronic Crimes Act, 2016.

The above-mentioned legislation was done during last three decades, but the current emerging trends of e-commerce demand more legal and technological efforts to keep up with the new trends. The Pakistan Telecommunication (Re-organization Act, 1996 mainly deals with the appointment of concerned authorities, establishment of companies and their licensing and registration issues. Electronic Transactions Act, 2002, was a bit updated legislation to cover electronic issues as this was the time of early information technology growth phase. This Act addresses the aspects of electronic documentation, certification and consequences of violations.

The creation of Prevention of Electronic Crimes Ordinance, 2007 was a little better version to deal with some of the important issues related to e-commerce as it introduced the strict punishments for different types of misuse of information technology systems. A similar legal document was introduced namely the Prevention of electronic Crimes Act, 2016 which can be considered a further

improvement in addressing cybercrimes including some of the crimes related to e-commerce. There were no clear provisions for e-commerce in any of the above legal documents but now it has become need of the time due to the fast-growing e-commerce trends in Pakistan.

National Policies

Two national level policies of Pakistan are worth mentioning in present circumstances of cyber security and e-commerce. These policies include E-commerce Policy, 2019 and National Cyber Security Policy, 2021. Both the policies show some serious concerns to combat the issues of cyber security and e-commerce in which Pakistan is far behind.

E-Commerce Policy, 2019

Pakistan's e-commerce policy was devised in October 2019 by Ministry of Commerce, Government of Pakistan and it was principally introduced covering the various vital aspects of e-commerce industry. This policy addresses the features of e-commerce which include consumer protection, ICT & telecommunication services, financial inclusion & payment digitization, regulation & facilitation, empowerment of youth & Small & Medium Enterprises (SMEs), taxation structure, data protection & investment, logistics and global connectivity & multilateral negotiations.

The main identified stakeholders of this e-commerce policy include e-businesses, freelancers, regulatory bodies, consumers, financial institutions, SMEs, revenue authorities and cross-border logistic entities. The intention to constitute a National e-Commerce Council is a remarkable feature of this policy. Several steps have been proposed to ensure consumer protection so that the confidence of consumers may be built on e-commerce.

National Cyber Security Policy, 2021

The National Cyber Security Policy was formulated in 2021 by Ministry of Information technology & Telecommunication, which covers a variety of Information and Communication Technology (ICT) related issues. Although it is at infancy stage, but it wraps important areas of ICT related aspects in present scenario. A detailed strategy of securing cyberspace is made at government level to ensure provision of safe, secure and reliable digital infrastructure for ICT stakeholders. A Cyber Governance Policy Committee constituted by the government of Pakistan, is primarily responsible to look into the matters of cyber security.

The Recommendations for Cyber Economy of Pakistan

Pakistan is at 46th position in e-commerce world ranking with the revenue of 4.2 billion U.S. dollars according to the International Trade administration, USA. The number of social media users in Pakistan has reached to 82.90 million which is 36.5% of total population. With such a huge number of social media users, Pakistan can have the advantage to boost her e-commerce by attracting them and giving them confidence on buying online. The mode of payment opted by most of the consumers in e-commerce of Pakistan is 'cash on delivery' and this is one of the factors that shows lack of confidence of consumers about cyber security. The recommendations and measures to improve e-commerce industry in Pakistan can be divided into following major two categories.

IT Related Measures

As the e-commerce is fundamentally based on the system of information technology i.e. electronic devices, internet and software applications etc. so, the system which is being used in e-commerce must be safe and secure in such a way that no cyber-criminal activity could be successful to breach the system. The suppliers must ensure that their websites must be frequently updated leaving no room

for cyber-attacks so that the sensitive data like identity and financial information could be saved from stealing. The timely information technology related measures and strong internet infrastructure for e-commerce would play a vital role in fostering the confidence in internet users of e-commerce which would be beneficial for cyber economy of any country.

Legal Measures

The legal aspect of e-commerce is very important to be considered on urgent basis. The governments need to establish a strong legal system by revising legislation, introducing specific provisions for e-commerce, ensuring the implementation of legal decisions and protecting the consumers. There should also be a redress and dispute resolution system having the strongly supported legal cover from state institutions. These legal steps would play an important role in building the consumer confidence.

Furthermore, both the national policies i.e. e-Commerce Policy, 2019 and National Cyber Security Policy, 2021, for combating cyber security and e-commerce issues, can play very important role in improving e-commerce industry if their execution, enforcement and frequent revisions are ensured at state level.

Conclusion

It is an undeniable fact that the world has changed drastically as economies of the world have embraced huge shifts of buyers and sellers from conventional markets to e-businesses. The markets have evolved in a digitalized way with the rapid growth of e-commerce around the globe. Those countries remained successful that timely considered and addressed the issues in growing phase of e-commerce. Information and Communication Technology played very significant role in growth and development of e-commerce industry.

There are several issues that arise time to time in e-commerce and these issues need appropriate policy measures to be tackled in order to ensure cyber security. The countries have devised their policies to strengthen information technology systems and legal set up to keep up with the new emerging trends in e-commerce industry, cyber security and online consumer protection. Pakistan has also made policies regarding cyber security and e-commerce but these at are their infancy stages. Pakistan has a great potential to earn from its e-commerce industry through ensuring security to cyberspace, protecting online consumers, safeguarding e-businesses and introducing legal provisions specifically for securing e-commerce stakeholders. Introduction of specific legal provisions, establishment e-courts, recruitment of cyber police and introducing Consumer Helpline Numbers would be revolutionary changes in this regard.

References

Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology*, *14*(1), 157-174.

Agustina, J. R. (2012). Book review of cyber criminology: Exploring internet crimes and criminal behavior. *International Journal of Cyber Criminology*.

Alkaabi, K. A. (2022). Customers' purchasing behavior toward home-based SME products: evidence from UAE community. *Journal of Enterprising Communities: People and Places in the Global Economy*, *16*(3), 472-493.

Amoako, G. K., Dzogbenuku, R. K., & Abubakari, A. (2020). Do green knowledge and attitude influence the youth's green purchasing? Theory of planned behavior. *International Journal of Productivity and Performance Management*, *69*(8), 1609-1626.

Anggusti, M. (2022). Cybercrime Change Consumers' Purchase Intention in Indonesia: A Moderating Role of Corporate Social Responsibility and Business Law. *International Journal of Cyber Criminology*, *16*(1), 20-39.

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber Criminology*, *13*(2).

Aseri, D. A. M. (2021). Security Issues For Online Shoppers. *International Journal of Scientific and Technology Research*, *10*(3), 112-116.

Barbulescu, O. (2015). The utility of the rescission clause in the settlement of disputes arising from international trade contracts. *Bulletin of the Transilvania University of Brasov. Economic Sciences. Series V*, *8*(2), 373.

Boateng, R., Heeks, R., Molla, A., & Hinson, R. (2008). E-commerce and socio-economic development: conceptualizing the link. *Internet Research*, *18*(5), 562-594.

Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

Cockshott, P., & Dieterich, H. (2011). The contemporary relevance of exploitation theory. *마르크스주의 연구*, *8*(1), 206-236.

Department of Commerce, International Trade Administration, USA https://ww.trade.gov/country-commercial-guides/pakistan-ecommerce

Fu, W. (2017, May). Legal Problem Research on the Protection of Consumer Rights in Electronic Commerce. In *2017 4th International Conference on Education, Management and Computing Technology (ICEMCT 2017)* (pp. 290-293). Atlantis Press.

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Kumar, A. (2018). Consumer Protection in Cyber Space. *Int'l JL Mgmt. & Human.*, *1*, 76.

Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber-crime. *International Journal of Cyber Criminology*, *9*(2), 185.

Neacsu, N. A. (2016). Consumer protection in electronic commerce. *Bulletin of the Transilvania University of Brasov. Economic Sciences. Series V*, *9*(1), 301.

Nogoev, A., Yazdanifard, R., Mohseni, S., Samadi, B., & Menon, M. (2011). The Evolution and Development of E-Commerce Market and E-Cash. In *International Conference on Measurement and Control Engineering 2nd (ICMCE 2011)* (Vol. 1, No. 1, pp. 1-5).

OECD. (2016). Consumer protection in E-commerce: OECD recommendations. OECD publishing. https://doi.org/10.1787/9789264255258-en.

Rezk, A., Barakat, S., & Saleh, H. (2017). The impact of cybercrime on E-Commerce. *International Journal of Intelligent Computing and Information Sciences*, *17*(3), 85-96.

Sepec, M. (2012). Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis. *International Journal of Cyber Criminology*, *6*(2), 984.

Setiawan, N., Tarigan, V. E., Sari, P. B., Rossanty, Y., Nasution, M. D. T. P., & Siregar, I. (2018). Impact of cybercrime in e-business and trust. *Int. J. Civ. Eng. Technol*, *9*(7), 652-656.

Shafiyah, N., Alsaqour, R., Shaker, H., Alsaqour, O., & Uddin, M. (2013). Review on electronic commerce. *Middle-East Journal of Scientific Research*, *18*(9), 1357-1365.

Shaik, D., & Poojasree, M. V. (2021, May). Consumer Protection in E-Commerce: A Legal and Compliance Framework in the Digital Market. In *1st International Conference on Law and Human Rights 2020 (ICLHR 2020)* (pp. 18-23). Atlantis Press.

Strupczewski, G. (2021). Defining cyber risk. *Safety science*, *135*, 105143.

Svare, H., Gausdal, A. H., & Möllering, G. (2020). The function of ability, benevolence, and integrity-based trust in innovation networks. *Industry and Innovation*, *27*(6), 585-604.

UNCTAD. (2017). Consumer protection in electronic commerce, https://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf.

Wang, Y., Li, Y., Zhang, J., & Su, X. (2019). How impacting factors affect Chinese green purchasing behavior based on Fuzzy Cognitive Maps. *Journal of Cleaner Production*, *240*, 118199.