International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 7, 2025
https://theaspd.com/index.php

An Empirical Analysis of Challenging factors to digital transformation and Consumer Protection in the Digital Environment and Production Control

Ronlad Yusak Bokaa[1], Herdianto Lantemonaa[1], Frangky Y Turanga[1], Rudolf Bernhard Widiadi Lengkonga[1], Ryalest Maydio Balylo Bokaa[1] and Altje Ester Polib[2]
[1]Department of Industrial Engineering, Minaesa Institute of Technology, South Stadium Street, Walian, Tomohon, 95439, Indonesia
[2]Department of Electrical Engineering, Minaesa Institute of Technology, South Stadium Street, Walian, Tomohon, 95439, Indonesia
lantemonah@gmail.com, turangfrangky@gmail.com, rudolf.lengkong@gmail.com, ryalestboka@gmail.com, altjeesterpoli@gmail.com

*Corresponding Author: ryboka26@gmail.com

ABSTRACT
The purpose of the study is to pinpoint the challenging factors affecting digital transformation and consumer protection in the digital environment. Through empirical research, this study verifies a conceptual framework that demonstrates the relationship between difficult variables, digital transformation, and protecting consumers in the digital domain. An online survey was conducted to test the research model. The survey had 597 valid responses. Descriptive statistics were used for the demographic profile, factor analysis for the validity of the construct statements, Cronbach's alpha for the reliability of the questionnaire, and regression analysis was used to test the hypotheses and validate the proposed model. The setting of the population under consideration supported each of the hypotheses that were developed, as the data demonstrate. The majority of consumers frequently disregard the legally binding terms and conditions of the contracts they sign because they lack the knowledge necessary to comprehend the importance of those clauses.
Keywords: *Digital Transformation, Consumers, Consumer Protection, Digital Environment, Production Control*

1. INTRODUCTION

Our economies and societies are being significantly impacted by the digital revolution, which is also altering how customers engage both with the internet marketplace and each other. Within this framework, customer data emerged as a valuable economic resource, facilitating an extensive array of inventive business models, technologies, and transactions. Customers may be more susceptible to actual or potential hazards and difficulties as a result of the growing intricacy of the internet world, which may limit their capacity to engage in digital transformation successfully. Consumers have benefited greatly from the virtual change in the economy and society, but there are also many new risks associated with it. It also mentioned enduring issues related to consumer guidelines, such as sustainable use and safeguarding the most defenseless consumer groups, international deceptive and fraudulent business practices, hazardous goods, misuse of customer personal data, and international cooperation in law enforcement and consumer protection.

In Indonesia, customers of goods and services are directly affected by the rapid evolution and innovation of business models, especially as technology advances across various sectors. As Salvador et al. (2020) explain, digitalization involves utilizing modern technological tools to improve organizational performance a trend increasingly visible in Indonesian businesses. Many local enterprises have restructured their operations to integrate innovative strategies that enhance both customer engagement and internal efficiency. This makes it essential to examine influencing factors such as customer experience and the suitability of different business models within Indonesia's unique market context. One significant aspect of digital transformation in Indonesia is the growing prominence of digital marketing. With a highly active online population and increasing mobile penetration, Indonesian marketers must develop specialized skills to influence consumer behavior effectively. Investigating the digital competencies required for successful e-commerce implementation across key Indonesian industries is crucial, particularly as businesses adapt to ongoing disruptions and technological shifts (Kovács & Keresztes, 2022).

2. LITERATURE REVIEW

2.1 Digital Transformation

Some organizations have adopted a commercial model of services that do not require the purchase of a product but rather the use of their services as a result of digital transformation. To achieve this, web servers are used to implement technologies and procedures that cater to the needs of their clients. The nebulous definition of an industry, like video games, emphasizes the significance of promptness, openness, and innovation in any business's endeavors to draw in and keep clients and expand its earnings potential (Vaudour and Heinze, 2020). According to Alunni and Llambías (2018), digitality is the adoption of business models and processes that help organizations become more competitive in the dynamic digital marketplace. Customers of the goods or services are directly impacted by the adaptation and invention of new business models in a market that has been altered by the quick advancement of technology in many fields (Kholod et al., 2021). According to Salvador et al., (2020), digitalization is the process of leveraging modern technological tools to enhance an organization's performance. A lot of businesses have changed the foundation of their operations to incorporate fresh ideas that enhance customer relations and operational procedures. Because of this, it's important to consider influencing factors like the customer experience and the business models being used. One aspect of business's digital transformation is the rise of digital marketing to the forefront within organizations. It takes different skills for marketers to change the way that consumers behave. It is important to research how certain competencies become essential in the use of e-commerce in various sectors, taking inspiration from the ongoing upheavals faced by businesses worldwide (Kovács & Keresztes, 2022).

2.2 Transparency and Disclosure

In the digital transformation, transparency and sufficient disclosures are crucial for fostering consumer trust and productive competition. The OECD, 2010 However, it seems that a common problem among the variety of new developments covered above is an absence of clarity and excessively complicated, legalistic, and, in any case, insufficient statements on the gathering, use, and sharing of customer data. According to the OECD (2019), certain information may be extremely sensitive.

A 2019 Customers International (CI) consumer study found that most customers had no idea how artificial intelligence (AI) is perceived by others. Nonetheless, the research also indicated that consumers may not be competent to understand and manage openness on their own. Furthermore, it's unclear if and how consumer trust in digital interactions will be impacted by a heightened awareness of these sophisticated technologies. Similarly, consumers of IoT enabled consumer goods may be ignorant of limitations on product ownership, interoperability, and ancillary support due in part to inadequate disclosures. The OECD, 2018: Digital assistants that support voice activated e-commerce and Internet of Things products lacking a conventional user interface present additional special disclosure challenge (The OECD, 2019).

H1: Transparency and Disclosure (TD) has a noteworthy impact on Digital Transformation (DT)

2.3 Complex Contractual Terms

One more issue concerning Internet shopping is the intricacy of contract clauses, which include provisions that benefit the seller. These terms and conditions are written in extremely technical, complex language that is challenging for the typical person to comprehend. They are also extremely boring, making it impossible for the typical customer to peruse them. The buyer is left with no option but to accept or reject, which puts them in a risky negotiation position. In the digital realm, there is a greater likelihood of minors entering into contracts. This is especially true given that teenagers are increasingly using the internet and preferring to shop for or buy products and services from online sources. An online business portal must take this possibility into account and indicate on its website or form that the person it is transacting with or entering into a contract with is a major.

H2: Complex contractual terms (CCT) have a noteworthy impact on Digital Transformation (DT)

2.4 Discrimination and Choice

More than ever, businesses have the opportunity to conduct consumer analysis thanks to the enormous volumes of customer information being gathered. Businesses may use these accounts to tailor offers in ways that are advantageous to customers, but they may also use them to unjustly treat customers by altering the content that is offered, the choices that are made, or the pricing (i.e., by preying on consumer behavioral biases). (Research Center on Consumer Policy, 2019), While personalization maybe it may benefit certain customers and be economical, it may also lead to unfair business practices. Individualization is seen by many customers as unfair, particularly when it exploits weaker or less fortunate customers (OECD 2018).

H3: Discrimination and choice (DC) have a noteworthy impact on Digital Transformation (DT)

2.5 Privacy and Security

A lot of customer data is needed for AI, IoT devices, and online platforms like PPMs. Although personalization and functionality are clear advantages, there may be privacy and security risks if companies fail to protect customer data properly or use it in ways that are harmful to customers (OECD 2019). Determining privacy is a notoriously difficult task. Four areas of worries about consumer privacy are described in Smith et al.'s (1996) outline: data acquisition, inappropriate access to personal data, unapproved use of personal data, as well as mistakes in personal data. These dimensions of concern have been understood to include the gathering of personal data, having control over how it is used being aware of private policies, and how that data is used in online marketing Malhotra et al., (2004). Errors in personal information and unapproved secondary use are the main concerns of other consumers. When the behavior of the merchant raises those questions, the customer may stop trusting the merchant. The appropriate handling of customer data is referred to by Milne and Gordon (2014) as an "implied social contract" with the customer. Milne et al., (1993) In the event of a confidentiality breach involving the individual and the organization, the victim may be entitled to compensation for the breach of trust. As data mining tools become more sophisticated, consumer database creation and management have developed into a lucrative and expanding business. A program designed to offer meaningful protection to online shoppers must sufficiently safeguard online shoppers who transact internationally and should give special attention to protecting sensitive data. For instance, if someone purchases a good or service online, they must go to a specific website and provide their name, address, contact information, birthdate, etc. However, what is the assurance that this individual won't give their personal information to a third party? It's been said that you don't appreciate your privacy until you've lost it. Amidst the swift advancements in technology and the ongoing development of e-commerce infrastructure, it is imperative to take action now to safeguard our privacy in the future.

H4: Privacy and security (PS) have a noteworthy impact on Digital Transformation (DT)

2.6 Phishing

Phishing, a word derived from the word "fishing," is the practice of an attacker tricking people into visiting a phony website by pretending to send them emails or instant messages, all the while obtaining the victim's data, including passwords, national security IDs, and user names. Thus, this data is utilized for upcoming targeted ads or even identity theft schemes (like transferring funds from the victim's bank account). Phishing, which is the illegal act of obtaining someone's personal information for one's financial gain, is still one of the most feared risks associated with e-commerce transactions in Indonesia, particularly when it comes to online shopping. It's also possible that phishing has reduced the trustworthiness and appeal of e-commerce among regular customers.

H5: Phishing (PHSG) has a noteworthy impact on Digital Transformation (DT)

2.7 Product Safety

Because IoT devices can be controlled remotely, there may be several safety risks associated with using them. Connected products that were deemed safe upon release may turn dangerous later on due to software updates, bugs, or data breaches, among other reasons. This might lead to the device or data being compromised, the connectivity being lost, or a malicious actor being able to remotely control the functionality. Similarly, there may be risks to product safety if AI technology uses autonomous or semi-autonomous decision-making. The OECD, 2018 (2018) US FTC (2016)

H6: Product safety (PRDSFT) has a noteworthy impact on Digital Transformation (DT)

2.8 Accountability

New product ecosystems and business models may make it unclear who will bear the final responsibility and liability if a customer transaction goes awry. When it comes to networked IoT ecosystems and devices, users could find it challenging to determine accountability and liability. Customers might find it challenging to identify the component of the ecosystem (or assistance for services) that contributed to the problem or error (OECD, 2018). The ability to obtain adequate redress, accountability, and liability are the main issues that consumers have with AI CI (2019). As stated in the OECD's 2019 AI Recommendation, AI actors are accountable for ensuring that AI systems function correctly and for abiding by its guiding principles. Additionally, in the case of PPMs, sellers may be able to escape accountability in areas where safeguarding consumer laws do not pertain to exchanges involving customers (OECD, 2016)

H7: Accountability (ACN) has a noteworthy impact on Digital Transformation (DT)

2.9 Interoperability

To make sure that various systems and devices can cooperate, interoperability is essential. A certain amount of compatibility is required to prevent "shut-in," promote consumer selection and rivalry, and protect privacy and security, even though certain interoperability restrictions may encourage innovation. The OECD, (2018) says that Consumer data interoperability, in addition to hardware and software interoperability, is probably crucial for promoting consumer choice and competition (CI, 2016)

H8: Interoperability (INTROP) has a noteworthy impact on Digital transformation (DT).

2.10 Consumer Protection in the Digital Economy

Consumer rights in electronic transactions are not legally protected at this point in the digital economy. The lack of consideration for the specifics of this format in both the current and pending drafts of Russian Federal Law "On Electronic Commerce" is likely to be a deterrent to the development of electronic commerce, according to our analysis of regulatory issues about the sale of goods and services in Russia using information technologies. Draft & Federal, (2006) created it to guarantee the protection of stakeholders' rights and lessen uncertainty when selling goods and services through the use of information technology (Ilovaysky et al., 2019)

A lot of violations result from the absence of a clear regulatory framework. It's a common misconception among sellers that the Consumer Protection Act solely covers transactions conducted online. The Supreme Court of the Russian Federation's Plenum adopted Resolution No. 17, "On Consideration by the Courts of Civil Cases on Disputes Concerning Protection of Consumer Rights." Moscow & Russia (2012) additionally skip over concerns about consumer protection in the digital sphere. The authors think that by amending the Act to state that its provisions also apply to relationships that arise in the digital realm, this situation can be rectified. However, if the unfair seller resides in the Russian Federation, the Law, specifically Article 26.1 ("Distance Selling of Goods"), still allows for the restoration of the consumer's violated rights. But as things stand, there is currently insufficient regulation of transactions with foreign sellers. International agreements like the General Agreement on Trade in Services (GATS), which was signed in 1994 (WTO) the UNCITRAL Model Law on Electronic Commerce, which was created and approved by the UN Commission on Trade and Development (1996), do not include provisions governing the prosecution of violators. For this reason, both domestic and international online hypermarkets (like AliExpress) provide buyer protection programs that they have created. Digital trade relationships are increasingly predicated on participant self-regulation. Some believe that as the digital economy grows, independent consumer protection will soon follow. (Vasilyeva, 2019).

H9: Transparency and Disclosure (TD) has a noteworthy impact on consumer protection in a digital environment (CPDE).

H10: Complex contractual terms (CCT) have a noteworthy impact on consumer protection in the digital environment (CPDE).

H11: Discrimination and choice (DC) have a noteworthy impact on consumer protection in the digital environment (CPDE).

H12: Privacy and security (PS) has a noteworthy impact on consumer protection in a digital environment (CPDE).

H13: Phishing (PHSG) has a noteworthy impact on consumer protection in the digital environment (CPDE).

H14: Product safety (PRDSFT) has a noteworthy impact on consumer protection in the digital environment (CPDE).

H15: Accountability (ACN) has a noteworthy impact on consumer protection in the digital environment (CPDE)

H16: Interoperability (INTEROP) has a noteworthy impact on consumer protection in the digital environment (CPDE)

H17: Digital transformation (DT) has a noteworthy impact on the Protection of consumers in the digital sphere (CPDE)

3. RESEARCH OBJECTIVE

- To identify the factors challenging the digital transformation and consumer protection in the digital environment
- To evaluate the effects of challenging components on digital transformation and consumer protection in the digital environment

- To put forth a theoretical structure showing the relationship between challenging factors digital transformation, and customer protection in the digital sphere and validate it through empirical analysis

4. CONCEPTUAL FRAMEWORK

The proposed model includes and represents the relationship between influencing and dependent factors: Transparency and Disclosure (TD); Complex contractual terms (CCT); Discrimination and choice (DC); Privacy and security (PS); Phishing (PHSG); Product safety (PRDSFT); Accountability (ACN); Interoperability (INTROP), along with the impact on Digital transformation (DT) and Consumer Protection in the Digital Environment (CPDE) (Figure 1).

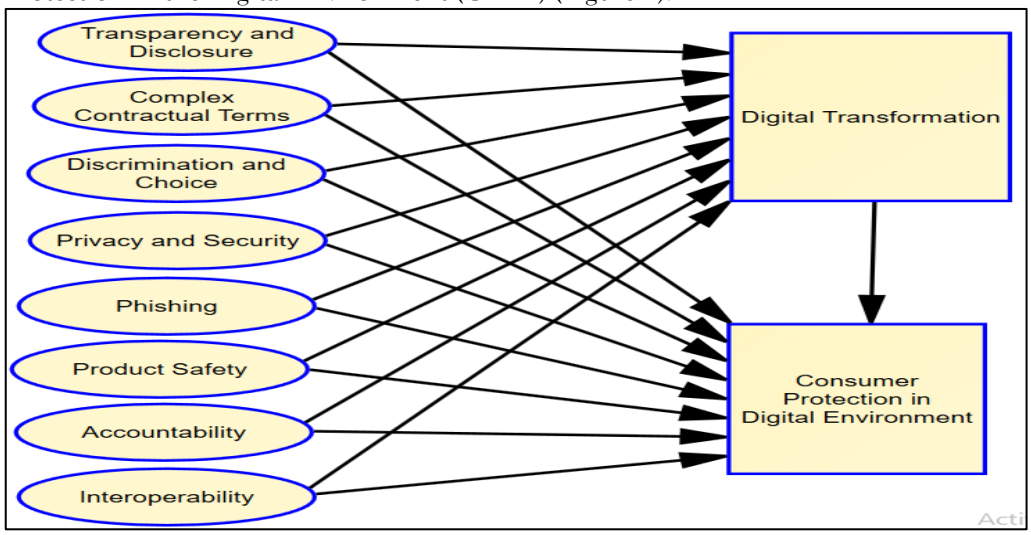

Figure1: Model showing the relationship between influencing & dependent factors

A novel concept is the combination of digital transformation and consumer protection in the digital world. Based on the parameters taken into consideration, we measured digital transformation and consumer protection for this study. Although it makes sense to presume that all the variables are related, this study additionally examines the relationship between consumer protection and the digital transition.

5. RESEARCH METHODOLOGY

The opinions of people from different age groups were used in a pilot project to evaluate the gathering of data. We conducted an online survey to test the research model. Seven hundred seasoned users completed the survey. Experienced users were those who had made at least one online purchase. The survey had 597 valid responses. IBM SPSS Statistics v.20 was used for analyses. Descriptive statistics were used for the demographic profile, factor analysis for the validity of the construct statements, Cronbach's alpha for the reliability of the questionnaire, and regression analysis was used to test the hypotheses and validate the proposed model.

6. RESEARCH ANALYSIS AND RESULTS

6.1. Demographic Profile

The respondents' demographic characteristics were evaluated using descriptive demographic statistics expressed as percentage proportion and frequency of occurrence. The study sample comprised respondents who have used an online platform one or more times. A systematic questionnaire was employed to gather information from April 2021 to May 2022. Respondents received 700 questionnaires through a random and selective sampling approach. Out of them, 597 were found to be error-free and perfectly finished. A thorough analysis determines that a response rate of 85.28% is of good quality. Table 1 provides socio-demographic details about the individuals. Of the 597 respondents, there were significantly more men (505, 84.6%) than women (92, 15.4%); the majority of the men (162, 27.1%) were situated in the 30- to 39-year-old range, and 259 (43.4%) had professional education and were making over 30,000 rupees (220, 36.9%).

Table 1. Descriptive Statistics of Demographic Profile

		Frequency	Valid %
Gender profile	Male	505	84.6
	Female	92	15.4

Age profile	20-29 years	82	13.7
	30-39 years	162	27.1
	40-49 years	115	19.3
	50-59 years	146	24.5
	60 years and above	92	15.4
Highest education level	Bachelor Degree	71	11.9
	Master's Degree	158	26.5
	Professional Education	259	43.4
	Other	109	18.3
Income	10,000- 20,000	133	22.3
	20,001- 30,000	206	34.5
	30,001- 40,000	220	36.9
	More than 40,000	38	6.4

6.2. Exploratory Factor Analysis

Using the PCA method, an exploratory factor analysis (EFA) was conducted for conforming entities. The concept validity was established by applying the EFA approach. Factor loadings >0.40 and >0.30 were deemed large enough to meet the minimal level, respectively. A carefully selected parameter was employed to verify the factor loadings. In contrast, results of factor loading less than 0.30 were disregarded, while those of 0.50 or more are considered very significant. A factor loading of at least 0.50 is the threshold for the current investigation. KMO factor analysis's significance for the data is indicated by values in the range of 0.5 and 1.0. Bartlett's sphericity test indicates that there is a correlation between the variables' items. The test's result is indicated by the significance level. A strong correlation likely exists between the elements if the figures are smaller than 0.05. Factor analysis cannot be performed on the data if the value is greater than 0.10 or similar. Considering the outcomes of the examination of factors, Table 2 is appropriate for the provided information.

Table 2. Results of Exploratory Factor Analysis

Statement	Factor loadings	KMO Measure of Sample Adequacy (>0.5)	Bartlett's Test of Sphericity		Items confirmed	Items dropped	Cum % of loading
			Chi Square	Sig. (<.10)			
Transparency and Disclosure (TD) -1	0.906	0.743	1.135E3	0.000	4	1	55.721
Transparency and Disclosure (TD) -2	0.757						
Transparency and Disclosure (TD) -3	0.692						
Transparency and Disclosure (TD) -4	0.435						
Transparency and Disclosure (TD) -5	0.851						
Complex contractual terms (CCT) -1	0.777	0.746	527.797	0.000	5	0	45.505 65.623
Complex contractual terms (CCT) -2	0.806						
Complex contractual terms (CCT) -3	0.985						
Complex contractual terms (CCT) -4	0.737						
Complex contractual terms (CCT) -5	0.682						
Discrimination and choice (DC) -1	0.189	0.860	2.715E3	0.000	4	1	71.524
Discrimination and choice (DC) -2	0.931						

Discrimination and choice (DC) -3	0.947						
Discrimination and choice (DC) -4	0.955						
Discrimination and choice (DC) -5	0.931						
Privacy and security (PS) –1	0.858	0.749	683.282	0.000	4	0	59.604
Privacy and security (PS) -2	0.812						
Privacy and security (PS) -3	0.579						
Privacy and security (PS) -4	0.808						
Phishing (PHSG) -1	0.952	0.719	7.293E3	0.000	5	0	90.672
Phishing (PHSG) -2	0.949						
Phishing (PHSG) -3	0.953						
Phishing (PHSG) -4	0.959						
Phishing (PHSG) -5	0.949						
Product safety (PRDSFT) -1	0.892	0.840	2.086E3	0.000	5	0	72.516
Product safety (PRDSFT) -2	0.911						
Product safety (PRDSFT) -3	0.890						
Product safety (PRDSFT) -4	0.821						
Product safety (PRDSFT) -5	0.731						
Accountability (ACN) -1	0.627	0.681	1.454E3	0.000	4	0	68.518
Accountability (ACN) -2	0.870						
Accountability (ACN) -3	0.940						
Accountability (ACN) -4	0.841						
Interoperability (INTROP) -1	0.816	0.703	412.086	0.000	4	0	51.760
Interoperability (INTROP) -2	0.777						
Interoperability (INTROP) -3	0.518						
Interoperability (INTROP) -4	0.730						
Digital transformation (DT) -1	0.791	0.556	200.446	0.000	4	0	40.577 68.212
Digital transformation (DT) -2	0.665						
Digital transformation (DT) -3	0.639						
Digital transformation (DT) -4	0.759						
Consumer protection in digital environment (CPDE) -1	0.853	0.889	1.668E3	0.000	5	0	70.615
Consumer protection in digital environment (CPDE) -2	0.874						
Consumer protection in digital environment (CPDE) -3	0.790						
Consumer protection in digital environment (CPDE) -4	0.861						
Consumer protection in digital environment (CPDE) -5	0.820						

6.3. Reliability Analysis

By utilizing Cronbach's alpha coefficient to compute each factor's internal consistency, the validity of the study scale and questionnaire can be confirmed. The purpose of this study is to ascertain if the ideas being assessed by observable factors are the same. This method can be applied to eliminate inaccurate variables from the study model. The acceptable alpha value, or Cronbach's alpha coefficient scale, is as follows:

a. A cut-off score of 0.60 or above is deemed appropriate for assessment.

b. Both internal consistency and usability fall within the range of 0.7 to 0.8.

c. Decent: 0.8–nearly 1

The corrected item-total correlation coefficient of the scale must be 0.3 or above, according to Hair et al., (2010). Since the value of 0.7 was found to be higher than the allowed range and to be inside the cutoff value of 0.70, the study employed this as its Cronbach's alpha cutoff. As Hoang and Chu, (2008) have shown, this proves that every definitional scale meets the dependability level. The questionnaire was a dependable research tool, as shown by Table 3's overall Cronbach's alpha coefficient of 0.979.

Table 3: Results of the Reliability test

Variable	Cronbach alpha
Transparency and Disclosure (TD)	0.787
Complex contractual terms (CCT)	0.646
Discrimination and Choice (DC)	0.865
Privacy and security (PS)	0.758
Phishing (PHSG)	0.974
Product safety (PRDSFT)	0.905
Accountability (ACN)	0.846
Interoperability (INTEROP)	0.674
Digital transformation (DT)	0.498
Consumer protection in digital environment (CPDE)	0.895
Overall Reliability of the Questionnaire	0.979

6.4. Correlation Analysis

The mean value is appropriately scaled, and the controlled variables are coded for correlation analysis after EFA and reliability analysis. The relationship between quantitative data is investigated using Pearson's coefficient of correlation (r), which looks at the linear connection between components. Numerous statistics can be employed to investigate the link between the variables because every correlation that shows statistical significance exists between the variables that are independent and dependent. The levels of the correlation coefficients offer more proof that the multi-collinearity problem does not exist. If there is a notable connection between the dependent and separate variables, then the variables can be included in a linear regression analysis. By examining the absolute value of R's magnitude, we can ascertain the degree of rigidity in a linear connection. The stronger the two variables' relationship, the closer r is to 1, and vice versa. Table 4 shows that, out of all the parameters considered, there was a significant correlation found between the variables. The variables about product safety (PRDSFT) and phishing (PHSG) exhibited the strongest link (0.950), while the variables about digital transformation (DT) and interoperability (INTROP) demonstrated the least significant correlation (0.600).

Table 4: Correlations

	TD	CCT	DC	PS	PHSG	PRDSFT	ACN	INTROP	CPDE	DT
TD	1									
CCT	.719**	1								
DC	.884**	.847**	1							
PS	.826**	.807**	.881**	1						
PHSG	.852**	.765**	.894**	.845**	1					
PRDSFT	.844**	.796**	.903**	.855**	.950**	1				
ACN	.863**	.756**	.890**	.869**	.892**	.895**	1			
INTROP	.793**	.787**	.851**	.965**	.810**	.826**	.836**	1		
CPDE	.814**	.791**	.873**	.870**	.917**	.941**	.877**	.838**	1	
DT	.837**	.558**	.685**	.633**	.669**	.652**	.677**	.600**	.629**	1

**. Correlation is significant at the 0.01 level (2-tailed).

6.5. Regression Analysis

To test hypotheses, show the statistical validity of the prototype assumption, and determine the impact of independent factors on dependent variables, the investigator carries out a coefficient analysis followed

by a significant multivariate regression analysis employing the enter method level of 5%. For each variable, mean and standard deviation value analyses were used to calculate the results and questionnaire items. Cronbach's alpha was employed to assess the research, and the instrument's reliability, and component analysis was used to examine its validity. Using stepwise regression analysis, the predictor-criterion link between the variables that are independent and dependent was discovered. This study, in contrast to previous ones, uses linear regression rather than nonlinear regression. The regression technique employed in this study was Ordinary Least Squares (OLS) regression. To evaluate if the model is adequate, scalable, and capable of rejecting the null hypothesis that the total regression coefficient is equal to zero, researchers employ the F-test, adjusted coefficient R2, and t-test.

Regression summary for dependent variables: Step-wise regression analysis is used in Table 5 to demonstrate which independent variables: Transparency and disclosure (TD), Complex contractual terms (CCT), Discrimination and choice (DC), Privacy and Security (PS), Phishing (PHSG), Product Safety (PRDSFT), Accountability (ACN), Interoperability (INTROP), and the impact on Digital transformation (DT) and Consumer protection in digital environment (CPDE) are significant predictors of the dependent variable. Moreover, it is believed that the variable Digital Transformation (DT) influences the variable Consumer Protection in Digital Environment (CPDE) independently. Based on the maximum R square values of 0.396 found in Table 5, the variable Digital transformation (DT) may account for approximately 39.6% of the influence on consumer protection in the digital environment (CPDE). Regression model validation at a 95% confidence level is shown by Table 6's ANOVA results. The factor's beta values are 0.629, which are largely typical of the effect on consumer safety in the digital environment (CPDE), according to the coefficient summary in Table 7.

Table 5: Regression for dependent variables

Model	Predictors	Dependent variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	TD, CCT, DC, PS, PHSG, PRDSFT, CAN, INTROP	DT	0.848	0.719	0.715	0.35872
2	TD, CCT, DC, PS, PHSG, PRDSFT, CAN, INTROP	CPDE	0.952	0.906	0.905	0.25483
3	DT	CPDE	0.629	0.396	0.395	0.64166

Table 6: Regression ANOVA table for dependent variables

Model	Predictors	Dependent variable		Sum of Squares	df	Mean Square	F	Sig.
1	TD, CCT, DC, PS, PHSG, PRDSFT, CAN, INTROP	DT	Regression	193.777	8	24.222	188.233	0.000
2	TD, CCT, DC, PS, PHSG, PRDSFT, CAN, INTROP	CPDE	Regression	367.198	8	45.900	706.831	0.000
3	DT	CPDE	Regression	160.401	1	160.401	389.579	0.000

Table 7: Regression coefficients table for dependent variables

Model		Dependent variable	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
1	Constant TD	DT	0.753	0.020	0.837	37.329	0.000
2	Constant CCT	DT	0.586	0.036	0.558	16.392	0.000
3	Constant DC	DT	0.558	0.024	0.685	22.906	0.000
4	Constant PS	DT	0.535	0.027	0.633	19.958	0.000
5	Constant PHSG	DT	0.460	0.021	0.669	21.926	0.000
6	Constant PRDSFT	DT	0.504	0.024	0.652	20.978	0.000
7	Constant ACN	DT	0.541	0.024	0.677	22.440	0.000
8	Constant INTROP	DT	0.544	0.030	0.600	18.296	0.000
9	Constant TD	CPDE	0.899	0.026	0.814	34.243	0.000
10	Constant CCT	CPDE	1.019	0.032	0.791	31.576	0.000
11	Constant DC	CPDE	0.873	0.020	0.873	43.765	0.000
12	Constant PS	CPDE	0.901	0.021	0.870	43.055	0.000
13	Constant PHSG	CPDE	0.774	0.014	0.917	56.224	0.000
14	Constant PRDSFT	CPDE	0.892	0.013	0.941	67.681	0.000
15	Constant ACN	CPDE	0.860	0.019	0.877	44.607	0.000
16	Constant INTROP	CPDE	0.932	0.025	0.838	34.472	0.000
17	Constant DT	CPDE	0.772	0.039	0.629	19.738	0.000

6.6. Results of Hypotheses Testing

Seventeen initial hypotheses were put out for the conceptual research framework, and as can be seen in Table 8, all of them were ultimately accepted.

Table 8: Summary of Hypotheses Testing

Hy. No.	Independent Variables	Dependent Variables	R-Square	Beta Coefficient	t-value	Sig Value	Status of Hypotheses
H1	Transparency and Disclosure (TD)	Digital transformation (DT)	0.719	0.837	37.329	0.000	Accepted
H2	Complex contractual terms (CCT)	Digital transformation (DT)	0.719	0.558	16.392	0.000	Accepted
H3	Discrimination and choice (DC)	Digital transformation (DT)	0.719	0.685	22.906	0.000	Accepted
H4	Privacy and security (PS)	Digital transformation (DT)	0.719	0.633	19.958	0.000	Accepted
H5	Phishing (PHSG)	Digital transformation (DT)	0.719	0.669	21.926	0.000	Accepted
H6	Product safety (PRDSFT)	Digital transformation (DT)	0.719	0.652	20.978	0.000	Accepted
H7	Accountability (ACN)	Digital transformation (DT)	0.719	0.677	22.440	0.000	Accepted
H8	Interoperability (INTROP)	Digital transformation (DT)	0.719	0.600	18.296	0.000	Accepted
H9	Transparency and Disclosure (TD)	Consumer protection in digital environment	0.906	0.814	34.243	0.000	Accepted

		(CPDE)					
H10	Complex contractual terms (CCT)	Consumer protection in digital environment (CPDE)	0.906	0.791	31.576	0.000	Accepted
H11	Discrimination and choice (DC)	Consumer protection in digital environment (CPDE)	0.906	0.873	43.765	0.000	Accepted
H12	Privacy and security (PS)	Consumer protection in digital environment (CPDE)	0.906	0.870	43.055	0.000	Accepted
H13	Phishing (PHSG)	Consumer protection in digital environment (CPDE)	0.906	0.917	56.224	0.000	Accepted
H14	Product safety (PRDSFT)	Consumer protection in digital environment (CPDE)	0.906	0.941	67.681	0.000	Accepted
H15	Accountability (ACN)	Consumer protection in digital environment (CPDE)	0.906	0.877	44.607	0.000	Accepted
H16	Interoperability (INTROP)	Consumer protection in digital environment (CPDE)	0.906	0.838	34.472	0.000	Accepted
H17	Digital transformation (DT)	Consumer protection in digital environment (CPDE)	0.396	0.629	19.738	0.000	Accepted

7. DISCUSSION

The present study is designed to create a research model that encompasses the online market's competitiveness, the digital economy's dynamics, the digital transformation, and above all consumer protection. Disclosure and transparency, discrimination and autonomy, intricate contractual language, security and privacy, product safety, phishing accountability, and, interoperability was the main relationship mediators that were represented in the model. The setting of the population under consideration supported each of the hypotheses that were developed, as the data demonstrate. The results of research on the relationship between transparency and disclosure, digital transformation, and consumer protection (H1 and H9; R-square = 0.719 and 0.906; beta coefficient = 0.837 and 0.814; t-value = 37.329 and 34.243) verified the presence of a significant positive relationship. Transparency and disclosures are crucial for fostering consumer confidence and healthy competition in the digital transition, which in turn protects consumers in the digital environment (OECD, 2010). Across the continuum of new developments, a lack of transparency and unduly complicated or insufficient disclosures about how customer data is acquired, utilized, and pooled seem to be a consistent problem. (ACCC, 2018; OECD, 2018a; CI and the Internet Society, 2019). Consumers appear to have little idea "who is in charge of things," per a Consumers International (CI, 2019) customer survey regarding customer views. However, the research also revealed that consumers may not be able to entirely grasp and regulate transparency on their own. It should be realized that for consumers to easily contact firms and for law enforcement and regulatory bodies to identify and find them, information must be timely and unambiguous. The business identity, legal name, trading name, primary physical address, phone number, website, email address, and other contact information, as well as government registration and license

numbers, may be included in the material.

One additional issue with internet shopping is the intricacy of contract clauses, which often include provisions that benefit the vendor. An average person would find it impossible to understand the extremely technical and complicated terminology utilized to compose these terms and conditions. An online business portal must therefore take this possibility into account and make it clear on its website or in its form that the person with whom it is transacting business or entering into a contract is a significant concern. Based on the empirical study of hypotheses 2 and 10, it was discovered that there is a constructive association between complex contractual terms, digital transformation, and consumer protection (R-square = 0.719 and 0.906; beta coefficient = 0.558 and 0.791; t-value = 16.392 and 31.576). Additionally, customers ought to have prompt access to information that is clear and concise about the products and services that companies provide, as well as the specific terms and circumstances of the transaction at hand. It is best to promote contracts with equitable terms that are simple, straightforward, and easy to understand (ECO, 2018; UNCTAD, 2020a).

An important positive connection between the two models was found by independently examining the relationship between discrimination and choice, digital transformation, and consumer protection. This finding supports Hypotheses 3 and 11 (R-square = 0.719 and 0.906; beta coefficient = 0.685 and 0.873; t-value = 22.906 and 43.765). The Consumer Policy Research Center (2019) states that corporations have more chances than ever before to participate in consumer analysis due to the acquisition of enormous volumes of customer information. Enterprises may leverage these profiles to tailor their services in ways that are advantageous to customers, but they may also use them to discriminate against customers based on offers, pricing, or how information is presented, taking advantage of behavioral biases. Personalization could result in unfair commercial practices, even though it might be more cost-effective and advantageous for certain consumers. Personalization is seen by many customers as unfair, particularly when it exploits weaker or less fortunate customers (US FTC, 2016). Additionally, it has been shown that online retailers discriminate based on the products they offer. For example, a customer may want to order a certain thing, but when he attempts to order it, he receives the message "that seller doesn't deliver this item to your location," even though he may order the same good from a large metropolis. This is a form of discrimination whereby consumers in cities and small towns are treated differently. Due to the internet retailers' strategy of restricting their product availability to particular locales, even rural villages are unable to utilize their services.

The empirical study of hypotheses 4 and 12 revealed a significant positive correlation between privacy and security, digital transformation, and consumer protection (R-square = 0.719 and 0.906; beta coefficient = 0.633 and 0.870; t-value = 19.958 and 43.055). Furthermore, in some markets, certain attributes like low competition, insufficient information, and/or market complexity may increase customer vulnerability (Nardo et al., 2011; Gutierrez and Thornton, 2014). In highly complex sectors like the financial services industry, even the most astute consumer may experience anxiety (Gutierrez & Thornton, 2014). Consumers in these markets often make no judgments at all, pass up opportunities, or adhere to heuristic thinking or basic norms (EC, 2015). Additionally, some product attributes can place clients at the greatest risk. These could be complex products that, for example, make use of the Internet and artificial intelligence (Andrei and Iacob, 2011). Even though personalization and functionality are clear advantages, there may be security and privacy issues if companies fail to appropriately store client data or make use of it in ways that negatively impact customers (OECD, 2018a).

Phishing is the practice of tricking people into visiting a fraudulent website by pretending to send them emails or instant messages. In the process, the attacker secretly obtains the victim's personal information, including passwords, national security IDs, and user names. This information is then used for identity theft attacks, such as transferring money from the victim's bank account, or for future target advertisements. Most notably, the results (hypotheses 5 and 13) demonstrate that phishing significantly affects consumer protection and digital transformation in the online market (R square = 0.719 and 0.906; beta coefficient = 0.669 and 0.917; T value = 21.926 and 56.224). Jakobsson & Myers, 2006 considered Phishing as a societal attack where a hacker uses a public or trustworthy association illegally in an automated blueprint to trick users into sending sensitive information to them. The attacker gains access to the victim's insightful information when the user believes the message to be authentic. Phishing is one of the biggest concerns because it affects a lot of internet users. Similar to this, Gupta et al. (2015) described phishing attacks, in which con artists utilize social engineering strategies to lead victims who click on an email link to malicious websites.

According to the US FTC (2018), as internet gadgets can be controlled remotely, there may be several

safety issues associated with using them. After a software patch, bug, or data breach, for instance, connected products that were deemed safe at the time of their release onto the market may become dangerous. This is because the compromised data or device may experience connectivity issues, be compromised remotely by malevolent actors, or have their functionality compromised. The empirical study of hypotheses 6 and 14 revealed a strong positive correlation between digital transformation, consumer protection, and product safety (R-square = 0.719 and 0.906; beta coefficient = 0.652 and 0.941; t-value = 20.978 and 67.681).

The online product safety guidelines published by Consumers International (CI, 2021) offer suggestions for online markets and governments looking to create a safer online environment. The Republic of Korea, Australia (ACCC, 2021), and the European Commission (EC, 2021) have all been urged to sign product safety promises. Through this undertaking, they promise to remove harmful products from their listings, stop them from being relisted, work with law enforcement, and report on the results. To promote basic protection between nations and support internet markets and the vendors on them, who operate across many countries, the OECD published policy recommendations on such commitments.

In the case of networked internet gadgets and ecosystems, customers may find it challenging to determine responsibility and accountability. Consumers could find it challenging to pinpoint the specific component of service support that led to the problem, according to the OECD (2018). According to the independent study, a positive correlation has been observed between the two constructs of accountability, digital transformation, and consumer protection (R-square = 0.719 and 0.906; beta coefficient = 0.677 and 0.877; t-value = 22.440 and 44.607). This finding supports hypothesis 7 and 15.

Consumers' top concerns include accountability and liability as well as having access to efficient remedies (CI, 2019; OECD, 2019a). In countries where safeguarding consumer laws do not pertain to exchanges between customers, the OECD suggests that sellers may be able to escape accountability and obligation (OECD, 2016). In computer security, accountability is an essential security feature that results in the non-repudiation of engaging parties that are pertinent to the transactions. Before utilizing the data, Hou and Yeh (2015) suggested certification approaches to guarantee verification among the user, the substantiation server, and a reliable third-party power. Alkeem and others. (2017) and Al Ameen et al., (2012) suggested systems that transmit and receive data via a cloud system utilizing a cryptographic protocol. With fourteen messages delivered through the network, Lo et al., (2017) established a robust asymmetric encryption technique that satisfies all security requirements and is very secure. A central approach was also proposed by Mashima & Ahamad (2012a, 2012b) to monitor record usage.

To make sure that various systems and devices can cooperate, interoperability is essential. A certain level of compatibility is required to prevent lock-in, promote consumer choice and competition, and protect privacy and security, even though some constraints on interoperability may encourage innovation (OECD, 2018a). Consumer data interoperability is probably crucial for promoting consumer choice and competition, in addition to hardware and software interoperability (CI, 2016). The empirical study of hypotheses 8 and 16 revealed a substantial positive correlation between interoperability, digital transformation, and consumer protection (R-square = 0.719 and 0.906; beta coefficient = 0.600 and 0.838; t-value = 18.296 and 34.472). Interoperability measures can encourage competition both within and between digital channels by enabling consumers to combine several complementary services from various suppliers and by preserving network effects on new services, depending on how they are designed. Particular studies have suggested that because of the speed of innovation, multi-sidedness, or advertising driven business models in particular online markets, firm led interoperability projects may be more constrained than in more traditional markets (Riley, 2020).

The confirmation of the previously reported empirical findings by the present study is one contribution to the body of literature. To our knowledge, there hasn't been much discussion of the connection between consumer protection and digital transformation in the cutthroat internet marketplace. More practically speaking, the results to date (Hypotheses 17; R-square = 0.396; Beta coefficient = 0.629; t-value = 19.738) indicate the new business models that ISPs should successfully leverage to maintain their performance. Businesses in the market should focus more on reacting to the topical market with a specific focus on moral, viable, and long-lasting products, responsible consumption, and rational decision-making as new online consumers arise.

In platform markets, consumers mostly utilize ratings and evaluations from other users to help them make decisions (OECD, 2017). According to an OECD consumer survey, customers in peer-platform marketplaces typically have greater faith in the platform itself than in the third party suppliers that operate there (OECD, 2016). However, an estimate by Fakespot (2021) states that in 2020, about 31% of reviews

on platforms were thought to be fraudulent. The French Consumer Code states that platforms bear responsibility for the veracity of reviews. France investigated in 2022 and discovered significant problems with transparency, such as the removal or delay of critical evaluations and the acceptance of phony reviews. A voluntary standard in Indonesia mandates that review administrators be set up on platforms to regulate reviews, remove biases, and prohibit false reviews (Indonesia, 2019 and 2023). While user ratings are an important tool for fostering trust on online platforms, there are situations in which they may not accurately represent certain aspects of a good or service such as safety requirements because users are unable to observe them or lack the necessary expertise to evaluate them. In these situations, regulation and oversight are necessary (UNCTAD, 2021).

8. CONCLUSION

Consumer interests must be protected in the electronic age. Two key components of an effective online consumer protection strategy are easy access to relevant redressable laws and the ability of the individual consumer to look out for their security. For online consumers, having the right information about the products is decisive since it can lend a hand to them in accepting the advantages and disadvantages of a specific transaction. If the client already knows this information, they won't be unnecessarily disappointed, which will prevent further problems. Additionally, as most customers lack the awareness essential to understand the significance of the provisions of the contracts, they agree to they are often ignored when it comes to the legally binding terms and conditions. When it comes to giving information to customers concerning their return and cancellation policies, such as the duration of time after entering into a legally binding agreement, merchants engage in dishonest behavior. Before the acquisition is done, it should be made clear that there is no right to a refund, cancellation, or return.

ACKNOWLEDGEMENTS

The authors acknowledge Minaesa Institute of Technology, Tomohon, for providing the necessary institutional support, research facilities, and academic environment that made this study possible.

Funding Details

This research received no external funding.

Authors' contributions

All authors contributed toward data analysis, drafting and revising the paper and agreed to be responsible for all the aspects of this work.

Declaration of Conflicts of Interests

Authors declare that they have no conflict of interest.

Use of Artificial Intelligence

Not applicable

Declarations

Authors declare that all works are original and this manuscript has not been published in any other journal.

REFERENCES

1.ACCC (2018), Digital Platforms Inquiry: Preliminary report, http://www.accc.gov.au (accessed on 17 July 2019). Retrieved From; https://policycommons.net/artifacts/1781769/digital-platforms-inquiry/2513415/

2.ACCC (2021). Australian Competition and Consumer Commission, 2021, Australian product safety pledge. Retrieved From https://www.accc.gov.au/system/files/Annual%20Report%202020%2021%20-%20Web.pdf

3.Alunni, Laura, and Nicolás Llambías. (2018). Explorando La Transformación Digital Desde Adentro. Palermo Business Review 17: 11–30. Available online: Retrieved From http://hdl.handle.net/10226/2059 (accessed on 10 August 2021).

4.Andrei, A.G.; Iacob, A. 2011. From user's motivations to branding: The case of social networks. In Proceedings of the 4th International Conference on Globalization and Higher Education in Economics and Business Administration-GEBA 2010, Iasi, Romania, 21–23 October 2010; Airinei, D., Pintilescu, C., Asandului, M., Andries, A.M., Eds.; Alexandru Ioan Cuza University of Iasi Publishing House: Iasi, Romania, 2011; pp. 139–144.

5.ASEAN, (2016- 2025) https://aseanconsumer.org/product-alert.

6.CI and the Internet Society (2019), The trust opportunity: Exploring Consumers' Attitudes to the Internet of Things, Retrieved From https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf (accessed on 13 May 2019).

7.CI (2019), Artificial Intelligence: Consumer Experiences in New Technology, Retrieved From https://www.consumersinternational.org/media/261949/ai- consumerexperiencesinnewtech.pdf (accessed on 13 May 2019).

8.CI (2016), The Internet of Things and challenges for consumer protection, Retrieved From

http://www.consumersinternational.org/media/1292/connection-and-protection-the internet-of-things-and-challenges-for-consumer-protection.pdf (accessed on 11 October 2017).
9.CI, (2021). Consumers International, 2021, Guidelines for online product safety. Retrieved From https://www.consumersinternational.org/media/451293/policy-action-framework.pdf
10. CI (2016). The Internet of Things and challenges for consumer protection, Retrieved From http://www.consumersinternational.org/media/1292/connection-and-protection-the-internetof-things-and-challenges-for-consumer-protection.pdf
11. Consumer Policy Research Centre (2019), A Day in the Life of Data, Retrieved From http://cprc.org.au/wp- content/ uploads/CPRC-Research-Report_A-Day-in-the-Life-of-Data_final-full-report.pdf.
12. Competition and Markets Authority UK (UK CMA). (2019). Consumer vulnerability: challenges and potential solutions. (2019), URL: Retrieved From https://www.gov.uk/government/publications/consumer-vulnerability-challengesandpotential-solutions/consumer-vulnerability-challenges-and-potentialsolutions (date of access: 16.03.21).
13. Consumer Affairs Victoria (CAV).(2004). What do we mean by vulnerable and disadvantaged consumers? (2004), URL: Retrieved From https://www.consumer.vic.gov.au/library/public ations/ resources- andeducation/research/what-do-we-mean-by-vulnerable-and-disadvantaged- consumersdiscussion-paper-2004.pdf (date of access: 16.03.21).
14. Council of the European Communities (EEC) (April 5, 1993) No. 93/13/EEC) (1993), URL Retrieved From: https://base.garant.ru/2565749/ (date of access: 16.03.21).
15. Competition Bureau Canada.(2018). The Little Black Book of Scams 2nd edition. (2018), URL: Retrieved From https://www.competitionbureau.gc.ca/eic/site/cb- bc.nsf/eng/04333.html (date of access: 16.03.21).
16. Colombia (2020). Colombia, Superintendency of Industry and Trade, 2020, Guide to Good Practice in Advertising through Influencers.
17. C Riefa,(2021). Consumer law enforcement as a tool to bolster competition in digital markets: A case study on personalised pricing in UNCTAD, Competition and Consumer Policies for Inclusive Development in the Digital Era (UNCTAD 2021) 15, Retrieved From https://unctad.org/system/files/official-document/ditccplp2021d2_en_0.pdf
18. Crane, C. (2019). The dirty dozen: the 12 most costly phishing attack examples. Available at: Retrieved From https://www.thesslstore.com/blog/the-dirty-dozen-the-12-mostcostly-phishing-attack examples/#:~:text At some level%2C everyone is susceptible to phishing, outright trick you into performing a particular task
19. D. Mashima and M. Ahamad, (2012a). "Enabling robust information accountability in e-healthcare systems," in Proceedings of the 3rd USENIX Workshop on Health Security and Privacy, Bellevue, WA, USA, August 2012a. Retrieved From https://www.semanticscholar.org/paper/Enabling-Robust-Information-Accountability-in-Mashima-Ahamad/de120f4b6045d9f88152674859ca02702e93251f
20. D. Mashima and M. Ahamad, (2012b). "Enhancing the accountability of electronic health record usage via patient-centric monitoring," in Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, ACM, Miami, FL, USA, pp. 409–418, January 2012b DOI:https://doi.org/10.1145/2110363.2110410
21. Draft Federal law No. 310163-4 "On electronic Commerce" (2006), URL: Retrieved From www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=42158#028127057741049954 (date of access: 16.03.21).
22. E. Al Alkeem, D. Shehada, C. Y. Yeun, M. J. Zemerly, and J. Hu, 2017. "New secure healthcare system using cloud of things," Cluster Computing, vol. 20, no. 3, pp. 2211–2229, 2017 DOI: https://link.springer.com/article/10.1007%2Fs10586-017-0872-x
23. ECO, 2018. The European Consumer Organisation, 2018, Ensuring consumer protection in the platform economy, Position paper. Retrieved From https://www.beuc.eu/position-papers/ensuring-consumer-protection-platform-economy
24. EC (2021). European Commission, 2021, Product safety pledge. Retrieved From https://ec.europa.eu/about_en.htm
25. El Ceo, (2022). Consumers go against travel agency and influencers, file complaint with Federal Consumer Protection Agency for 1.8 Mex$, available at Retrieved From https://elceo.com/negocios/consumidores-van-vs-agencia-de-viajes-e-influencers-meten-queja-ante-profeco-por-1-8-mdp/.
26. European Commission (EC). 2015. Report on Competition Policy 2015. Available online: ec.europa.eu/competition/publications/annualreport/2015/part1_en.pdf
27. EU, (2023) https://ec.europa.eu/safety-gate-alerts/screen/webReport.
28. European Commission (EC) (2016), URL: Retrieved From https://ec.europa.eu/info/sites/info/files/consum er-vulnerabilityfactsheet_en.pdf (date of access: 16.03.21).
29. Fakespot (2021). https://www.fakespot.com/2021holidayreport.
30. Federal service for supervision of consumer protection and human welfare (2019a). (Rospotrebnadzor). Consumer protection in the Russian Federation in 2018: State report. Moscow, Russia (2019a)
31. Federal service for supervision of consumer rights protection and human welfare (Rospotrebnadzor) (2020a), URL: Retrieved From http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=199634#0719158699309 6075 (date of access: 16.03.21).
32. Federal service for supervision of consumer protection and human welfare (Rospotrebnadzor). (2020b). Consumer protection in the Russian Federation in 2019: State report. Moscow, Russia (2020b)
33. Federal Ministry for Economic Affairs and Energy of Germany (2017), G20 Digital Economy Ministerial Conference, Retrieved From http://www.g20.utoronto.ca/2017/g20-digital-economy-ministerial-declaration-english-version.pdf (accessed on 16 May 2019).
34. Federal Trade Commission US (US FTC).(2018). Protecting older consumers 2017-18: A report of the Federal Trade Commission. (2018), URL: Retrieved From https://www.ftc.gov/system/files/documents/repo rts/protecting-olderconsumers-2017-2018-report- congress-federal- tradecommission/protecting_older_consumers_-_ftc_report_10-18-18.pdf (date of access: 16.03.21).
35. Federal service for supervision of consumer rights protection and human welfare (Rospotrebnadzor).(2019b). Recommendations to citizens: how to avoid becoming a victim of fraud? (2019b), URL: Retrieved From https://www.rospotrebnadzor.ru/about/info/news /newsdetails.php?ELEMENTID=10961&sphrase_id=1821993 (date of

access: 16.03.21).
36. G20 (2018), G20 Leaders' declaration: Building consensus for fair and sustainable development, Retrieved From https://www.consilium.europa.eu/media/37247/buenos_aires_leaders_declaration.pdf (accessed on 16 May 2019).
37. Government of the Russian Federation. (2017). The decree of the Government of the Russian Federation "On approval of Strategy of state policy of the Russian Federation in the field of consumer protection for the period till 2030" (August 28, 2017 No. 1837-r). Moscow, Russia (2017).
38. Global Recalls Portal, OECD, (2012) https://globalrecalls.oecd.org/.
39. Gutierrez, A.; Thornton, T.F. 2014. Can consumers understand sustainability through seafood eco-labels? A US and UK case study. Sustainability 2014, 6, 8195–8217. DOI: https://doi.org/10.3390/su6118195
40. Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. (2015). "Phoneypot: data-driven understanding of telephony threats," in Proceedings 2015 network and distributed system security symposium, (Reston, VA: Internet Society), 8–11. DOI: https://dx.doi.org/10.14722/ndss.2015.23176
41. Herley, C., and Florˆencio, D. (2008). "A profitless endeavor," in New security paradigms workshop (NSPW '08), New Hampshire, United States, October 25–28, 2021, 1–12. DOI: https://dx.doi.org/10.1145/1595676.1595686
42. I.B Ilovaysky, Y.Y Kayl, D.A. Tokarev & V.A.(2019). Usanova Institutional Model for the Protection of Rights of the Parties Concerned in the Sale of Goods and Services with the Use of Information Technologies. (Switzerland, Cham: Springer Science + Business Media, 2019). Retrieved From https://link.springer.com/chapter/10.1007/978-3-030-13397-9_90
43. ICPEN, (2016).International Consumer Protection and Enforcement Network, 2016, Online reviews and endorsements: IPCEN guidelines for digital influencers. Retrieved From https://homeofdirectcommerce.com/news/international-consumer-protection-enforcers-issue-guidelines-on-online-reviews-and-endorsements/
44. Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia [Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. State Gazette of the Republic of Indonesia], 2019(185).
45. Indonesia. (2023). Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Lembaran Negara Republik Indonesia [Presidential Regulation Number 47 of 2023 concerning the National Cybersecurity Strategy and Cyber Crisis Management. State Gazette of the Republic of Indonesia], 2023(88).
46. Iuga, C., Nurse, J. R. C., and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. Hum. Cent. Comput. Inf. Sci. 6, 8. doi: https://dx.doi.org/10.1186/s13673-016-0065-2
47. Jakobsson,M., and Myers, S. (2006). Phishing and countermeasures: understanding the increasing problems of electronic identity theft. New Jersey: John Wiley and Sons. DOI: http://dx.doi.org/10.1002/9780470086100
48. J.-L. Hou and K.-H. Yeh, 2015. "Novel authentication schemes for IoT based healthcare systems," International Journal of Distributed Sensor Networks, vol. 11, no. 11, Article ID 183659, 2015. DOI: https://doi.org/10.1155/2015/183659
49. Kholod, Sergii, Valentyna Pavlova, Anhelina Spitsyna, Yuliia Maistrenko, Oksana Anufrieva, and Vadym Lukianykhin. (2021). Transfor-mation of the Personnel Management System in the Conditions of Digitalization of HR Processes. Studies of Applied Economics 39. (CrossRef) DOI: http://dx.doi.org/10.25115/eea.v39i6.5015
50. Kovács, I., and Keresztes, É. R. (2022). Young Employees' Perceptions about Employability Skills for E-Commerce. Economies, 10(12), 309, https://doi.org/10.3390/economies10120309
51. Lina Kahn, Amazon's Antitrust Paradox (2017) 126 Yale Law Journal, 710-805, https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf ; See also Nancy Scola, 'Lina Kahn is not worried about going too far' Retrieved From https://nymag.com/intelligencer/article/lina-khan-ftc-profile.html
52. M. Al Ameen, J. Liu, and K. Kwak, 2012. "Security and privacy issues in wireless sensor networks for healthcare applications," Journal of Medical Systems, vol. 36, no. 1, pp. 93–101, 2012. DOI: http://dx.doi.org/10.1007/s10916-010-9449-4
53. Milne, J., Suddaby. G., & Higgins, A. (2014). Blended learning: How teachers balance the blend
54. of online and classroom components. Journal of Information Technology Education: Research, 13, 121-140. Retrieved
55. from: http://www.jite.org/documents/Vol13/JITEv13ResearchP121-140Jeffrey0460.pdf
56. Morgan, S. (2019). 2019 official annual cybercrime report. USA, UK, Canada. Available at: Retrieved From https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual Cybercrime-Report.pdf .
57. Nardo M, Loi M, Rosati R, Manca A. 2011. The Consumer Empowerment Index. EUR 24791 EN. Luxembourg (Luxembourg): Publications Office of the European Union; 2011. JRC64349. Retrieved From https://www.semanticscholar.org/paper/The-consumer-empowerment-index.-A-measure-of-and-of-Nardo-Loi/351cd8a65375fa006fd18acc342741aab2a65a14
58. New digital profession from the state (n.d.). (2021). URL: Retrieved From https://цифровойсертификат.рф/?utm_source=fbwp&utm_medium=cpc&utm_campaign=teacher&utm_term=stat&fbclid=IwAR065dBxOY_lP fwEm9Cd7s0jPN4Um_i0imcdb1O1-Ey9BNUBszibGMp44BY (date of access: 16.03.21).
59. N.-W. Lo, C.-Y. Wu, and Y.-H. Chuang, 2017. "An authentication and authorization mechanism for long-term electronic health records management," Procedia Computer Science, vol. 111, pp. 145–153, 2017. DOI: https://doi.org/10.1016/j.procs.2017.06.021
60. OECD (2016), OECD Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris, DOI: https://dx.doi.org/10.1787/9789264255258-en.
61. OECD (2018), Toolkit for Protecting Digital Consumers, OECD, Paris, Retrieved From https://www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf (accessed on 7 May 2019).
62. OECD (2010), Consumer Policy Toolkit, OECD Publishing, Paris, DOI: https://dx.doi.org/10.1787/9789264079663-en.
63. OECD (2017), Trust in peer platform markets: Consumer survey findings, OECD Digital Economy Papers, No. 263, OECD Publishing, Paris, DOI: https://dx.doi.org/10.1787/1a893b58-en.
64. OECD (2019), An introduction to online platforms and their role in the digital transformation, OECD Publishing, DOI: https://doi.org/10.1787/53e5f593-en.
65. OECD (2018a). "Consumer policy and the smart home", OECD Digital Economy Papers, No. 268, OECD Publishing, Paris, DOI: https://dx.doi.org/10.1787/e124c34a-en.

66. OECD (2019a). Artificial Intelligence in Society, OECD Publishing, http://www.oecd.org/internet/artificial-intelligence-in-society-eedfee77-en.htm.
67. Ollmann, G. (2004). The phishing guide understanding & preventing phishing attacks abstract. USA. Available at: Retrieved From http://www.ngsconsulting.com.
68. Organization for Economic Cooperation and Development (OECD). (2014a), URL: http://www.oecd.org/sti/consumer/Toolkit- recommendation-booklet.pdf (date of access: 16.03.21).
69. Organization for Economic Cooperation and Development (OECD). (2010), URL: DOI: https://dx.doi.org/10.1787/9789264079663-en (date of access: 16.03.21).
70. Organization for Economic Cooperation and Development (OECD). (2012). Report on Consumer Protection in Online and Mobile Payments. Paris, France: OECD Publishing. (2012), URL: DOI: https://doi.org/10.1787/20716826 (date of access: 16.03.21).
71. Organization for Economic Cooperation and Development (OECD).(2014b). Consumer Policy Guidance on Mobile and Online Payments. OECD (2014b), URL: DOI: https://dx.doi.org/10.1787/5jz432cl1ns7-en (date of access: 16.03.21).
72. Organization for Economic Cooperation and Development (OECD) (2019a), URL: Retrieved From https://one.oecd.org/document/DSTI/CP(2019)10/FINAL/en/pdf/ (date of access: 16.03.21).
73. Organization for Economic Cooperation and Development (OECD). (2019b). Good practice guide on online advertising. (2019b),URL: DOI: https://doi.org/10.1787/20716826 (date of access: 16.03.21).
74. Organization for Economic Cooperation and Development (OECD). (2016), URL: DOI: https://dx.doi.org/10.1787/9789264255258-en
75. Ovelgönne, M., Dumitras , , T., Prakash, B. A., Subrahmanian, V. S., and Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks. ACM Trans. Intell. Syst. Technol. 8, 1–25. doi: https://dx.doi.org/10.1080/00207284.1985.11491413
76. Peru (2019). Peru, National Consumer Protection Authority, 2019, Guide to Advertising for Influencers.
77. Plenum of the Supreme Court of the Russian Federation.(2012). The resolution of Plenum of the Supreme Court of the Russian Federation "About consideration by courts of civil cases on disputes on protection of consumer rights" (June 28, 2012 No. 17). Moscow, Russia (2012) Retrieved From https://cis-legislation.com/document.fwx?rgn=27878
78. Plenum of the Supreme Arbitration Court of the Russian Federation. (2016). Resolution of the Plenum of the Supreme Arbitration Court of the Russian Federation "Freedom of contract and its limits" (March 14, 2014 No. 16, Moscow, Russia) Retrieved From https://cis-legislation.com/document.fwx?rgn=17016
79. P Siciliani, C. Riefa, H Gamper,(2019). Consumer Theories of Harm: An economic approach to consumer law enforcement and policy making (Hart Publishing 2019). DOI: http://dx.doi.org/10.5040/9781509916887
80. Riley, C. (2020). "Unpacking interoperability in competition", Journal of Cyber Policy, Vol. 5:1, DOI: https://doi.org/10.1080/23738871.2020.1740754
81. Russian Federation.(1992). Law of the Russian Federation "On consumer protection" (February 7, 1992 No. 2300-1). Moscow, Russia (1992). Retrieved From https://base.garant.ru/510106035/
82. Russian Federation. (1994). Civil code of the Russian Federation (part one) (November 30, 1994 No. 51-FZ, Moscow, Russia) Retrieved From https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=39457
83. Russian Federation.(2017). Federal law of "On amendments to certain legislative acts of the Russian Federation" (July 18, 2019 No. 191-FZ, Moscow, Russia). Retrieved From: http://en.kremlin.ru/events/president/news/54656
84. Salvador, Yudith, Mariluz Llanes, and Miguel Suarez. (2020). Digital Transformation in Public Administration: Axes and Essential Factors. Avances 22: 590–602. Available online: Retrieved From https://dialnet.unirioja.es/servlet/articulo?codigo=7925389 (accessed on 13 August 2021).
85. Salvador, E., Simon, J. P., & Benghozi, P. J. (2019). Facing Disruption: The Cinema Value Chain in the Digital Age. International Journal of Arts Management, 22(1), 25–40. https://www.researchgate.net/publication/327417997_Facing_disruption_the_cinema_value_chain_in_the_digital_age

86. See for eg, C Riefa, (2020). The protection of vulnerable consumers in the digital age, (UNCTAD RPP 2020), Retrieved From https://unctad.org/system/files/non-official document/ccpb_RPP_2020_05_Present_Christina_Riefa.pdf who conceptualises the digital sphere as a systemic vulnerability; Also see Natali Helberger, Orla Lynskey, Hans-W Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz, EU Consumer Protection 2.0., Structural Asymetries in Digital Consumer Markets (BEUC, March 2021) 5 who explain: 'in digital markets, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion. In digital marketplaces, most if not all consumers are potentially vulnerable'.
87. See for eg,(2018). https://www.beuc.eu/press-media/news-events/euroconsumers-launch-collective-action- against-facebook. However, note that this is not the case everywhere. Notably see in the UK, Llyods v Google where the Supreme Court rejected the possibility of group litigation for the enforcement of section 13 of the Data Protection Act 2018 Retrieved From (https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf).
88. Smith, H. J., Milberg, S., and Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2): 167-196. DOI: https://doi.org/10.2307/249477
89. The Children's Online Privacy Protection Act of October 21, (1998) (COPPA). URL: Retrieved From https://www.govinfo.gov/content/pkg/PLAW- 105publ277/pdf/PLAW-105publ277.pdf (date of access: 16.03.21).
90. US FTC (2016), Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, Retrieved From https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion- understanding-issues/160106big-data-rpt.pdf (accessed on 27 September 2018).
91. US FTC (2018), Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, Retrieved From https://www.ftc.gov/reports/mobile-security-updates-understanding- (accessed on 18 July 2019).
92. United Nations Conference on Trade and Development (UNCTAD). (2018), URL: Retrieved From https://unctad.org/meetings/en/Presentation/WG%20Vulnerable%20and%20Disadvantaged%20Consumers%20.pdf (date

of access: 16.03.21).
93. United Nations Commission on international trade law (UNCITRAL). (1996), URL: Retrieved From https://base.garant.ru/2555780/ (date of access: 16.03.21).
94. United Nations Conference on Trade and Development (UNCTAD). (2018). Working Group on Vulnerable and Disadvantaged Consumers Contribution, Intergovernmental Group of Experts on Consumer Law and Policy. (2018), URL: Retrieved From https://unctad.org/meetings/en/Presentation/WG%20Vulnerable%20and%20Disadvantaged%20Consumers%20.pdf (date of access: 16.03.21).
95. UNCTAD, (2020a). The COVID-19 crisis: Accentuating the need to bridge digital divides.
96. UNCTAD, (2020b). TD/RBP/CONF.9/9.
97. UNCTAD, 2021. Competition and Consumer Protection Policies for Inclusive Development in the Digital Era (United Nations publication, Geneva). Retrieved From https://dig.watch/updates/competition-and-consumer-protection-policies-inclusive-development-digital-era-unctad
98. United States of America (2019). United States of America, Federal Trade Commission, 2019, Disclosures 101 for social media influencers.
99. US FTC (2018). Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, Retrieved From https://www.ftc.gov/reports/mobile-security-updates-understanding
100. V. Naumov, (2000). Recommendations for organizing the activities of individuals in the field of Internet Commerce in the Russian Federation (2000), URL: Retrieved From https://www.osp.ru/ecom/2000/07/13031267 (date of access: 16.03.21).
101. Vaudour, Fanny, and Aleksej Heinze. (2020). Software as a service: Lessons from the video game industry. Global Business and Organizational Excellence 39: 31–40. (CrossRef) DOI: http://dx.doi.org/10.1002/joe.21982
102. Y.A. Vasilyeva,(2019). Risks for consumers of logistics services in the conditions of digitalization of society (Saint Petersburg, Russia: Kult-inform- press publishing house, 2019). Retrieved From https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/08/e3sconf_afe2023_04047.pdf
103. World consumer rights day (2017). calls for protecting consumer rights in the digital age (2017), URL: Retrieved From https://zppdon.ru/news/9234/ (date of access: 16.03.21).
104. World trade organization (WTO) (1994), URL: Retrieved From http://ivo.garant.ru/#/document/2541542/paragraph/650:0 (date of access: 16.03.21).
105. Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J. Am. Soc. Inf. Sci. 59 (4), 662–674. doi: https://doi.org/1010.1002/asi.20779