THE ROLE OF PERCEIVED RISK AND SECURITY LEVEL IN BUILDING TRUST IN E-GOVERNMENT SOLUTIONS

Joanna Ejdys, Romualdas Ginevicius, Zoltan Rozsa, Katarina Janoskova

Introduction

One of the factors determining the current and future social and economic advance is the level of society's digitisation, which is applicable to each sphere of human life (Ejdys & Halicka, 2018; Polak-Sopinska & Wisniewski, 2009). This level is measured by the scale and scope of the phenomenon, i.e. subjective, geographical dynamics of change and the scale of effects caused (Chodakowska & Nazarko, 2017). Digitalisation processes gave rise to a new type of society referred to as the information society. E-government is one of the areas of ICT application in the information society. The term e-government, i.e. electronic public administration, refers to a system (organisational and legal, institutional, and IT) which enables to deal with administrative matters by electronic means. According to the definition proposed by the European Commission, e-government is the use of ICT tools and systems to provide better public services to citizens and businesses (Digital Single Market: Glossary).

The level of digitalisation of public sector services (the development of e-government services) in Poland is lagging behind highly developed countries. In the ranking of the level of digital public services, Poland holds the 14th place with the indicator of 10.5%, which is 0.4 percentage points below the average of the EU-28 (10.9%) (Digital Single Market. Digital Economy & Society). According to Eurostat, the digital interaction between Poles and public institutions is very weak. The percentage share of citizens digitally interacting with public institutions amounts to 30%, which is low compared to the Scandinavian countries, namely, Denmark with 88%, Norway with 85%, and Finland with 82% (Digital Economy and Society Database, 2016). According to the scope of the use of electronic public administration services, Poland's indicators are much lower than the EU average. For example, the average EU indicator for the downloading of forms by citizens is 41.0%, submission of completed forms – 42.0%, and obtaining information from websites – 55.0%. Scandinavian countries are undoubtedly leaders in the use of e-government services. For example, the number of citizens who send forms electronically amounts to 68.0% in Estonia, 62.0% in Norway, and 60.0% in Finland. According to the UN report, the E-Government Development Index (EGDI) classifies Poland as 36th out of surveyed 191 countries, having the EGDI index of 0.7211. The leader in the ranking is the United Kingdom with the EGDI index of 0.9193 (see United Nations E-Government Survey 2016). In the light of the unsatisfactory implementation of e-government solutions, the search for reasons explaining the current state of affairs is justified.

Successful implementation of e-government solutions depends on technological, organisational, human, economic, social and cultural factors (Kumar et al., 2007; Shareef et al., 2011). Social factors include trust in e-government. Trust plays an important role in economic and technological exchanges (Reiersen, 2017) and determines how technologies are assessed by different stakeholders (Nazarko, 2017). Trust in e-government should be understood as trust in technological solutions mainly in the field of ICT offered by public administrative bodies. The issue of building trust in projects related to e-government has been recognised by many researchers as one of the key success factors. The lack of trust is perceived as a fundamental barrier to the implementation of e-government solutions, mainly from the perspective of users (Warkentin et al., 2002; Carter & Weerakkody, 2008; Shareef et al., 2011; Mellouli et al., 2016). Even though e-government solutions are often characterised by a high level of transparency

 DOI: 10.15240/tul/001/2019-3-014

and determine a level of innovativeness of services provided by the administration, many people are still suspicious of ICT solutions (Colesca, 2009). Trust in e-government services becomes particularly important due to the lack of direct (face-to-face) contact between interacting parties (Wisniewski & Polak-Sopinska, 2009). This context makes it relatively easy to lose trust in e-government and rather difficult to regain it following accidents (Kim et al., 2008; Benlian & Hess, 2011; Hole, 2016). The public's trust in e-government is characterised by the impersonal nature of Internet relationships, the extensive use of technology and the uncertainty and risks associated with open access to ICT infrastructure (AlAwadhi & Morris, 2008).

Knowledge of the reasons why users trust or distrust the services offered by e-government is a key to building stable trust (Hole, 2016). In many countries, citizens still do not trust the services provided by e-government, which harms further technology adoption. According to Alzahrani et al. (2017), there is still a need for research to fill the existing gap in the area of the factors determining trust in e-government. The literature review showed that among many factors determining trust in e-government, the most important reflect the level of security and risk perceived by users. Authors addressing the issue of e-government adoption indicate that trust, security and transparency are the main factors of acceptance of such solutions (Colesca, 2009).

The identified research gap is related to the lack of knowledge regarding the relatively low level of implementation and adoption of e-government solutions in Poland. The scientific aim of the paper is to determine the extent, to which the user-perceived risk and security of e-government services determine the level of trust in technology and influence future intentions of e-government adoption.

The remainder of the article consists of the following sections: Section 2 reviews the literature on the issues relating to trust in e-government solutions. Also, it presents an overview of constructs determining trust in e-government, indicating that risk and perceived security are an important element in most theoretical models of trust and technology adoption. Results of the literature review served as a basis for the formulation of hypotheses and the theoretical model presented in Section 3. Section 4 describes the methodology. Results are described in Section 5. Finally, Section 6 summarises the findings and, the conclusions briefly explain the limitations of the research and implications for future research efforts.

1. Determinants of Trust in E-Government Technology – A Literature Review

The current and future development of technology depends on two fundamental factors: the level of technological knowledge and the adoption of technology by society (Nazarko et al., 2017; Radziszewski et al., 2016). The authors of the book *Technolife 2035: How Will Technology Change our Future* capture the process of new technology adoption through the prism of the Diffusion of Innovations theory (DOI) (Hiltunen & Hiltunen, 2015). Many theoretical models have been developed to explain the processes involved in the acceptance of the technology. The most popular models are the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the D&M IT Success model. The model developed by Davis used the principles of Theory of Reasoned Action (TRA) developed by Ajzen and Fishbein, which explained human behaviour (Ajzen & Fishbein, 1980). Finally, Davis and Venkatesh assumed that two basic factors influence the attitudes towards the use of the system: ease of use and usefulness of the system/technology (Venkatesh & Davis, 1996). The technology acceptance model, originally known as the TAM, has been modified as TAM2 and TAM3 (Venkatesh & Davis, 2000; Venkatesh & Bala, 2008). Trust is one of the important factors determining the level of technology acceptance, often reflected in theoretical models. Trust is seen as one of the success factors ensuring an effective adoption of technologies (Lippert & Davis, 2006). Trust has particular importance under conditions of uncertainty, the unpredictability of development and increasing human dependence on technology. Trust is also an important way of reducing risk and uncertainties related to the adoption of technology (Kim et al., 2008; Pavlou, 2003; Hernández-Ortega, 2011).

The literature review and definitions by other authors gave rise to the following definition of technology trust: trust is the result of expected or experienced characteristics of the technology and environmental factors, an inclination of

the technology user to rely on the technology in a situation of potential risks associated with its use, determining the intentions for the future use of the technology. As a measuring construct, trust is an object of interest from the perspective of antecedents of technology trust, measurement scales of technology trust, and the process of influence of trust on other constructs in technology acceptance models. Research on the factors determining technology trust focuses on attempts to classify them into technological, social, economic and institutional factors. Most of the studies on the inclusion of trust variables in technology acceptance models refer to the study of trust, as a determinant of perceived usefulness on the one hand and, on the other hand, as a factor dependent on perceived ease of use. At the same time, trust is analysed as a determinant of behavioural intention and attitude towards using technology (Gefen et al., 2003; Lean et al., 2009). From a broader perspective, the object of interest of researchers are the factors determining the trust in technology, but also the influence of trust on the results related to the use of technology.

Research on trust as a determinant focuses mainly on two areas: (i) study of the factors that shape initial trust in technology to overcome the risks and uncertainties associated with the adoption of new technologies (Wang & Benbasat, 2005) and (ii) study of trust as a determinant of the continued use of technology from the perspective of technology users (Li et al., 2008).

Trust research is often contextual and technology-specific. Researchers focusing on the topic of trust examine various technologies, such as e-commerce (Shiau & Dwivedi, 2013), m-commerce, electronic banking and electronic payment systems (Hernández-Ortega, 2011), national identification systems (Li et al., 2008), health information systems (Lemire et al., 2008), information systems in logistics (Tung, 2008; Salam, 2017), information systems (Lai, 2011), e-government (Myeong et al., 2014), e-ticketing (Lee et al., 2010), online communication (Lankton & McKnight, 2011) electronic invoicing systems (Hernández-Ortega, 2011), software for electronic tax returns (Chen, 2015), electronic health systems (Söderström, 2016), biosensors (Mazey, 2017), and driverless cars (Kaur & Rampersad, 2018). E-government solutions are also among the technologies investigated by research on trust (Alzahrani et al., 2017), in which researches try to explain the determinants of technology adoption. The perspective of trust emphasises the importance of fostering and developing citizen trust for successful e-government acceptance and adoption (Colesca, 2009).

The authors of the United Nations E-Government Survey 2016 on "E-Government in Support of Sustainable Development" indicated that the development of e-government services required the creation of an environment of trust, also relating to public institutions and the government, and not only to technological solutions (United Nations E-Government Survey, 2016). Trust in technology seems to be particularly important in an uncertain environment, which includes the Internet and all technologies using the Internet, where there are no formal rules and customs or agreements (Veselý & Dohnal, 2006; McKnight et al., 2002).

The results of the Belanche, Casaló and Flavián (2012) studies confirm that trust has a direct impact on user attitudes and consequently on the intentions for the future use of e-government services. Carter and Bélanger (2008) analysed the impact of trust in the Internet and institutions, which determine the willingness to use e-government services in the future. Liu and Zhou (2010) claimed that for the successful adoption of e-government, establishment of citizen trust is an absolute necessity. Similar research was carried out by Kurfala et al. (2017) who considered variables such as trust in the Internet and trust in administration in their research on the process of adoption of e-government. A literature review carried out by Alzahrani et al. (2017) identified four groups of factors determining trust in e-government technologies: technical, institutional, risk factors and those reflecting the individual characteristics of users. Shareef and others developed their own E-Government Adoption Model (GAM), indicating that the existing models, based Diffusion of Innovations and the Theory of Planned Behaviour do not consider the specificity of e-government. In the adoption model used by the authors, one of the analysed constructs was trust. Three factors that determine trust in e-government, namely, uncertainty, security and privacy, showed a positive relationship between trust and adoption of e-government solutions (Shareef et al., 2011). Some studies have included

trust as an element of adoption models, such as the Technology Acceptance Model and the Diffusion of Innovations theory (Gefen, 2002; Pavlou, 2003; Warkentin et al., 2002), but few of them have focused on the implications of trust on e-government adoption.

Trust as an abstract concept reflects the complex range of relationships between the factors that determine trust. Ranaweera et al. (2016), analysing the factors shaping trust in e-government, pointed out the following five groups of factors: trust in public institutions and the Internet, ensuring security, ensuring privacy, risks and uncertainties, and quality of information. The output variable was the current and future use of e-government services by users (Ranaweera et al., 2016). The e-government adoption model developed by Horst et al. (2007) considered several variables, including risk, user concerns (anxiety), controllability, subjective standards, and the user trust and experience with electronic services in general. Voutinioti (2013) included three categories of trust in the e-government acceptance model, namely trust in the Internet, trust in institutions, and trust in the e-government services provided to the public, analysing their relationship with intentions to use e-government (Horst et al., 2007). Alzahrani et al. (2017) carried out a systematic and critical review of four groups of factors that determine trust in e-government, such as citizen aspects, technology, government agencies and risk factors. Alzahrani et al. (2017) claimed that risk is a significant factor that impacts the trust of citizens in e-government. Technological risks, such as security and privacy, as well as performance risk, are considered important factors that have an impact on trust in e-government.

The issue of trust in e-government is also recognised by institutions carrying out research within the framework of the European Union's public statistics (EUROSTAT). One of the areas of research on the use of e-government is the recognition of the reasons for the failure to submit complete (completed) electronic forms. Among the reasons for the phenomenon surveyed, respondents mentioned fears related to ensuring protection and security of their personal data, problems with electronic signature, lack of knowledge and authentication of documents, outsourcing of these activities by others (accountants, family members, advisors), lack of knowledge and skills, inability to receive an immediate answer, greater trust in the personal submission of the document and needs of personal meetings with officers (Digital Public Services, 2016).

Literature studies confirmed the existing research interest in factors that determine trust in e-government. The adoption of an e-government solution will depend on the attitudes of users, which can be shaped in advance. Among many factors determining trust in e-government, the level of security and the risk perceived by users related to the use of technology are indicated as important factors which determine trust in technology and future intention of technology use as well.

Identified theoretical and practical problems pose the following research questions: How perceived risk and security determine the trust of the Polish society toward e-government and future adoption of e-government? In this context, the authors concentrated on the relationships among trust in technology, the level of security, and the risk perceived to build a theoretical research model.

2. Research Model and Hypotheses

The risk associated with the use of e-government results from the fact that the nature of the relationship between man and technology is impersonal and virtual. When engaging in any online transaction process, consumers are rightly alarmed about the different types of risks that confront them. Because risk is difficult to measure objectively, researchers more often focus on user risk perceptions. Perceived risk is defined as the citizen's subjective expectation of suffering a loss in pursuit of the desired outcome (Warkentin et al., 2002). The vast majority of researchers agree that perceived risk is a significant antecedent of trust (Ranaweera, 2016; Rutkauskas & Stasytytė, 2011). On the other hand, trust reduces the perceived risk (Lewis & Weigert, 1985). Often, trust is described as a function of the degree of risk involved in the situation (Koller, 1988). Risks can be perceived by technology users in terms of avoided loss/threats (i.e. benefits) or perceived risks associated with the use of the technology. From this perspective, we can speak of net risk, reflecting the difference between avoided losses (benefits) and exposure to threats.

Risk will always create the need for trust, and trust will determine the willingness to take

risks. Society would not have to accept risk if there were other functional alternatives (Lewis & Weigert, 1985). Trust and perceived risk are essential constructs when uncertainty is present (Luhmann, 1979; Mayer et al., 1995). The risk reflects the user's feelings about the possibility of losses incurred and the expected benefits associated with the use of technology (Ranaweera, 2016). According to Carter and Bélanger (2008), perceived risk is a citizen's subjective expectation of suffering a loss in pursuit of a favoured outcome. Research conducted by Carter and Bélanger, in which authors assume that higher trust of the Internet (trust in technology) reduces perceived risk, did not support such a hypothesis. At the same time, other authors confirmed that higher trust in the government reduces the risk perceived in relation to the use of an e-government service (Carter & Bélanger, 2008; Khasawneh & Abu-Shanab, 2013). Considering the above, the following hypothesis was formulated:

Hypothesis (H1): Perceived risk (PR) will negatively influence trust in e-government solutions.

In some studies, there has been a link between trust and perceived security of e-government solutions. According to Liu and Zhou (2010), an Internet-based e-government solution should ensure citizen authentication and data confidentiality, reflecting the security level. Also, Ranaweera agreed that security issues should be considered strengthening the trustworthiness of e-government services among people (Ranaweera, 2016). Perceived security is an important element in building trust in e-government solutions (Verkijika & Wet, 2018; Ranaweera, 2016; Ayyash et al., 2013; Liu & Zhou, 2010). Chen highlights security as a big issue, which needs to be addressed (Chen, 2008). Also, Hernandez-Ortega claims that security is a critical element for trust. Considering the importance of perceived security in e-invoicing, Hernandez-Ortega analysed its effect on user trust and found that security has a high impact on trust (Hernandez-Ortega, 2011). Considering the above, the authors formulated the following hypothesis:

Hypothesis (H2): Perceived security (PS) will positively influence trust in e-government solutions.

Normally, the risk involved in an online environment is high, and this is a barrier to adoption of e-services (Ranaweera, 2016). According to Pavlou, perceptions of trust and risk are likely to be important factors in predicting the intention to use B2C e-commerce (Pavlou, 2003). Many other authors maintained that perceived risk was an important variable that affected an end-user's intention to use digital technologies (Jasimuddin et al., 2017). It seems that perceived risk should negatively influence the intention to use an e-government service, but research conducted by Carter and Bélanger (2008) rejected such a hypothesis by proving that higher levels of perceived risk did not impede the intention to use. In a research conducted by Pavlou (2003), the constructs of trust and perceived risk were considered fundamental in predicting B2C e-commerce acceptance. Also, among nine groups of factors determining the use of the e-government services, Thunibat et al. (2011) distinguished perceived risk. Based on the literature above, the authors proposed the following hypothesis:

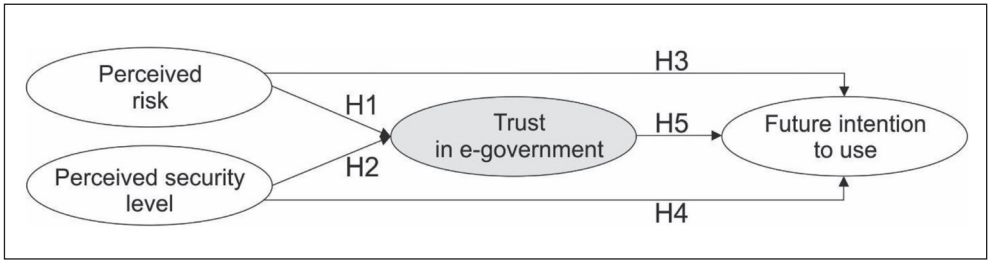
Hypothesis (H3): Perceived risk (PR) will negatively influence the future intention to use e-government.

Many authors agree that the user perception of security determines their future intentions to use the technology or discard it (Joshi & Islam, 2018; Al-Thunibat, Zin, & Sahari, 2011). A lesser feeling of security contributes to a lower level of adoption or abandonment of e-solutions (Ranaweera, 2016). Considering the above, the authors formulated the following hypothesis:

Hypothesis (H4): Perceived security (PS) will positively influence the future intention to use e-government.

According to the Theory of Reasoned Action (Ajzen & Fishbein, 1980), in case of technology adoption, the higher the degree of trust in the technology, the higher the degree of the user's intentions to continue employing it (Hernandez-Ortega, 2011). Trust in technology ensures building stable relations between users and a given technology, which determines its future use. Developing their model for the adoption maturity of e-government solutions, Joshi and Islam (2018) pointed out that trust was an important element of sustainable adoption of e-government solutions. Carter and Bélanger built the hypothesis that reflected relationships

Fig. 1: Conceptual model



Source: own

between trust in the Internet and the intention to use an e-government service. Authors proved that trust in the Internet positively influenced the intention to use e-government (Carter & Bélanger, 2008). Also, the research conducted by Hernandez-Ortega proved that trust in technology positively influenced the intentions to continue using the technology (Hernandez-Ortega, 2011). Weerakkody et al. (2013) confirmed the previous conclusions regarding the positive impact of trust on the adoption and continued use of electronic government services. Considering the above, the authors formulated the following hypothesis:

Hypothesis (H5): Perceived trust (PT) will positively influence the future intention to use e-government.

Fig. 1 presents the conceptual model that reflects links between all theoretical variables and hypotheses.

3. Research Methodology

3.1 Data

The conducted research focused on e-Declaration – an electronic technology for submitting tax returns. This service and ICT tools were created by the Ministry of Finance for the electronic filing of tax returns. It is the most frequently used e-government service by Polish citizens. In 2018, the inhabitants of Poland filled more than 11 million tax returns electronically.

Research data was collected using a survey method. The conducted research was quantitative and allowed to verify the accepted research hypotheses. The process of data collection was carried out with the use of CATI (Computer Assisted Web Interview) technique.

The survey respondents Polish residents who had used the e-Declaration system within the last two years, i.e. they sent their tax return via the Internet. The research process was carried out by employees of the Ministry of Finance (MF). As part of this cooperation, the author developed a research questionnaire, which was validated by employees of the Ministry of Finance. The task of the Ministry of Finance was to send randomly an e-mail message with a link to the electronic survey to taxpayers registered in the MF database.

The study assumed the acquisition of a representative sample, which allowed the results to be generalised for the entire population. The minimum sample size was 1,067, assuming a confidence level of 0.95 (1-α) and a maximum permissible error of 3% calculated for the general population of about 11 million taxpayers using the e-government system. The survey was conducted in May 2018. Successive (due to the technical limitations of the mailbox) lots of e-mails from the dedicated account ankietaPB@mf.gov.pl, allowed for ongoing monitoring of the status of the survey completion. As soon as 2,067 completed questionnaires were received, the e-mail dispatch was suspended. After the analysis of the returned questionnaires and the elimination of forms with data gaps, 1,054 completed questionnaires containing 100% of answers were selected.

Of the 1,054 respondents, 484 (45.9%) were women, and 570 (54.1%) were men. The proportion of respondents aged 26-40 was 52.1% (549 persons), followed by 29.5% (311 persons) aged 41-60. The number of respondents in the age groups of 18-25 and

Tab. 1: Constructs and items

Constructs (source)	Abbr.	Observed variables (Items)	Mean	Cronbach's alpha
Perceived security level (Bélanger & Carter, 2008; Ranaweera, 2016; Shareef, Kumar, Kumar, & Dwivedi, 2011; Lee, Kim, & Ahn, 2011; Kurfal, Arifoglu, Tokdemir, & Paçin, 2017; Colesca, 2009; Hernandez-Ortega, 2011)	PS1	I can use the e-Declaration system comfortably due to Internet safety	5.54	0.933
	PS2	I feel that legal and technical safeguards in the e-Declaration system protect me from problems related to the use of the Internet	5.29	
	PS3	I feel confident that encryption systems and other technological solutions allow me to use the e-Declaration system in a securely	5.38	
	PS4	In general, I believe that the Internet is secure in the context of tax returns (e-Declaration)	5.33	
Perceived risk (Authors)	PR1	Using the e-Declaration system, I am exposed to the risk of failure to deliver the tax return at the right time and to the right institution (risk of results)	3.35	0.614
	PR2	Using the e-Declaration system, I am exposed to the risk of losing my personal data (information risk, privacy)	3.38	
Trust in e-Declaration (Lippert, 2007; Colesca, 2009; Al-Hujran, Al-Debei, Chatfield, & Migdadi, 2015)	T1	The e-Declaration system works according to my expectations	5.49	0.926
	T2	I am convinced that the e-Declaration system will function properly when I need it	5.38	
	T3	I can rely on the e-Declaration system	5.69	
	T4	The e-Declaration system is predictable and unchanged	5.42	
Future intention to use (Venkatesh, Morris, Davis, & Davis, 2003; Carter & Bélanger, 2005; Be´langer & Carter, 2008; Venkatesh, Thong, & Xu, 2012; Al-Hujran, Al-Debei, Chatfield, & Migdadi, 2015; Kurfal, Arifoglu, Tokdemir, & Paçin, 2017)	FI1	I intend to make greater use of the e-Declarations system	5.13	0.738
	FI2	I intend to make greater use of e-government services	5.61	

Source: own

over 61 years of age constituted about 9% of the respondents each (9.1% – 96 persons and 9.3% – 98 persons).

3.2 Measures

Since some constructs included in the theoretical model could not be directly observed, a series of measures was used in each case. Based on the literature study, four items have been identified to measure the Perceived Security (PS) level, four – the Perceived Risk (PR), four – the Trust in e-Government, and two – the Future Intention to use (Tab. 1). All constructs were measured using a seven-point Likert scale to access the degree to which a respondent agreed or disagreed with each of the items (1 = totally disagree; 7 = totally agree). Cronbach's alpha coefficients of the constructs were used to verify the reliability of the scale and proved the acceptable reliability of the scale ranging from 0.738 to 0.933 (Tab. 1). Descriptive statistics and composite reliability for the constructs and items are presented in Tab. 1.

4. Results

To verify the hypotheses, the authors used a two-step approach. First, the correlation analysis was used and followed up with the structural equation model (SEM).

Tab. 2 shows the correlation matrix for variables. Significant correlations were found between all constructs, but the strength of dependence was poor or moderate. In the case of relationships between constructs of perceived risk and other variables, a negative correlation appeared with a poor to moderate dependence.

The structural model was subsequently tested. The Generalized Least Squares (GLS) model with AMOS was set to test the hypothesised relationships shown in Fig. 1. GLS is a tool for estimating unknown parameters in a linear regression model. In the structural equation modelling (SEM), a measurement model allows setting the relationships between observed variables (i.e. indicators) and their respective unobserved (latent) variables by defining a particular structural model (Ejdys, 2016).

The appropriateness of the measurement model was evaluated by using the Chi-Square statistics. As Tab. 3 shows, the χ^2 value was statistically significant (χ^2 = 171.72, p < 0.005) indicating a good model fit to the data. As this measure is excessively conservative and is biased against large samples (Bollen, 1989), several disparate indices must be taken into consideration jointly to evaluate an accurate reflection of the overall model fit. The indices included the Root Mean Square Error of Approximation (RMSEA), the goodness-of-fit index (GFI), the adjusted goodness-of-fit index (AGFI), and comparative fit index (CFI). The results of the SEM test are provided in Tab. 3. The approximate fits are also good, specifically, the Normed Chi-Square (i.e. χ^2/df) value = 3.733, which is well within the acceptable range for this heuristic (Bentler & Chou, 1987; Bollen, 1989), RMSEA = 0.051, and is a good value (Konarski, 2010; Bollen, 1989; Ejdys, 2016). This means that the model is likely to be interpreted as a real model of the relationship between the variables.

Fig. 2 presents the individual structural path estimates. Tab. 3 reports the results for the structural model depicted in Fig. 2.

The hypotheses can be confirmed through the interpretation of the structural path coefficients. The results of testing the relationships between constructs in the model

Tab. 2: Correlation matrix (Spearman's coefficient)

	Perceived security level	Perceived risk	Trust in e-Declaration	Future intention to use
Perceived security level	1	-0.271**	0.683**	0.455**
Perceived risk	-0.271**	1	-0.224**	-0.112**
Trust in e-Declaration	0.683**	-0.224**	1	0.434**
Future intention to use	0.455**	-0.112**	0.434**	1

Source: own

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

Tab. 3: Results of the test hypotheses

Hypothesis	Estimate	S.E.	C.R.	P	Hypothesis testing
Hypothesis (H1). Perceived risk (PR) will negatively influence trust in e-government solutions (T)	0.042	0.027	1.521	0.128	Reject
Hypothesis (H2). Perceived security (PS) will positively influence trust in e-government solutions (T)	0.723	0.030	24.074	***	Support
Hypothesis (H3). Perceived risk (PR) will negatively influence the future intention (FI) to use e-government	0.127	0.036	3.499	***	Support
Hypothesis (H4). Perceived security (PS) will positively influence the future intention (FI) to use e-government	0.261	0.046	5.657	***	Support
Hypothesis (H5). Perceived trust (PT) will positively influence the future intention (FI) to use e-government	0.292	0.047	6.191	***	Support
χ^2 = 171.72; d.f. = 46; χ^2/d.f. = 3.733; p < 0.005 RMSEA = 0.051; GFI = 0.973; AGFI = 0.954 *** p < 0.001, Hoelter — 386 Adopted level of the statistical significance was 0.001					

Source: own

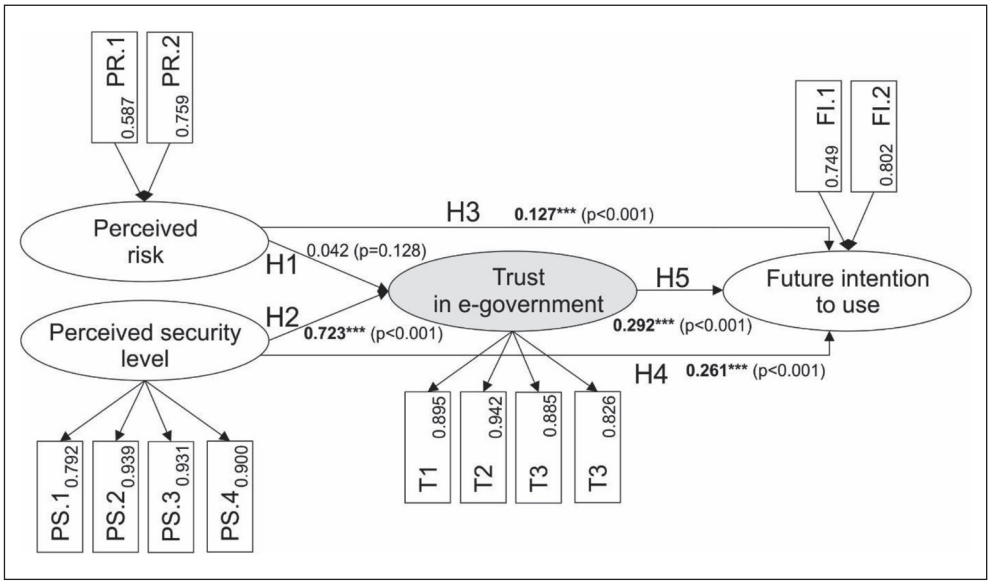
show that only a part of the relationship is statistically significant. Trust in e-Declaration (T) is statistically important due to the perceived security level (PS). Thus, this positive relationship confirmed that hypothesis H2 was supported. The conducted research did not confirm a statistically significant relationship between the perceived risk (PR) and trust in the e-Declaration (T), so the hypothesis H1 was rejected. The research also confirmed that trust in e-Declaration (T), perceived security level (PS) and perceived risk (PR) have a statistically significant impact on future intentions (FI) of users, which allowed to support hypotheses H3, H4 and H5 (Tab. 3).

5. Discussion

The obtained results did not confirm a statistically significant relationship between the perceived risk and trust in e-Declaration, thus rejecting hypothesis H1. The variables reflecting the level of perceived risk concerned the possibility of losing personal data (PR2) and the situation of delivering the e-Declaration at the right time and to the right institution (PR1). The risks were rated low by respondents (the mean PR1 – 3.35, PR – 3.38), confirming that respondents did not consider these risks significant. The obtained results were different from those relating to the technologies offered by the business sector (and not government). According to the results of other authors (Carter & Bélanger, 2008; Khasawneh & Abu-Shanab, 2013), a highly rated level of trust in the e-Declaration would possibly reduce the level of perceived risk related to technologies offered by the government.

In several studies by other authors, security elements are regarded as a key factor for building trust in technology. In the Polish context, this factor is also decisive. The results of research performed by the Polish Ministry of Digitalisation showed that the level of security in dealing with official matters via the Internet was relatively low (score of 6.4 on a 10-degree scale, the Polish Ministry of Digitalization, 2016). The statements in the research questionnaire targeted the sense of Internet security perceived by the respondents as well as legal and technical security measures that ensure the safety of users. The results obtained by the authors confirmed a statistically significant relationship between the perceived

Fig. 2: Measurement model



Source: own

Note: Values on paths between latent variables are standardised regression coefficients and numbers at latent variable indices are factor loads.

level of security and trust in technology, and thus substantiated the hypothesis H2. This is convergent with the results obtained by other authors. In the model proposed by Shareef et al. (2011), the variable determining trust in e-government solutions was perceived as the level of uncertainty, understood as the risk of transactions conducted over the Internet, resulting from uncontrolled situations in the virtual environment. The authors showed a negative impact of the level of uncertainty on the level of trust in technology. The second variable in the model was the perceived level of user security. The research carried out by the Shareef et al. as well as other studies have led to a hypothesis indicating that the perceived level of security affected the level of trust in e-government solutions.

The authors were also interested in the relationship between the perceived level of security and risk and the intentions of users to use e-government solutions in the future. The results obtained allowed to support both hypotheses H3 and H4. The analysis of correlation coefficients confirmed that a higher level of perceived risk contributes to a lower level of trust in e-Declaration. Results achieved were opposite to the results of Carter and Bélanger (2008) and Jasimuddin et al. (2017) who proved that higher levels of perceived risk did not decrease the intention to use. The obtained results, which supported the hypothesis H4, were consistent with the results of other authors and confirmed that a lower level of perceived safety lowered the level of solution adoption (Ranaweera, 2016).

An important relationship was studied in the model between trust in e-Declaration and future intentions to use e-government solutions. The hypothesis H5, reflecting this relationship, was supported. Belanche, Casaló and Flavián achieved similar results for e-government solutions (2012). The team of Jacob et al. (2017), studying the adoption of eGovernment solutions, expanded the UTAUT model with a construct of trust and showed a statistically significant impact of technology trust on the future intentions of users. The literature studies

on the adoption of e-government solutions carried out by the Witarsyah, Fudzee and Salamata (2017) also confirmed the positive impact of trust on the future intentions of users.

Conclusions

Popularisation of e-administration solutions and the relatively low level of adoption of e-administration technologies by the Polish society were the main premise of the research undertaken by the authors. The literature studies on factors determining the adoption of e-administration technology allowed to narrow down the discussed issues to the aspects related to the risk and security level perceived by users in the context of technology adoption. The verification of the theoretical model was carried out using the e-Declaration technology, which allows to fill in and submit tax returns via the Internet. In the constructed model, the output variables were, on the one hand, trust in e-Declaration and, on the other hand, future intentions of users to use the e-Declaration system.

The obtained results confirmed that among two input variables in the model, the level of security perceived by the users determined the level of trust in the e-Declaration. Compared to technologies offered by the private sector (e.g. e-commerce), the level of perceived risk did not turn out to be a statistically significant determinant of trust in e-Declaration – a tool offered by public institutions. The research supports a conclusion that when building models of trust in e-government, it is worth adopting only one of the variables of perceived security or perceived risk, considering the purpose and subject matter of the authors' research.

The statistically important relationship between perceived security and trust in e-government technology indicated the practical utility of using a security variable in the promotion and encouragement of the public to use the solutions offered by the administration. It also indicates the direction in which technological innovation in the area of e-government should develop, so that it is aligned with the Responsible Research and Innovation paradigm (Nazarko, 2016).

At the same time, the research confirmed that both the perceived risk and the perceived security level determine the future intentions of users to use ICT solutions offered by public administration.

In the context of the results obtained, future research should focus on clarifying the role of perceived risks in building trust in different technologies offered by the private sector and public administrations. It could be worth-while investigating the extent to which the varying level of perceived risk resulting from threats experienced by users determines trust and the future intention to use the technology. It can be assumed that in the case of technologies (e.g. robots in everyday life) where the perceived level of human risk is higher, the level of risk would play a key role in building trust in technology.

References

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

AlAwadhi, S., & Morris, A. (2008). The Use of the UTA UT Model in the Adoption of e-Government. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (HICSS 2008). https://doi.org/10.1109/HICSS.2008.452.

Al-Thunibat, A., Zin, N., & Sahari, N. (2011). Modelling the Factors That Influence Mobile Government Services Acceptance. *African Journal of Business Management, 5*(34), 13030-13043. https://doi.org/10.5897/AJBM11.2083.

Alzahrani, L., Al.-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review, 26*(1), 164-175. https://doi.org/10.1016/j.ibusrev.2016.06.004.

Ayyash, M. M., Ahmad, K., & Singh, D. (2013). Investigating the effect of information systems factors on trust in e-government initiative adoption in Palestinian public sector. *Research Journal of Applied Sciences, Engineering and Technology, 5*(15), 3865-3875. https://doi.org/10.19026/rjaset.5.4447.

Belanche, D., Casaló, L. V., & Flavián, C. (2012). Integrating trust and personal values into the Technology Acceptance Model: The case of e-government services adoption. *Cuadernos de Economía y Dirección de la Empresa, 15*(4), 192-204. https://doi.org/10.1016/j.cede.2012.04.004.

Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems, 17*(2), 165-176. https://doi.org/10.1016/j.jsis.2007.12.002.

Benlian, A., & Hess, T. (2011). The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities. *International Journal of Electronic Commerce, 15*(4), 7-56. https://doi.org/10.2307/41300715.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5-25. https://doi.org/10.1111/j.1365-2575.2005.00183.x.

Carter, L., & Weerakkody, V. (2008). E-government adaptation: a cultural comparison. *Information System Frontier, 10*(4), 473-482. https://doi.org/10.1007/s10796-008-9103-6.

Chen, J. V., Jubilado, R. J. M., Capistrano, E. P. S., & Yen, D. C. (2015). Factors affecting online tax filing – An application of the IS Success Model and trust theory. *Computers in Human Behavior, 43*, 251-262. https://doi.org/10.1016/j.chb.2014.11.017.

Chen, L. (2008). A Model of Consumer Acceptance of Mobile Payment. *International Journal of Mobile Communications, 6*(1), 32-52. https://doi.org/10.1504/IJMC.2008.015997.

Chodakowska, E., & Nazarko, J. (2017). Environmental DEA method for assessing productivity of European countries. *Technological and Economic Development of Economy, 23*(4), 589-607. https://doi.org/10.3846/20294913.2016.1272069.

Colesca, S. E. (2009). Understanding Trust in e-Government. *Inzinerine Ekonomika-Engineering Economics, 63*(4), 1-15.

Ejdys, J. (2016). Prospective Quality Attributes of Nursing Home Care Services. In *Proceedings of the 9th International Scientific Conference Business and Management*, *Vilnius, Lithuania, 12-13 May 2016*. https://doi.org/10.3846/bm.2016.59.

Ejdys, J., & Halicka, K. (2018). Sustainable Adaptation of New Technology – The Case of Humanoids Used for the Care of Older Adults. *Sustainability*, *10*(10), 3770. https://doi.org/10.3390/su10103770.

European Commission. (2016). *Digital Public Services. Europe's Digital Progress Report 2016*. Retrieved from: https://ec.europa.eu/isa2/sites/isa/files/official-documents/digital-public-services.pdf.

European Commission. (2018a). *Digital Single Market. Digital Economy & Society*. Retrieved from www.digital-agenda-data.eu/charts/desi-composite#chart.

European Commission. (2018b). *Glossary. Digital Single Market.* Retrieved from https://ec.europa.eu/digital-single-market/en/glossary#letter_e.

Eurostat. (2016). *Digital Economy and Society Database*. Retrieved from www.ec.europa.eu/eurostat/web/digital-economy-and-society/data/database.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *Database for Advances in Information Systems, 33*(3), 38-53. https://doi.org/10.1145/569905.569910.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90. https://doi.org/10.2307/30036519.

Hernández-Ortega, B. (2011). The role of post-use trust in the acceptance of a technology: Drivers and consequences. *Technovation*, *31*(10-11), 523-538. https://doi.org/10.1016/j.technovation.2011.07.001.

Hiltunen, E., & Hiltunen, K. (2015). *Technolife 2035. How Will Technology Change our Future*. Cambridge: Cambridge Scholars Publishing.

Hole, K. J. (2016). Building Trust in E-Government Services. *Computer*, *19*(1), 66-74. https://doi.org/10.1109/MC.2016.4.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in the Netherlands. *Computers in Human Behavior, 23*(4), 1838-1852. https://doi.org/10.1016/j.chb.2005.11.003.

Jacob, D. W., Fudzee, M. F., Salamat, M. A., Kasim, S., Mahdin, H., & Ramli, A. A. (2017). Modelling End-User of Electronic-Government Service: The Role of Information Quality, System Quality and Trust. In *IOP Conference Series: Materials Science and Engineering, 226* (pp. 1-10). https://doi.org/10.1088/1757-899X/226/1/012096.

Jasimuddin, S. M., Mishra, N., & Saif Almuraqab, N. A. (2017). Modelling the factors that influence the acceptance of digital technologies in e-government services in the UAE: a PLS-SEM Approach. *Production Planning & Control, 28*(16), 1307-1317. https://doi.org/10.1080/09537287.2017.1375144.

Joshi, P. R., & Islam, S. (2018). E-Government Maturity Model for Sustainable E-Government Services from the Perspective of Developing Countries. *Sustainability, 10*(6), 1882. https://doi.org/10.3390/su10061882.

Kaur, K., & Rampersad, G. (2018). Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *Journal of Engineering and Technology Management, 48,* 87-96. https://doi.org/10.1016/j.jengtecman.2018.04.006.

Khanyako, E., & Maiga, G. (2013). An information security model for e-Government services adoption in Uganda. In *2013 IST-Africa Conference & Exhibition.* Retrieved from https://ieeexplore.ieee.org/document/6701771/.

Khasawneh, R. W., & Abu-Shanab, E. (2013). E-government acceptance factors: trust and risk. In *The 6th international conference on information technology* (pp. 8-10). http://icit.zuj.edu.jo/icit13/Papers%20list/Camera_ready/E-Technology/613_final.pdf.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564. https://doi.org/10.1016/j.dss.2007.07.001.

Koller, M. (1988). Risk as a determinant of trust. *Basic and Applied Social Psychology, 9*(4), 265-276. https://doi.org/10.1207/s15324834basp0904_2.

Kolnhofer Derecskei, A. (2018). Relations between risk attitudes, culture and the endowment effect. *Engineering Management in Production and Services, 10*(4), 7-20. https://doi.org/10.2478/emj-2018-0019.

Kumar, V., Mukerji, B., Butt, I., & Persaud, A. (2007). Factors for successful e-government adoption: A conceptual framework. *The Electronic Journal of e-Government, 5*(1), 63-76.

Kurfal, M., Arifoglu, A., Tokdemir, G., & Paçin, Y. (2017). Adoption of e-government services in Turkey. *Computers in Human Behavior, 66*, 168-178. https://doi.org/10.1016/j.chb.2016.09.041.

Lai, K. W. I., Tong, V. W. L., & Lai, D. C. F. (2011). Trust factors influencing the adoption of internet-based interorganizational systems. *Electronic Commerce Research and Applications, 10*(1), 85-93. https://doi.org/10.1016/j.elerap.2010.07.001.

Lankton, N. K., & McKnight, H. D. (2011). What Does it Mean to Trust Facebook? Examining Technology and Interpersonal Trust Beliefs. *Data Base for Advances in Information Systems, 42*(2), 32-54. https://doi.org/10.1145/1989098.1989101.

Lean, O. K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). Factors influencing intention to use e-government services among citizens in Malaysia. *International Journal of Information Management, 29*(6), 458-475. https://doi.org/10.1016/j.ijinfomgt.2009.03.012.

Lee, C. B. P., & Wan, G. (2010). Including Subjective Norm and Technology Trust in the Technology Acceptance Model: A Case of E-Ticketing in China. *Data Base for Advances in Information Systems, 41*(4), 40-51. https://doi.org/10.1145/1899639.1899642.

Lemire, M., Paré, G., Sicotte, C., & Harvey, C. (2008). Determinants of Internet use as a preferred source of information on personal health. *International Journal of Medical Informatics, 77*(11), 723-734. https://doi.org/10.1016/j.ijmedinf.2008.03.002.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*(4), 967-985. https://doi.org/10.2307/2578601.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *Journal of Strategic Information Systems, 17*(1), 39-71. https://doi.org/10.1016/j.jsis.2008.01.001.

Lippert, S. K., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behaviour. *Journal of Information Science, 32*(5), 434-448. https://doi.org/10.1177/0165551506066042.

Liu, Y., & Zhou, C. (2010). A citizen trust model for e-government. In *Software Engineering and Service Sciences (ICSESS), IEEE International Conference* (pp. 751-754). https://doi.org/10.1109/ICSESS.2010.5552260.

Luhmann, N. (1979). *Trust and Power*. London: John Wiley.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734. https://doi.org/10.2307/258792.

Mazey, N. CHL, & Wingreen, S. C. (2017). Perceptions of trust in bionano sensors: Is it against our better judgement? An investigation of generalised expectancies and the emerging technology trust paradox. *International Journal of Distributed Sensor Networks, 13*(7), 1-16. https://doi.org/10.1177/1550147717717388.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359. https://doi.org/doi:10.1287/isre.13.3.334.81.

Mellouli, M., Bentahar, O., & Bidan, M. (2016). Trust and e-government acceptance: The case of Tunisian on-line tax filing. *Electronic Journal Information Systems Evaluation, 19*(3), 197-212.

Muraya, B. M. (2015). Factors affecting successful adoption of e-government in Kenya's public sector (Unpublished masters thesis). United States International University Africa, Nairobi, Kenya.

Myeong, S., Kwon, Y., & Seo, H. (2014). Sustainable E-Governance: The Relationship among Trust, Digital Divide, and E-Government. *Sustainability, 6*(9), 6049-6069. https://doi.org/10.3390/su6096049.

Nazarko, J., Ejdys, J., Halicka, K., Magruk, A., Nazarko, Ł., & Skorek, A. (2017). Application of Enhanced SWOT Analysis in the Future-oriented Public Management of Technology. *Procedia Engineering*, *182,* 482-490. https://doi.org/10.1016/j.proeng.2017.03.140.

Nazarko, L. (2016). Responsible Research and Innovation – A New Paradigm of Technology Management. In *9th International Scientific Conference "Business and Management 2016"*. https://doi.org/10.3846/bm.2016.71.

Nazarko, L. (2017). Future-Oriented Technology Assessment. *Procedia Engineering, 182,* 504-509. https://doi.org/10.1016/j.proeng.2017.03.144.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 69-103.

Polak-Sopinska, A., & Wisniewski, Z. (2009). The analysis and assessment of adjustment of selected web sites and web browsers to the needs of people with disabilities. *Lecture Notes in Computer Science, 5616*(22), 768-777. https://doi.org/10.1007/978-3-642-02713-0_82.

Polish Ministry of Digitalization. (2016). *E-administracja w oczach internautów (E-Government in the eyes of Internet users)*, Sopot.

Radziszewski, P., Nazarko, J., Vilutiene, T., Dębkowska, K., Ejdys, J., Gudanowska, A., Halicka, K., Kilon, J., Kononiuk, A., Kowalski, K. J., Król, J. B., Nazarko, Ł., & Sarnowski, M. (2016). Future trends in road pavement technologies development in the context of environmental protection. *The Baltic Journal of Road and Bridge Engineering, 11*(2), 160-168. https://doi.org/10.3846/bjrbe.2016.19.

Ranaweera, H. M. B. P. (2016). Perspective of trust inwards e-government initiatives in Sri Lanka. *SpringerPlus, 5*(22), 1-11. https://doi.org/10.1186/s40064-015-1650-y.

Reiersen, J. (2017). Trust as a booster. *Journal of Business Economics and Management, 18*(4), 585-598. https://doi.org/10.3846/16111699.2017.1334228.

Rotchanakitumnuai, S. (2007). The important risk factors of E-Government service adoption. In *2007 International Conference on Wireless Communications, Networking and Mobile Computing*. https://doi.org/10.1109/WICOM.2007.904.

Rukiza, V., Karokola, G., Mwakalinga, J., & Kowalski, S. (2011). Secure e-government adoption: A case study of Tanzania. In *Proceedings of the European Security Conference (ESC 2011)* (pp. 18-32). Örebro, Sweden.

Rutkauskas, A. V., & Stasytytė, V. (2011). Peculiarities of risk concept formation. *Business: Theory and Practice, 12*(2), 141-149. https://doi.org/10.3846/btp.2011.15.

Salam, A. F., Rao, H. R., & Pegels, C. C. (2003). Consumer-perceived risk in e-commerce transactions. *Communications of the ACM, 46*(12), 325-331. https://doi.org/10.1145/953460.953517.

Salam, M. A. (2017). The mediating role of supply chain collaboration on the relationship between technology, trust and operational performance. An empirical investigation. *Benchmarking: An International Journal*, *24*(2), 298-317. https://doi.org/10.1108/BIJ-07-2015-0075.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting website visitors into buyers: how website investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*(2), 133-148. https://doi.org/10.1509/jmkg.70.2.133.

Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). E-Government Adoption Model (GAM): Differing service maturity levels. *Government Information Quarterly, 28*(1), 17-35. https://doi.org/10.1016/j.giq.2010.05.006.

Shiau, W.-L., & Dwivedi, Y. K. (2013). Citation and co-citation analysis to identify

core and emerging knowledge in electronic commerce research. *Scientometrics, 94*(3), 1317-1337. https://doi.org/10.1007/s11192-012-0807-5.

Söderström, E., Eriksson, N., & Åhlfeldt, R.-M. (2016). Managing healthcare information: analyzing trust. *Journal of Health Care Quality Assurance, 29*(7), 786-800. https://doi.org/10.1108/IJHCQA-11-2015-0136.

Tung, F.-C., Chang, S.-C., & Chou, C.-M. (2008). An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics, 77*(5), 324-335. https://doi.org/10.1016/j.ijmedinf.2007.06.006.

United Nations. (2016). *United Nations E-Government Survey 2016. E-Government in Support of Sustainable Development*. New York: United Nations.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Science, 39*(2), 273-315. https://doi.org/10.1111/j.1540-5915.2008.00192.x.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, V., & Davis, F. D. (1966). A Model of the Antecedents of Perceived Ease of Use: Development and Test. *Decision Sciences, 27*(3), 451-481. https://doi.org/10.1111/j.1540-5915.1996.tb00860.x.

Verkijika, S. F., & Wet, L. D. (2018). E-government adoption in sub-Saharan Africa. *Electronic Commerce Research and Applications, 30*, 83-93. https://doi.org/10.1016/j.elerap.2018.05.012.

Veselý, Š., & Dohnal, M. (2016). Formalized qualitative modeling of online trust: introduction of the method and a detailed example. *E&M Ekonomie a Management*, *19*(2), 201-213. https://doi.org/10.15240/tul/001/2016-2-014.

Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems, 6*(3), 72-101. https://aisel.aisnet.org/jais/vol6/iss3/4.

Warkentin, M., Gefen, D., Pavlou, P., & Rose, G. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets, 12*(3), 157-162.

Weerakkody, V., El-Haddadeh, R., Al-Sobhi, F., Shareef, M. A., & Dwivedi, Y. K. (2013). Examining the influence of intermediaries in facilitating-government adoption: An empirical investigation. *International Journal of Information Management, 33*(5), 716-725. https://doi.org/10.1016/j.ijinfomgt.2013.05.001.

Wisniewski, Z., & Polak-Sopinska, A. (2009). HCI standards for handicapped. *Lecture Notes in Computer Science, 5614*(21), 672-676. https://doi.org/10.1007/978-3-642-02707-9_76.

Witarsyah, D., Fudzee, M. F., & Salamat, M. A. (2017). A conceptual study on generic end users adoption of e-government services. *International Journal of Advanced Science Engineering Information Technology, 7*(3), 1000-1006. https://doi.org/10.18517/ijaseit.7.3.1654.

Assoc. Prof. Joanna Ejdys
Bialystok University of Technology
Faculty of Engineering Management
Poland
j.ejdys@pb.edu.pl

Prof. Romualdas Ginevicius
Bialystok University of Technology
Faculty of Engineering Management
Poland
r.ginevicius@pb.edu.pl

Assoc. Prof. Zoltan Rozsa
Alexander Dubček University of Trenčín
Faculty of Social and Economic Relations
Slovakia
zoltan.rozsa@tnuni.sk

Ing. Katarina Janoskova, PhD.
University of Zilina
Faculty of Operation and Economics
of Transport and Communications
Slovakia
katarina.janoskova@fpedas.uniza.sk

Abstract

THE ROLE OF PERCEIVED RISK AND SECURITY LEVEL IN BUILDING TRUST IN E-GOVERNMENT SOLUTIONS

Joanna Ejdys, Romualdas Ginevicius, Zoltan Rozsa, Katarina Janoskova

Increasingly, social and economic development is determined by the technologies, including ICT. Technologic development can be seen, on the one hand, as an opportunity and, on the other hand, as a threat to the socio-economic development. The substitution of human-to-human relationships with human-to-machine or machine-to-machine connections is becoming increasingly more controversial, thus providing a basis for scientific deliberations. Trust, which is the cornerstone of all interpersonal relationships, is frequently mentioned in the context of interactions between humans and technologies, becoming the object of scientific interest. One of the growing ICT areas is services provided by public administration (e-government) enabling citizens to deal with official matters via the Internet. Considering a relatively low level of e-government technology adoption in Poland, compared to other European countries, it is justified to search for reasons for such a state of affairs. Trust seems to have an important place among many factors determining the development of e-government technology. In technology acceptance models, among the determinants of trust in technology, especially in the context of personal data security, an important role is played by the perceived level of risk and security associated with the use of solutions. This article aimed to identify if the perceived risk and security of e-government technology determine the level of trust in the technology and future intentions of its adoption. Based on the literature review, the authors hypothesised that trust in e-government technology and the future intention of its use could be directly shaped by perceived risk and security. An electronic questionnaire was used to collect research data from Polish citizens. All in all, 1,067 forms were filled. Results received using the structural equation modelling confirmed that the most important factor shaping trust in technology was a perceived level of security. Results also confirmed a positive impact of trust on the future intended use.

Key Words: *E-government, trust in technology, perceived risk, safety.*

JEL Classification: *G34, M12.*

DOI: *10.15240/tul/001/2019-3-014*