SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 169

CURRENT CONCERNS IN DIGITAL ECONOMY ERA. LESSONS LEARNT FORM POLISH ADVANCED INTERNET USERS

Agata RUDNICKA[1*], Dominika KACZOROWSKA-SPYCHALSKA[2], Janusz REICHEL[3], Monika KULIK[4]

[1] University of Lodz, Faculty of Management; agata.rudnicka@uni.lodz.pl, ORCID: 0000-0002-9151-4263
[2] University of Lodz, Faculty of Management; dominika.spychalska@uni.lodz.pl, ORCID: 0000-0002-2566-0297
[3] University of Lodz, Faculty of Management; janusz.reichel@uni.lodz.pl, ORCID: 0000-0002-7594-380X
[4] Orange Polska SA
* Correspondence author

Purpose: Digital Economy development is influenced by many factors, including the users' acceptance of the technology. The interesting group of users are technologically advanced and may shape the technology's use and enhance its development. The purpose of the study is to explore the way customers are present on the Internet, and their attitudes to ethics and responsibility in the virtual environment.
Design/methodology/approach: The study was conducted on a representative group of 1002 adult Internet users from Poland. The CAVI method on the research consumer panel was used. The authors empirically examine the developed research hypotheses using statistical tests.
Findings: The study results show that advanced technology users have a more conscious approach to their presence on the Internet. Technology advanced users are familiarised with the tools and applications that may supper them with everyday activities and ease their professional duties. They are also more concerned about ethical and safety issues. At the same time, as consumers of technology, they are ready to disclose personal data if some benefits are seen.
Originality/value: Research results support the development of understanding online activities of Internet users. They indicate some crucial points for a technology provider in designing and improving new tools and applications. Technology advanced users as testers can spread the technology appliances and support their acceptance if they find them ethical and safe. It leads to the development of the digital economy and benefits the whole society.

Keywords: digital technology, advanced technology users, online consumers, ethical concerns, customers responsibility, the safety of the technology.

Category of the paper: Research paper.

1. Introduction

Technological development is not only the sum of activities undertaken by the business. It also includes the approach of Internet users who are ready to use new solutions and tools and accept solutions proposed by companies to accelerate their progress (Amoroso, Hunsinger, 2009; Reisdorf, Groselj, 2017).

The Digital Economy and Society Index (DESI) for EU countries allow monitoring of countries' progress in digitisation. As an example of a Central and Eastern Europe (CEE) country in this index, Poland occupies one of the last positions, despite the readiness of enterprises to be technologically advanced. The development of artificial intelligence and the availability of modern technologies and resources for further digitisation are noticed in Poland (DESI EU). However, they are insufficient for real growth, as evidenced by their position in the classification. The article examines the issues related to how technology is used by a representative group of adult Poles, referring to the use of Internet services, human capital and the integration of digital technologies that are the dimensions of the DESI index.

Technology use means several issues that should be considered when planning the development of an offered solution. These are how users approach a presented technology, the level of acceptance, ethical dimension and attitudes towards responsibility and safety related to its use (Hesselman et al., 2020). Especially the area of ethics and safety can show what is a priority for users when introducing technological opportunities.

The paper aims to understand how Internet users use new technologies and what challenges they perceive regarding their presence in the digital world.

2. Conceptual background and hypotheses development

2.1. Digital economy - state – of – the art in Poland

Nowadays, the access to information, models of its processing and management, and economic competence, including the so-called reengineering of business processes (Chancellery of the Prime Minister, 2020). According to the McKinsey report *Digital Challengers in the next normal. Central and Eastern Europe on a path to digitally-led growth* (McKinsey & Company, 2020), Poland shows great growth potential for the digital economy although its current level of digitization is lower than in the countries of Northern and Western Europe. This is also confirmed by the Digital Economy and Society Index (DESI) (European Commission, 2021), according to which in 2021 Poland was ranked 24th among the 27 EU Member States. The dynamics of the observed changes in the CEE countries belonging to the EU, except Bulgaria and Romania, were faster than in Poland. Access to broadband Internet,

digital public services and possibilities of using open data were highly rated. Unfortunately, it is worrying that digital skills, both basic and above basic, of the Polish society as well as the level of digital technology usage by Polish enterprises are below the average for the entire European Union. Undoubtedly, Poland's fourth place among the EU Member States deserves praise in terms of actions for data openness (European Commission, 2021), including the impact of the category of open data on Polish society and business.

Acquiring, collecting, analyzing, processing and consciously using technology in various sectors and industries of individual economies is now considered a fundamental competence of market participants. In line with the assumptions of *Shaping Europe's Digital Future* (European Commission, 2020a), the implementation of activities aimed at adapting the EU to the digital age is one of the most important priorities for the coming years, while taking care of democratic values, ethics of applied solutions and sustainable development. Similar postulates can also be noticed in a number of other documents and studies, such as the European Commission's report *Liability for Artificial Intelligence and other emerging digital technologies* (European Commission, 2019), *White Paper on Artificial Intelligence - A European approach to excellence and trust* (European Commission, 2020b), *Artificial Intelligence and fundamental rights* (European Union Agency For Fundamental Rights, 2020) and in national documents of individual countries, e.g. *Policy for the Development of Artificial Intelligence in Poland from 2020" (MP2021.23).* Even though according to McKinsey experts, both Poland and other CEE countries have a large digital potential, unfortunately, like the entire EU, they are giving way to American and Chinese BigTechs, building their position rather on the implementation of foreign technologies - they are their recipients, not creators and suppliers. A crucial problem in this respect may be the limited level of connection between the world of business and science, slowing down the dynamics of knowledge transfer and its potential rapid commercialization.

Polish enterprises generally have a positive attitude towards the potential implementation of new technologies, including in particular the use of social media in the process of communication and building the image of their brand, electronic information exchange and online sales. However, according to the indicator of the use of digital technologies, 60% of enterprises are characterized by a very low level of digitization, and only 11% of them are enterprises with a high degree of digitization, which puts Poland below the European average (European Commission, 2021a). Unfortunately, extensive changes can be seen primarily in large enterprises employing over 250 people. In the case of enterprises from the SME sector, only 32% increased their use of digital tools and platforms, and 18% invested in new hardware or software (McKinsey & Company, 2020).

In the opinion of 63% of Poles, the activities carried out in this area by enterprises are primarily the result of generating innovations aimed at a better understanding of clients and the increasing intensification of the process of satisfying their needs, so as to provide them with the widest range of benefits (customer-centric orientation). At the same time, however, almost a quarter believe that the introduced changes are driven only by the will to increase the

economic benefits related to the conducted activity (minimizing costs, increasing efficiency, maximizing profit) (PAYBACK Poland, 2021).

The interest in e-commerce public administration services has increased significantly, including in the area of food products and entertainment (McKinsey & Company, 2020; PWC, 2021). In 2020, almost 42% of respondents appreciate technologies although to a large extent they were limited to simple activities, such as submitting completed e-forms. A significant limitation in the use of the Internet potential in various spheres of activity of Poles seems to be the level of difficulty in their absorption, determined by their digital skills. Unfortunately, this indicator in Poland is below the EU average and is at the level of 44% (the EU average is 58%) (European Commission, 2021). In the population of people aged 16-74 who use the Internet, people with a low level of general digital skills accounted for 31.5%, people with basic digital skills – 24.1%, and people with above basic digital skills - 26.1% (GUS, 2020). However, this does not change the dominant belief among Poles that modern technologies are a necessary condition for the development of the economy, as indicated by 94% of respondents by Payback (Payback Poland, 2021). Obviously, this requires a comprehensive look at the connection and dependencies of various stakeholder groups in accordance with the quadruple helix model (business, state administration, research and development entities, society).

2.2. Digital economy – ethics, safety and responsibility

The Digital Economy and the development of new technologies caused a lot of ethical and moral concerns raised. There are some ethical principles and references developed which are designed to frame the scope of activities of all parties engaged in the virtual presence (e.g., Stahl, Timmermans, Mittelstadt, 2016; Saltz, Dewar, 2019; Allen, 2019; Floridi, 2019). The separate principles of ethical approach in AI are studied too e.g., Jobin and others identify 11 principles for ethical AI (Jobin, Ienca, Vayena, 2019). The moral challenges of AI have their own place in the debate about the need to define the limits of AI development without limiting the possibility of maintaining the autonomy of decisions, process control or data protection (e.g., Oxborough et al., 2018; Green, 2018; Floridi et al., 2018; Royakkers et al., 2018). Equality, non-discrimination, respect and dignity issues are additional matters in this discussion (Algorithm Watch, 2019). Ethical aspects of technology are associated with different kinds of risks to be managed (Meek et al., 2016).

A security risk is any possible event or sequence of actions that may lead to a breach of one or more security components (Tsiakis, Stephanides, 2005). From the consumer's perspective, security is an important decision-making factor. Privacy issues are positively related to the likelihood of buying online (Miyazaki, Fernandez, 2001; Salisbury et al., 2001; Yang, Jun, 2002; Milne, 2000; Chang, Chen, 2009).

There are two dimensions of security: objective and subjective from the point of view of new technology users (Linck et al., 2006). Regardless of the applied technological solutions and legal guidelines, the customers' sense of security is necessary to create the required level of trust enabling online transactions (Chellappa, Pavlou, 2002; Ally, Toleman, 2005).

Security and privacy can be considered as two separate constructs (Belenger et al., 2002). However, due to the fact that security mainly relates to shared data, this aspect is often associated with privacy concerns (Miyazaki, Fernandez, 2000; Gurung, Raja, 2016; Sheehan, Hoy, 2000; Ariffin et al., 2018).

The extent to which internet users are concerned about their online safety and privacy varies from country to country. A 2019 study on internet security and trust conducted by the Center for International Governance Innovation (CIGI) and Ipsos, in collaboration with UNCTAD and the Internet Society, found that 78% of internet users in 25 economies are at least somewhat worried about their own online privacy (CIGI-Ipsos et al., 2019).

One of the most important aspects of security is data security. (Smith et al., 1996; Kshetri, 2016). A key factor influencing privacy concerns is the user's perception of control over personal information (Xu, et al., 2012; Hong, Thong, 2013; Sheehan, Hoy, 2000). It is also noted that the magnitude of the impact of online privacy concerns may depend on consumer characteristics such as gender, age and education (Riquelme, Roman, 2014).

Research shows that concerns about the misuse of personal data are the main cause of distrust on online markets (Gupta, Dubey, 2016; Fortes, 2017; Hofacker, 2016; Boone et al., 2019).

Concerns are growing about issues related to privacy and security, democracy and ethical challenges, as well as the risk of mass surveillance and digital colonialism (Couldry, Mejias, 2019; Mayer-Schönberger, Ramge, 2018).

According to the Ipsos Global Trends Global Survey (2020), concern about Today, nearly three-quarters of the world is concerned about how companies collect and use our digital data. 67% of respondents are also concerned about how governments use our personal information - an increase of 6% from 2013. More than eight out of ten respondents believe that companies should provide more details about the data their websites collect.

Our data and privacy are becoming an element of commercial exchange (Acquisti et al., 2013; Martin, Murphy, 2017). While there seem to be growing concerns around the world about data privacy and online security, there is a "data privacy paradox" - users of new technologies are willing to share personal data, and thus their privacy, in exchange for various services or better offer (Kokolakis, 2017; Mosteller, Poddar, 2017). The scale of this phenomenon is growing. (Ipsos, 2020). Despite the perceived risk, more people would prefer not to know much about data privacy (Milne, Culnan, 2004).

However, the terms of use that should detail the company's practices are unclear and complex (Mukherjee, Nath 2003; Kim et al., 2010). They are designed to ensure organizational compliance and limit liability, not to understand the consumer (MacDonald, Cranor, 2008; Reidenberg et al., 2015).

Security, and in particular theft and misuse of information, as well as privacy issues, are also key matters undertaken by various government agencies and consumer organizations (European Commission, 2021; OECD, 2016).

The increasing digitization of economic activity and the development of data-driven and IoT business models are raising new security concerns (Tawalbeh et al., 2020). Protection of digital data and internet security should be a shared responsibility.

The provisions on consumer protection also overlap with public policies on national security, data privacy, law enforcement, and data flow and ownership (Ferracane, 2017; Ciuriak, 2018).

Despite these actions, a decline in trust among all stakeholders can be observed. Consumers begin to lose confidence in the way organisations and governments use data about them, and organizations lose confidence in their ability to secure data and use it to value creation (UMCTAD, 2016).

3. Research method and results

The survey was addressed to people who use the Internet and meet the connectivity condition. The study encompassed 1002 adult Internet users from Poland to achieve statistically significant results. The CAWI method was used. The data collection stage was done by Kantar Polska S.A. The sample is representative of Polish society. Respondents were divided into two main groups: “technologically advanced users” and “the rest”. The differentiation was made on the basis of one of the questions. The respondents assigned to the advanced users’ group replied "I rather agree" or "I strongly agree" to the following statements:

1. I am interested in technological news, I try to keep up to date.
2. I am one of the first among my friends and family to test new solutions (3) I handle most of my everyday matters (financial management, ticket purchases, fees, shopping) online.

This group included 266 respondents.

Two statistical tests were employed to verify the study’s research hypotheses. A Chi-square test and test comparing two independent population proportions were used to verify the assumed hypotheses. The second test aimed to verify the hypotheses concerning the value of proportions in the general population.

The readiness of this group to test and use technological solutions in everyday activities was the basis for the formulation of the first research hypothesis:

H1: There are differences in the use of the Internet by technologically advanced users and other users.

The test statistic (Pearson Chi-Square = 90,19, p-value = 0,00, df = 16) shows that there is a significant difference in the distribution of the use of technology between technologically advanced users and other users. Association between analyzed variables, measured by Cramer's V (0,1032) is moderate.

The results comparing answers in both groups are presented in the table below (Table I). Technologies used both for private and professional purposes are listed in the table. Due to the fact that it was the first study of this type, it was decided not to categorize a given type of technology into work, home, private life, etc.

Table 1.
The use of technology by technologically advanced and other Internet users

Technologies	Technologically advanced	Rest of respondents	u
Online shopping (in online stores, auction platforms, e.g. Allegro, OLX)	86%	84%	0,773
Use of electronic mail (e-mail)	84%	85%	- 0,39
Use of internet / mobile banking (financial management via a computer or smartphone)	80%	79%	0,34
Use of messaging services (e.g. Facebook Messenger, WhatsApp, Skype, Zoom) for private purposes.	82%	77%	1,70
Use of social media (Facebook, Twitter, Instagram, Pinterest)	83%	75%	2,66*
Geolocation, the use of navigation, maps on the phone	71%	66%	1,49
Use of messaging services (e.g. Facebook Messenger, WhatsApp, Skype, Zoom) for professional purposes.	64%	54%	2,82**
Cloud data storage and sharing (OneDrive, Google Drive, DropBox, iCloud etc.)	67%	48%	5,32**
SMS micropayments e.g. sent for charity	52%	40%	3,39**
Biometric security (fingerprints, facial recognition)	57%	36%	5,96**
Intelligent health monitoring devices (smartwatches, fitness bands, heart rate monitors, blood pressure monitors, glucometers, scales)	51%	34%	4,88**
Online purchase of insurance	47%	31%	4,68**
Online medical advice, telemedicine	42%	28%	4,21**
Communication with chatbots/machines serving clients on the chat via instant messaging.	43%	25%	5,50**
Smart home - control of house/apartment elements using remote channels, e.g. via a smartphone	28%	12%	6,06**
Virtual or augmented reality (e.g. VR goggles)	26%	11%	5,87**
Use of drones	15%	9%	2,73**

u – Test for two structure indicators.
* - statistically significant at the level of significance of 0,05.
** - statistically significant at the level of significance 0,01.

Source: Own elaboration based on study results.

Another key point of technology use that has been discussed for several years is its ethical dimension. The importance of digital ethics increases. Hypothesis 2 was based on the assumption that there is a difference in the approach to ethical issues among the group of respondents who use various technological solutions in their daily activities.

H2: There are differences in the approach to the ethical aspects of new technologies in the group of technologically advanced users and the rest of the respondents.

The test statistic (Pearson Chi-Square = 4,04, p-value = 0,67, df = 6) shows that there is no significant difference in the approach to the ethical aspects of new technologies between technologically advanced users and other users. In order to determine a difference in the approach to each ethical aspect questions in the estimated proportions reflects a difference in the population proportions, and respondents' statements and test statistic were presented (Table II).

Table 2.
Do you agree or not with the following statements (% of respondents who answered yes to the following statements)

	Technologically advanced	**Rest of respondents**	**u**
I am concerned about the growing phenomenon of 'fake news' - the deliberate duplication of false information	80%	65%	4,53**
I am concerned that companies have my personal data or data about my behaviour on the Internet, e.g. the history of pages viewed	72%	65%	2,08*
I am concerned about the lack of control over the collection and storage of data about me by companies operating on the Internet	73%	62%	3,22**
I wonder to what extent I have real control over the content I receive on the Internet	73%	58%	4,32**
There are situations when I do not know why a given advertisement reaches me on the Internet or over the phone	60%	55%	1,41
I don't know how to reduce the amount of advertising and unsolicited information I receive.	48%	50%	-0,56
Companies on the Internet divide their customers into 'better' and 'worse' and they approach each group differently	55%	36%	5,40**
It seems to me that the scope of information I have contact with, e.g. in the media, is inappropriate for my interests.	48%	30%	5,28**
It seems to me that the scope of information with which I have contact, e.g. in the media, is not appropriate to my values and beliefs	43%	29%	4,17**

u – Test for two structure indicators
* - statistically significant at the level of significance of 0,05
** - statistically significant at the level of significance 0,01

Source: Own elaboration based on study results.

Table III completes and develops the thread outlined in the previous question about the context of data appearance, data access, processing and aggregation. The respondents could refer to such topics as: rules of using data, the risk of information manipulation, but also the development of technologies that are still not very common. People who consider themselves technological advanced generally have more concerns about the use of digital technologies except "the development of wearables technology".

The test statistic (Pearson Chi-Square = 15,49, p-value = 0,16, df = 11) shows that there is no significant difference in approach to the ethical aspects of new technologies between technologically advanced users and other users.

Table 3.
Do you agree or not with the following statements (% of respondents who answered yes to the following statements)

	Technologically advanced	**Rest of respondents**	**u**
Information manipulation on the Internet, no possibility of selecting real information	82%	69%	4,07**
Collecting and connecting with an individual data on Internet activity and data trading	75%	63%	3,55**
Privacy restrictions related to the development of monitoring	72%	58%	4,03**
Showing ads with inappropriate content for the recipient	68%	58%	2,86**
Using data relating to internet activity to advertise products and services	68%	57%	3,14**
The growing amount of information reaching people, information overload	64%	52%	3,37**
Unclear rules of operation of financial systems	63%	48%	4,20**
Chips that extend human capabilities	63%	55%	2,26*
Accurate life expectancy determination based on continuous health monitoring	58%	45%	3,64**
Development of wearables technology	52%	45%	1,96
The development of artificial intelligence (AI / SI)	47%	37%	2,86**
Introduction of autonomous cars	46%	32%	4,08**

u – Test for two structure indicators
* - statistically significant at the level of significance of 0,05
** - statistically significant at the level of significance 0,01

Source: Own elaboration based on study results.

The issue of autonomy and decision-making undoubtedly raises concerns. Technology is designed to facilitate the implementation of tasks, not to take control of our decision-making or cause external organizations to obtain data that we do not want to disclose. Table IV shows which elements related to these dimensions are of concern among two different groups of respondents. The test statistic (Pearson Chi-Square = 4,04, p-value = 0,67, df = 6) shows that there is no significant difference in approach to the ethical aspects of new technologies between technologically advanced users and other users.

Table 4.
Autonomy and privacy concerns (% of respondents agree with the statement)

	Technologically advanced	Rest of respondents	u
I am afraid that I will be under surveillance (without my knowledge and / or consent)	74%	66%	2,40*
I'm afraid that thanks to technology, people will know more about me than they want	75%	65%	2,99**
I am concerned that a third party will take control of my phone/email/bank account	70%	66%	1,19
I am afraid that knowing myself will become the basis for manipulating my decisions/opinions/behaviours	72%	57%	4,30**
I am afraid that an improperly designed system will discriminate me	62%	47%	4,19**
I am afraid that a third party will take control of my smart home appliances / smart home, car	55%	47%	2,24*
I am afraid that the robot will take my job in the future	48%	39%	2,55*

u – Test for two structure indicators
* - statistically significant at the level of significance of 0,05
** - statistically significant at the level of significance 0,01

Source: Own elaboration based on study results.

The last hypothesis concerned the scope of responsibility that technologically advanced users take for the use of technology. The aim was to check whether people who follow technological news and use technology to ease their daily tasks have a sense of responsibility for the information provided and data protection.

H3: Technologically advanced users take more responsibility for the use of technology comparing the rest of the respondents. The research results are presented in table V. Test statistic (Pearson Chi-Square = 19,56, p-value = 0,00, df = 3) shows that there is a significant difference in responsibility for the use of technology between technologically advanced users and other users. Association between analyzed variables, measured by Cramer's V (0,0885) is weak.

Table 5.
Perception of responsibility for activities related to the online presence (% answers of respondents who agreed with the statements)

	Technologically advanced	Rest of respondents	u
As technology advances, the boundaries of what is ethical are shifting	92%	77%	5,34**
All unethical activities are unacceptable	83%	71%	3,83**
As technology develops, greater emphasis should be placed on online threats and data privacy	72%	58%	4,03**
I can agree to some concessions regarding the security of my data if I am offered better terms, e.g. a contract or purchase	51%	25%	7,80**

u – Test for two structure indicators
* - statistically significant at the level of significance of 0,05
** - statistically significant at the level of significance 0,01

Source: Own elaboration based on study results.

The verification of research hypotheses revealed that there are statistically significant differences between technologically advanced and other users in the researched sample and the general population. Research hypotheses 1 and 3 were verified positively. The second hypothesis was not verified positively for the researched sample but there are some differences on the level of the general population for particular statements measuring the approach to the ethical aspects of new technologies. Additionally, thanks to the additional statistical verification it was revealed that the differences between two groups of Internet users are statistically significant in the general population.

4. Discussion

It seems to be particularly important to recognize the factors which may prevent technology acceptance or make it less beneficial for the users. The "technological advanced" group is characterized by high awareness of the risks related to the transfer of data or the use of technologies to facilitate everyday functioning.

Users' fears stem from the feeling of lack of control over the process of obtaining information about them. For designers and technology suppliers, the area of education should become a necessity. Users who understand technology will be able to use it properly. This is especially important for less advanced users. The role of education was also indicated as important by other authors (Kim et al., 2017).

Automation and robotisation are essential factors in developing the digital economy. Enterprises implementing such technologies should also address the processes of information in their projects. Familiarizing with technology and building a sense of security as well as showing possible alternatives in those areas where robotisation may dominate the performance of certain tasks seem to be the priority.

Technologically advanced users have more concerns about losing control of what happens when the information is disclosed to companies. For companies, it is a great challenge not only because of law but also ethical issues (Buchanan et al., 2007).

The topic highlighted by the surveyed group is data manipulation and information bubble. It is a significant factor that influences the social development of a technologized society. In this dimension, the ethics of business activities becomes crucial. Not only technologies should be devoid of features that determine discriminatorily, excluding or limiting access to complete information and freedom of decision, but also the information itself made available on the web. This includes advertising, press releases, reports and other types of communications received by people using the Internet. This support the other studies about the potential risks of online discrimination (Speicher et al., 2018). With the limitation of autonomy, apart from manipulating the content, there is also a problem of a loss of decision-making.

5. Limitations and conclusions

There are some limitations to this study. The survey answers were collected based on one country so it would be interesting to compare results with other countries located at different positions in the DESI index. The study is broad and does not specify the concrete areas of the Digital Economy and was oriented on the broad context of activities undertaken online. The study did not analyse the factors influencing the potential paradox that arises between the awareness of threats and the readiness to disclose data that may favour the use of unethical behaviour and other abuses by enterprises. Future research may go deeper to understand the mechanisms of ethical and security concerns in specific contexts and situations.

Ethics and a sense of security are crucial factors for designing and developing new technologies. These elements should be implemented on several levels. Transparent, data-driven and factual presentation of information in communication processes will satisfy the need to have access to reliable information about the technology. Technological ethics in which designed solution is free from violations of human rights. Ethics of the technology provider is understood as ethical behaviour in relations with users, including the process of establishing formal relations through contracts. The ethics of the technology provider also covers the way how the obtained data is used, combined and processed. The development of the digital economy requires sustained efforts on the part of businesses as well as authorities and users.

References

1. Acquisti, A., John, L.K., Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42(2),* pp. 249-274. doi:10.1086/671754.
2. Ahmed, U., Chander, A. (2015). *Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows*. E15 Initiative. Geneva, Switzerland: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum.
3. Algorithm Watch (2019). *The AI Ethics Guidelines Global Inventory*. Available at: https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/, 20.10.2020.
4. Allen, A.L. (2019). Debating ethics and digital life. *European Data Protection Law Review, 5(1),* pp. 7-12. DOI: https://doi.org/10.21552/edpl/2019/1/4.
5. Ally, M., Toleman, M. (2005). *A framework for assessing payment security mechanisms and security information on e-commerce web sites*. Paper presented at the 9th Pacific Asia Conference on Information Systems (PACIS), Bangkok, Thailand. http://aisel.aisnet.org/pacis2005, 20.10.2020.

6. Amoroso, D.L., Hunsinger, S. (2009). Measuring the Acceptance of Internet Technology by Consumers. *International Journal of E-Adoption*, *1(3),* pp. 48-81. doi:10.4018/jea.2009092903.
7. Ariffin, S.K., Mohan, T., Goh, Y.-N. (2018). Influence of consumers' perceived risk on consumers' online purchase intention. *Journal of Research in Interactive Marketing*, *12(3),* pp. 309-327. doi:10.1108/jrim-11-2017-0100.
8. Belanger, F., Hiller, J.S., Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11(3-4),* pp. 245-270. doi:10.1016/s0963-8687(02)00018-5.
9. Boone, T., Ganeshan, R., Jain, A., Sanders, N.R. (2019). Forecasting sales in the supply chain: Consumer analytics in the big data era. *International Journal of Forecasting*, *35(1),* pp. 170-180. doi:10.1016/j.ijforecast.2018.09.003.
10. Buchanan, T., Paine, C., Joinson, A.N., Reips, U.-D. (2006). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58(2),* pp. 157-165. doi:10.1002/asi.20459.
11. Buchanan, T., Paine, C., Joinson, A.N., Reips, U. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58(2),* pp. 157-165. https://doi.org/10.1002/asi.20459.
12. Chang, H.H., Chen, S.W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management*, *46(7),* pp. 411-417. doi:10.1016/j.im.2009.08.002.
13. Chellappa, R.K., Pavlou, P.A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15(5/6),* pp. 358-368. doi:10.1108/09576050210447046.
14. CIGI-Ipsos (2019). Global Survey on Internet Security & Trust, Social Media, Fake News & Algorithms. Centre for International Governance Innovation. Available from: https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/, 20.07.2021.
15. Ciuriak, D. (2018). Digital Trade: Is Data Treaty-Ready? *CIGI Paper, NO. 162.* Waterloo: Center for International Governance Innovation. *SSRN Electronic Journal*. doi:10.2139/ssrn.3110785.
16. Couldry, N., Mejias, U.A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, *20(4),* pp. 336-349. doi:10.1177/1527476418796632.
17. Digital Economy and Society Index for Poland, https://digital-strategy.ec.europa.eu/en/policies/desi-poland, February 2022.

18. Digital Economy and Society Index, https://digital-strategy.ec.europa.eu/en/policies/desi, February 2022.
19. European Commission (2021b). *Open Data Maturity.* EU.
20. European Commission (2019). *Liability for Artificial Intelligence and other emerging digital technologies*, EU.
21. European Commission (2020a). *Shaping Europe's Digital Future*. EU.
22. European Commission (2020b). *White Paper On Artificial Intelligence - A European approach to excellence and trust.* EU.
23. European Commission (2021a). *The Digital Economy and Society Index – Poland.* EU.
24. European Commission: Factsheet (November 2020). *New Consumer Agenda, New Consumer Program. Measures to protect European consumers 2020-2025*. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2069, 20.07.2021.
25. European Union Agency For Fundamental Rights (2020). *Artificial Intelligence and fundamental rights*. EU.
26. Ferracane, M. (2017). Restrictions on Cross-Border Data Flows: A Taxonomy. *SSRN Electronic Journal*. doi:10.2139/ssrn.3089956.
27. Floridi, L. (2019). Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical. *Philosophy & Technology*, *32(2),* pp. 185-193. doi:10.1007/s13347-019-00354-x.
28. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, *28(4),* pp. 689-707. doi:10.1007/s11023-018-9482-5.
29. Fortes, N., Rita, P., Pagani, M. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *International Journal of Internet Marketing and Advertising*, *11(4),* p. 307. doi:10.1504/ijima.2017.087269.
30. Goyens, M. (2019). Effective Consumer Protection Frameworks in a Global and Digital World. *Journal of Consumer Policy*. doi:10.1007/s10603-019-09423-2.
31. Green, B.P. (2018). Ethical reflections on Artificial Intelligence. *Scientia et Fides*, *6(2),* pp. 9-31. DOI: https ://doi.org/10.12775 /setf.2018.015.
32. Gupta. M.P., Dubey, A. (2016). E-commerce-study of privacy, trust and security from consumer's perspective. *International Journal of Computer Science and Mobile Computing, 5(6).* pp. 224-232.
33. Gurung, A., Raja, M.K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security*, *24(4),* pp. 348-371. doi:10.1108/ics-05-2015-0020.
34. GUS (2020). *Information society in Poland in 2020.* Warszawa- Szczecin.
35. Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J.H., Jonker, M., de Ruiter, J., Sperotto, A., van Rijswijk-Deij, R., Moura, G.C.M., Pras, A., de Laat, C. (2020).

A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management*, *28(4),* pp. 882-922. doi:10.1007/s10922-020-09564-7.

36. Hofacker, C.F., Malthouse, E.C., Sultan, F. (2016). Big Data and consumer behavior: imminent opportunities. *Journal of Consumer Marketing*, *33(2),* pp. 89-97. doi:10.1108/jcm-04-2015-1399.
37. Hong, W., Thong, J.Y.L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37(1),* pp. 275-298. Available at: https://www.jstor.org/stable/43825946.
38. Ipsos Global Trends. Data dilemmas (2020). Ipsos Global Trends Survey. https://www.ipsosglobaltrends.com/2020/02/data-dilemmas/, 19.07.2021.
39. Jobin, A., Ienca, M., Vayena, E. (2019). Artificial Intelligence: The global landscape of ethics guidelines. *Health Ethics & Policy Lab.* Zurich, Preprint version. https://arxiv.org/pdf/1906.11668, 22.02.2021.
40. Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice*, *11(11),* p.jpw150. doi:10.1093/jiplp/jpw150.
41. Kim, B.-H., Kim, K.-C., Hong, S.-E., Oh, S.-Y. (2016). Development of cyber information security education and training system. *Multimedia Tools and Applications*, *76(4),* pp. 6051-6064. doi:10.1007/s11042-016-3495-y.
42. Kim, C., Tao, W., Shin, N., Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, *9(1),* pp. 84-95. doi:10.1016/j.elerap.2009.04.014.
43. Kirillova, E.A., Shergunova, E.A., Ustinovich, E.S., Nadezhin, N.N., Sitdikova, L.B. (2016). The Principles of the Consumer Right Protection in Electronic Trade: A Comparative Law Analysis. *International Journal of Economics and Financial Issues*, 6(2S), pp. 117-122. Available at: https://www.econjournals.com/index.php/ijefi/article/view/2540, 7.09.2022.
44. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, pp. 122-134. doi:10.1016/j.cose.2015.07.002.
45. KPRM (2021). *Polityka dla rozwoju sztucznej inteligencji w Polsce od 2020 roku.* Uchwała nr 96 Rady Ministrów, Dz.U. 12.01.2021, poz. 23.
46. Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38(11),* pp. 1134-1145. doi:10.1016/j.telpol.2014.10.002.
47. Linck, K., Pousttchi, K., Wiedemann, D.G. (2006). *Security Issues in Mobile Payment from the Customer Viewpoint,* pp. 1-11. 14th European Conference on Information Systems (ECIS), Göteborg/Schweden, https://mpra.ub.uni-muenchen.de/id/eprint/2923.
48. Martin, K.D. Murphy, P.E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45(2),* pp. 135-155. DOI 10.1007/s11747-016-0495-4.

49. Mayer-Schönberger, V., Ramge, T. (2018). A Big Choice for Big Tech. Share Data or Suffer the Consequences. *Foreign Affairs, 97(5),* pp. 48-54.
50. McDonald, A.D., Cranor, L.F. (2008). The cost of reading privacy policies. *Journal of Law and Policy for the Information Society, Vol. 4,* pp. 540-565.
51. McGeveran, W. (2018). The Duty of Data Security, 103 MINN. L. REV. pp. 1135 103, https://heinonline.org/HOL/LandingPage?handle=hein.journals/mnlr103&div=33&id=&page=.
52. McKinsey & Company (2020). *Digital Challengers in the next normal. Central and Eastern Europe on a path to digitally-led growth*.
53. Meek, T., Barham, H., Beltaif, N., Kaadoor, A., Akhter, T. (2016). *Managing the ethical and risk implications of rapid advances in artificial intelligence: A literature review*. 2016 Portland International Conference on Management of Engineering and Technology (PICMET). doi:10.1109/picmet.2016.7806752.
54. Milne, G.R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing*, *19(1),* pp. 1-6. doi:10.1509/jppm.19.1.1.16934.
55. Milne, G.R., Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18(3),* pp. 15-29. doi:10.1002/dir.20009.
56. Miyazaki, A.D., Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing*, *19(1),* pp. 54-61. doi:10.1509/jppm.19.1.54.16942.
57. Miyazaki, A.D., Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, *35(1),* pp. 27-44. doi:10.1111/j.1745-6606.2001.tb00101.x.
58. Mosteller, J., Poddar, A. (2017). To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors. *Journal of Interactive Marketing*, *39*, pp. 27-38. doi:10.1016/j.intmar.2017.02.003.
59. Mukherjee, A., Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, *21(1),* pp. 5-15. doi:10.1108/02652320310457767.
60. OECD (2016). *Consumer protection in E-commerce: OECD recommendation*. OECD Publishing, https://doi.org/10.1787/9789264255258-en.
61. Oxborough, C., Cameron, E., Rao, A., Birchall, A., Townsend, A., Westermann, C. (2018). *Explainable AI: Driving business value through greater understanding*. PWC. https://www.pwc.co.uk/audit-assurance/assets/explainable-ai.pdf, 15.10.2020.

62. PAYBACK Poland (2021). *Polacy entuzjastami nowych technologii? - Opinion Poll.* https://brief.pl/polacy-entuzjastami-nowych-technologii-wyniki-payback-opinion-poll-badanie/, 19.07.2021.
63. PwC (2021). *A new image of the Polish consumer.* Global Consumer Insights Survey 2020.
64. Reidenberg, J.R., Russell, N.C., Callen, A.J., Qasir, S., Norton, T.B. (2015). Privacy harms and the effectiveness of the notice and choice framework. *Journal of Law and Policy for the Information Society,* Vol. 11(2), pp. 543-568, https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc11&div=19&id=&page=.
65. Reisdorf, B.C., Groselj, D. (2015). Internet (non-)use types and motivational access: Implications for digital inequalities research. *New Media & Society*, *19(8),* pp. 1157-1176. doi:10.1177/1461444815621539.
66. Reyna, A., Helberger, N., Borgesius, F.Z. (2017). The perfect match?a closer look at the relationship between eu consumer law and data protection law. *Common Market Law Review*, *54(5),* pp. 1427-1465. doi:10.54648/cola2017118.
67. Riquelme, P.I., Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets*, *24(2),* pp. 135-149. doi:10.1007/s12525-013-0145-3.
68. Royakkers, L., Timmer, J., Kool, L., van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, *20(2),* pp. 127-142. doi:10.1007/s10676-018-9452-x.
69. Salisbury, W.D., Pearson, R.A., Pearson, A.W., Miller, D.W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101(4),* pp. 165-177. doi:10.1108/02635570110390071.
70. Saltz, J.S., Dewar, N. (2019). Data science ethical considerations: a systematic literature review and proposed project framework. *Ethics and Information Technology*, *21*. doi:10.1007/s10676-019-09502-5.
71. Sheehan, K.B., Hoy, M.G. (2000). Dimensions of Privacy Concern among Online Consumers. *Journal of Public Policy & Marketing*, *19(1),* pp. 62-73. doi:10.1509/jppm.19.1.62.16949.
72. Smith, H.J., Milberg, S.J., Burke, S.J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20(2),* p. 167. doi:10.2307/249477.
73. Speicher, T., Ali, M., Venkatadri, G., Ribeiro, F.N., Arvanitakis, G., Benevenuto, F., Mislove, A. (2018). *Potential for discrimination in online targeted advertising. Conference on Fairness, Accountability and Transparency. PMLR*. pp. 5-19.
74. Stahl, B.C., Timmermans, J., Mittelstadt, B.D. (2016). The Ethics of Computing. *ACM Computing Surveys*, *48(4),* pp. 1-38. doi:10.1145/2871196.
75. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10(12),* p. 4102. doi:10.3390/app10124102.

76. Tsiakis, T., Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24(2),* pp. 105-108. doi:10.1016/j.cose.2005.02.001.
77. Uchwała Nr 196 RADY MINISTRÓW z dnia 28 grudnia 2020 r. w sprawie ustanowienia *Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020*.
78. United Nations Conference on Trade and Development (2016). Data Protection Regulations and International Data Flows: Implications for Trade and Development. Geneva Switzerland: UNCTAD. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf, 15.07.2021.
79. Xu, H., Teo, H.-H., Tan, B.C.Y., Agarwal, R. (2012). Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, *23(4),* pp. 1342-1363. doi:10.1287/isre.1120.0416.
80. Yang, Z., Jun, M. (1970). Consumer Perception of E-Service Quality: From Internet Purchaser and Non-Purchaser Perspectives. *Journal of Business Strategies*, *25(2),* pp. 59-84. doi:10.54155/jbs.25.2.59-84.