ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Privacy on the Internet: An Empirical Study of Poles' Attitudes

Received: 03.11.2022
Accepted: 12.12.2022
Published: 15.12.2022

Daniel Mider Faculty of Political Science and International Studies, University of Warsaw, Poland, ORCID: 0000-0003-2223-5997

Abstract

The value system of Poles in terms of the phenomenon of privacy on the Internet was analysed. The following aspects were taken into account: privacy on the Internet as a moral value, privacy on the Internet as a subject of legal regulations (current or future) and actual actions taken by users to protect privacy. The differentiation of Polish society in terms of the three above-mentioned areas was also examined. Results were obtained on the basis of a quantitative empirical study conducted on a representative sample (N=1001) of adult Poles. The method of computer assisted telephone interviews (CATI) was used. Descriptive statistics and selected inductive statistics were used in the analyses. Intra-group differentiation was investigated using a method called two-step cluster analysis. Poles have low technical competences in the field of Internet privacy protection. This value is appreciated; however, it rarely translates into active protection of one's own identity and information. A strong polarization of Poles' attitudes towards the requirement to disclose their identity on the Internet was identified, as well as ensuring access to any user information by law enforcement agencies. Poles are willing to accept legal regulations preventing their profiling. We note a moderately strong negative attitude towards state institutions as a factor limiting privacy on the Internet and a significantly lower (but still negative) attitude towards Internet service providers. Poles differ in terms of attitudes towards privacy on the Internet (IT competences, age, education, gender, socioeconomic status and size of the place of residence).

Keywords

online behavior, online freedom, privacy paradox, privacy perceptions

1. Introduction

In this article, we analysed the value system of Poles in terms of the phenomenon of privacy on the Internet. The following aspects were considered: privacy on the Internet as a moral value, privacy on the Internet as a subject of legal regulations (current or future), and actual actions taken by users to protect privacy. The differentiation of Polish society in terms of the three above-mentioned areas was also examined, creating its segmentation.

Cite this article as:
D. Mider, "Privacy on the Internet: An Empirical Study of Poles' Attitudes," ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1459

Corresponding author:
Daniel Mider, Faculty of Political Science and International Studies, University of Warsaw, Poland, ORCID: 0000-0003-2223-5997; E-mail: d.mider@uw.edu.pl

We are constantly witnessing data privacy violations of ordinary Internet users. These threats are multi-vector. Cybercriminals are an obvious source of threats, although awareness of the scale of these threats is low among ordinary users. As an exemplification, it can be mentioned that the leaked databases, available to anyone interested who is willing to pay, often have over 20 billion records (i.e., user login and password pairs, directly or in an encrypted form) [1]. Another vector of threats is Big Tech. Global social media operators collect data excessively and this data is used – directly or indirectly – to manipulate social groups, as demonstrated by whistleblowers Christopher Wylie and Brittany Kaiser, former employees of Cambridge Analytica. The non-obvious entity violating user data is national states that implement surveillance programs which collect data in an oppressive manner. The best-known example is the US National Security Agency's surveillance system, code-named PRISM, which was disclosed by Edward Snowden [2]. In the study entitled "The Future of Privacy" conducted by the Pew Research Center in 2014, over 2,500 experts expressed a pessimistic view that privacy on the Internet would disappear by 2025 [3].

In the context of the above-mentioned facts, the research problem was defined by posing the following research questions:

- What is the level of Poles' awareness of violations of their privacy on the Internet?
- What are the predictors of differences in attitudes towards online privacy: sociographic, psychographic, or behavioural characteristics?
- What are their attitudes towards possible legal regulations regarding restrictions or extensions of privacy protection?
- Do they practically protect their privacy on the Internet and to what extent?
- Do they want their privacy to be protected by themselves, or do they prefer
  the obligation to protect to be transferred to another entity?

The above-mentioned problems are listed in the area of interest of numerous researchers. These considerations omit numerous legal sociological and IT references, focusing primarily on the current empirical findings in the field of attitudes towards the phenomenon of privacy. An important field of interest is the awareness of privacy risks and ways of understanding this concept in the context of functioning on the Internet. Above all, the speed of changing technology is emphasized, and as a result, it is difficult to precisely define the concept of privacy. According to some researchers, this concept is almost impossible to define [4]. Research on privacy shows a low level of awareness of this phenomenon by societies. On the other hand, regardless of the superficial understanding of privacy issues, it is widely appreciated. The respondents blame the violation of privacy, while understanding the value of sharing information. However, they do not want the sharing of information against their will and intentions [5]. To date, the most comprehensive and cited privacy survey was conducted by an American public opinion poll Pew Research Center [6]. A valuable and interesting empirical study was also the EMC Privacy Index, which over time transformed into the Dell Technologies Global Data Protection Index [7]. The latter, however, has evolved towards cybersecurity issues (e.g., threats such as phishing or ransomware). Comprehensive research of privacy on the Internet has not been carried out in Poland so far. This fact became the basis for undertaking the examination of this issue. Research on the broadly understood privacy appeared in Poland sporadically and referred to the degree of measurement to which various values are held. Two such studies have recently been carried out: relating to the extent to which Poles value and are willing to protect their data [8], and a study by the Center for Studies on Democracy of the SWPS University on the value of privacy and freedom on the Internet [9]. However, the raw data was not released - the research is available through press articles and in the form of short reports.

Academic studies of socio-demographics which correlates attitudes towards privacy are commonly studied. First of all, researchers focus on the gender category [10–12]. Conclusions were also formulated in relation to the age of the respondents, indicating groups particularly sensitive to threats of privacy: adolescents [13, 14] and seniors [15].

Researchers' efforts also focus on the phenomenon of the correlation between awareness of threats to privacy and the lack of importance; or even neglect of its protection by users. This phenomenon has been referred to as the privacy paradox [16–18]. This particularly applies to the use of smartphones [19, 20]. It has been shown that online behaviour on the Internet often resembles the behaviour of users with low IT competences [21].

The interest in the issue of privacy in the academic and political environment, especially in the perspective of the above-mentioned threats, has been attracting attention since the 19th century. The cornerstone of the modern debate on privacy is an article by American lawyers Samuel D. Warren and Louis D. Brandeis [22]. The right to privacy is placed among the first-generation human rights and is subject to universal regulation at the level of international and national legislation (Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, Convention for the Protection of Human Rights and Fundamental Freedoms). It is also worth adding that one of the earliest topics related to the ethics of new technologies that aroused public interest was privacy. In the mid-1960s, the US government created large databases containing information about citizens (these were census data, tax records, military service records, and social records). It was then that the first public debate on limiting the government's appetite for information about citizens was initiated. Another discussion began in the 1980s as a result of the development of information technology. Continuing that a social movement was formed, the doctrinal basis of which was the belief that the right to privacy was defective by state institutions. It was argued that states have violated the requirement to care for this value and in this respect pose the greatest threat to the citizen. Moving forward the term Privacy Enhancing Technologies (PET) was created, meaning such technical solutions that provide users with complete privacy and exclusive control over the data they create and send. The perceived threats have now led to the development of the concept of individual digital self-determination. This concept assumes that the interactions in cyberspace, especially by large entities: should be transparent, data should not be excessively collected, and the user should not be manipulated on the basis of algorithms and information unintentionally left in cyberspace (metadata). In addition, everyone should independently manage information about themselves and decide who and under what conditions has the right to access it. Currently, it is postulated that these freedoms should be introduced into the Charter of Fundamental Rights of the European Union.

For the purposes of this text: the concept of privacy and the concept of anonymity, and those closely related to it, have been defined (bearing in mind that these terms are considered widely in academic publications) [23]. Privacy is understood as a situation where everyone knows our identity, but no one knows what we are doing, and therefore what data we exchange. On the other hand, anonymity is a situation where no one knows who we are (so they do not know, for example, our name and surname, or any other information about us that can reveal who we are); however, everyone can see our actions. It is emphasized that the two concepts connect with each other, because in numerous online activities the possibility of maintaining privacy without anonymity is difficult or even impossible to implement [24].

2. Methods

The research questions were answered during a quantitative empirical study conducted by the Association of Political Science Graduates affiliated with the

Faculty of Political Science and International Studies at the University of Warsaw. The research was financed by the Justice Fund and administered by the Minister of Justice. The measurement entitled *Premises of a sense of security. Privacy, anonymity, freedom, and security* were conducted from December 1st to 23rd, 2021 using the computer-assisted telephone interview method as a representative (gender, age, size of the place of residence, and education) sample of N=1001 adult (18+) Poles. The measurement, fulfilling the requirements of the so-called statistical representativeness, can be generalized from the sample to the population of adult Poles. The maximum standard error of the estimation was ±3.1%.

The measurement was carried out using the Computer Aided Telephone Interviews (CATI) technique. This technique has been considered better than classic standardized face-to-face interviews (Paper and Pencil Interviews, PAPI) and online surveys (Computer Assisted Web Interviews, CAWI). In relation to the above-mentioned techniques, CATI has numerous methodological, psychological, interactional, organizational, and technical advantages which made it a useful tool for this project. As regards to the methodology, it involves a higher accessibility of respondents and a higher availability of the sampling frame (as compared to other methods) corresponding to general population. In terms of the psychological and interactional aspect, the comfort of interaction between the interviewer and the respondent is significantly greater. Communication over the phone distinctly increases the sense of anonymity for the respondent, which translates into respondents' feeling more at ease about expressing their views on difficult or sensitive issues. In terms of the technical and organizational aspect, an important feature of telephone interviews is the high level of control over the research process. This concerns both the human factor (interviewers and respondents), as well as the collected data. Also, the use of computer programmes and telephone contact significantly decrease the financial and organizational costs necessary to carry out the research. As a result, we achieve a higher response rate as compared to other research methods, higher quality of data which are precise and accurate, and a low level of errors, as well as reliability and accuracy.

A *sine qua non* condition of generalization of the results from the sample to the studied population is sampling (i.e., simple random sampling) according to the standards, and its sufficient size. Sampling will be made with the use of the method ensuring the randomness of sampling, developed as part of US state methodology of quantitative research (and widely adopted in research practice). The procedure was developed by Warren Mitofsky and Joseph Wakesberg. It is referred to in research practice as Random Digit Dialling (RDD) [25], and among researchers using computer-assisted telephone interviews it is considered an optimal and classic method [26].

The scope of the research procedure carried out included the assessment of attitudes towards the phenomenon of privacy in the following three aspects: moral, legal, and behavioural.

The moral aspect of attitudes towards privacy on the Internet. It is understood as the ethical limits of protecting and concealing one's identity on the Internet, set from the perspective of ordinary users, i.e., the weakest entities. In order to test this aspect, the following three questionnaires were selected from the research tool:

- M1. Edward Snowden is a former employee of the American intelligence (CIA) who in 2013 disclosed classified information regarding numerous global surveillance programs of the USA, undertaken by the country in cooperation with companies and some European countries. How do you evaluate such a phenomenon of mass surveillance by states on the Internet?

It was a closed, one-answer question. The respondent could indicate one of the following five answers: I strongly support, I rather support, I rather consider it unacceptable, I consider it completely unacceptable, and I have no opinion on this subject (the

last item was not read by the interviewer). Such a scale was chosen due to the possibility of treating the variable as ordinal and, as a result, calculating such statistics as the mean or standard deviation. The next two questions used as indicators of the moral aspect were as follows:

- M2. Profiling and tracking us online by service providers is simply the price we should pay for our convenience.
- M3. Anyone who wants to be anonymous on the Internet is either a cybercriminal or has bad intentions.

Questions M2 and M3 were closed-ended single-answer questions. The respondent could choose from the following responses: strongly disagree, rather disagree, rather agree, strongly agree.

Legal aspect of attitudes towards privacy on the Internet. Views on support for legal compulsion to disclose one's identity in all online interactions, the possibility of deanonymising and decrypting any private information online by law enforcement, and the legal regulation of user profiling by content providers on the Internet were examined. The following questions were asked:

- L1. Law enforcement authorities should, in important situations, be able to access any of our information on telephones, computers or the Internet, no matter how secure it is.
- L2. Profiling and tracking by service providers on the internet should be prohibited by law.
- L3. Everyone on the Internet should use in all interactions their first and last name, and this should be prescribed by law.
- L4a. The current legal provisions ensure adequate protection of people's privacy in their online activities.
- L4b. The current provisions on the protection of personal data, and therefore, above all, the GDPR, ensure adequate protection of people's privacy in their online activities.

Questions L4a and L4b were a special case. The sample was divided into two parts (the savings were dictated by the research costs), respectively L4a obtained n=500, and L4b n=501 answers. As part of the moral and legal aspect, attitudes towards the institutions of the first sector; i.e., the state (questions M1 and L1), and the second sector; i.e., enterprises owning social media (questions M2 and L2), were also taken into account. In the Results part, the statements were reformulated so as to be able to present the respondents' answers in a homogenous manner (direction of variables).

Behavioural aspect of attitudes towards privacy on the Internet. In this aspect, it was examined which Internet protection measures are actually taken by the respondents. It strictly depends on IT competences. The following question was asked:

Please consider which of the following ways to protect information on the Internet are undertaken by you...

Protection of identity and sensitive information on the Internet is not easy, so the respondent could choose from the following list of indicators: B1. I delete documents/files that should not fall into the wrong hands. B2. I am using the browser in incognito mode. B3. I use aliases so that I cannot be traced back to my real name. B4. I delete cookies/delete browser history. B5. I use a temporary username or email. B6. I encrypt files/documents. B7. I use Virtual Private Networks (VPNs). B8. I exercised the so-called "right to be forgotten". B9. I use advanced anonymisation tools (e.g., The Onion Router – Tor, Invisible Internet Project – I2P, Linux TAILS, Linux Whonix, OTR communication encryption).

These were dichotomous, one-answer questions, for each of them the respondent could answer "yes" or "no". The security measures indicated in the questions measured the level of technical and IT advancement of the respondent, including also verifying activities that could be considered wrong, not contributing to the strengthening of privacy. Items B1 and B2 are among the counter-effective actions (myths, mistakes). B3, B4 are among the elementary, basic, and partially effective actions. Activities that can be described as intermediate are: B5, B6, B7. By contrast, advanced privacy measures include questions B8 and B9.

In order to indicate social, demographic, and psychographic predictors of individual attitudes; inductive statistics were used. Chi-square is used to determine whether or not there is a relationship between the variables. In order to find out how strong a relationship is (expressed in the range from zero to one), the Harald Kramer's statistics (V) and the Karl Pearson's contingency coefficient (C) were used.

Cluster Analysis. In the next step of the research procedure, it was checked what types of attitudes towards privacy on the Internet can be distinguished in Polish society. For this purpose, segmentation was made in order to discover the smaller structures of Polish society in terms of attitudes towards privacy.

The premise for the use of this statistical method is the necessity to reduce data resulting from the multi-faceted nature of privacy. Cluster analysis is a group of diverse statistical techniques used to classify cases into groups that are relatively homogeneous within themselves and heterogeneous among themselves. These groups are called clusters. Cluster analysis is the so-called unsupervised learning method – "without a teacher". This method is opposed to discriminant analysis (supervised classification). In unsupervised classification, the group structure does not have to be known *a priori*. This makes cluster analysis attractive as an exploratory tool. Cluster analysis detects structures in data without explaining why these structures exist. It is a method concurrent with human intuitive, everyday reasoning; which consists on grouping objects on the basis of similarity.

The method was invented in anthropology by Harold E. Driver and Alfred L. Kroeber in 1932 [27]; although the need for such a data mining technique was previously expressed by a Polish scientist: a supporter of statistical studies in anthropology, Jan Czekanowski [28]. It was popularized in science by Raymond B. Cattel using for the classification of personality traits [29]. The career of this method began in the 1960s and 1970s [30]. It has stimulated worldwide research into clustering methods and has initiated numerous publications on the subject; furthermore, it is widely used in various scientific disciplines [31].

Specifically, Two-Step Cluster analysis, was used. This analytical technique has particularly useful features: the ability to construct a model using both interval and nominal variables, and it allows the analysis of databases with large numbers of units of analysis. The input data finally selected for the segmentation performed were the 8 previously mentioned attitudes and behaviours of users: M1, M2, M3, L1, L2, L3 and B9. Additionally, the behavioural variable has been enabled: I use pseudonyms on the Internet so that they cannot be associated with my real name (possible answers "yes" or "no").

3. Results

The following analytical aspects are presented below: moral attitudes towards privacy on the Internet, attitudes towards legal regulations of this phenomenon (including the assessment of first and second sector institutions), and behavioural aspects of privacy protection by ordinary Internet users. The analytical part ends with segmentation: groups of Poles with different attitudes towards the phenomenon of privacy on the Internet have been identified.

3.1. Moral attitudes of Poles towards privacy on the Internet

Poles represent various attitudes towards the moral aspects of privacy on the Internet. More than three-quarters of them (82.1%) have a negative opinion of the mass surveillance system codenamed PRISM. On the other hand, only slightly more than a quarter of them (28.2%) consider it acceptable that companies providing services on the Internet collect excessive amounts of data from users. Opinions about the value of anonymity are divided. It should be emphasized that almost two-thirds of Poles (62.1%) recognize that anonymity on the Internet is a positive value and does not have to serve unethical or even criminal activities.

Table 1. Moral subaspects of attitudes towards privacy on the Internet

Statements	Response rate (in %)		
	Negative responses (negative attitudes towards privacy in cyberspace)	Undecided	Affirmative responses (positive attitudes towards privacy in cyberspace)
M1. Assessment of the phenomenon of mass surveillance by state entities (E.J. Snowden's case)	10.3	7.6	82.1
M2. User convenience is not enough to pay for online profiling and tracking by service providers	50.8	11.0	28.2
M3. Wanting to remain anonymous does not mean being a criminal or having malicious intent	29.7	8.2	62.1

The fact that more than half of service providers consider the activities of service providers on the Internet regarding data collection as ethical will undoubtedly hinder both the introduction of legal solutions limiting these providers that regulate this market, as well as the public discussions on this subject. The knowledge of Internet users about the unethical activities of corporations in the field of obtaining excessive amounts of data and the unethical methods of their use is still small.

Those located in the political center, center-left, or center-right express particularly strong opposition to government surveillance. In addition, people who do not have specific political views or who define themselves as off-scale left-right, and therefore probably people with mixed or libertarian views, are negative about state surveillance [χ^2 (24, N=1001) = 49.53; p≤0.01; V=0.131; C=0.22]. Predictors of positive attitudes towards privacy on the Internet are living in a medium or large city; i.e., over 50,000 inhabitants, but this value is on the border of statistical significance [χ^2 (21, N=1001) = 29.75; p≤0,1; V=0.12; C=0.20]. The subjective sense of economic status is a weak but statistically significant correlate of positive attitudes towards privacy on the Internet. It is non-linear; i.e., the opposition to government surveillance is higher among those who indicate average or moderately high income [χ^2 (15, N=1001) = 30.49; p≤0.01; V=0.11; C=0.18]. The lowest percentage of opposition to government surveillance was recorded among those who say they have insufficient money for even the cheapest food. Opposition to government surveillance is most strongly correlated with political attitudes identified on the basis of self-identification. The premise of negative attitudes towards collecting excessive amount of data by corporations is age. We can see a positive

correlation here, so, the younger the respondent, the more likely he is to accept corporate data collection [χ^2 (1, N=1001) = 10.51; p≤0.001; V=0.13; C=0.21].

The higher the age [χ^2 (1, N=1001) = 133.19; p≤0.001; V=0.24; C=0.38], the smaller the size of the place of residence [χ^2 (1, N=1001) = 5.63; p≤0.001; V=0.14; C=0.24], the less consent to moral justification of anonymity on the Internet. Moreover, we find the most positive attitudes towards anonymity on the Internet in people who describe themselves as right-wing [χ^2 (24, N=1001) = 51.64; p≤0.001; V=0.13; C=0.22].

3.2. Poles' attitudes towards legal regulations concerning privacy on the Internet

The results presented in Tab. 2. reveal the polarization of views regarding the regulation of privacy on the Internet; we observe a low level of libertarian attitudes. A moderate consensus is possible regarding the limitation of data collection by economic entities managing social media. In this case, the majority (60.0%) of the respondents would be willing to accept the legal limitation of this phenomenon.

Table 2. Legal subaspects of attitudes towards privacy on the Internet – changes to law

Statements	Response rate (in %)		
	Negative responses (negative attitudes towards privacy in cyberspace)	Undecided	Affirmative responses (positive attitudes towards privacy in cyberspace)
L1. Law enforcement authorities should not be able to access each of our information, even in important situations	46.8	9.4	46.6
L2. We must be legally prohibited from being tracked and profiled by service providers on the Internet	30.5	9.4	60.0
L3. The law should not require you to appear on the Internet only under your first and last name	44.0	6.7	49.3

A statistically significant and moderately strong correlation was observed between supporting the idea of legal regulations and the age of the respondents [L1. χ^2 (1, N=1001) = 9.48; p≤0.001; V=0.12; C=0.21; L2. χ^2 (1, N=1001) = 4.21; p≤0.05; V=0.16; C=0.30; L3. [χ^2 (1, N=1001) = 34.13; p≤0.001; V=0.17; C=0.32]. The phenomenon is especially intensified in the group over 55 years of age. Gender is a weak correlate of support for legal regulations, but it was treated as a phenomenon accompanying advanced age. The right-wing (62.7%) and people with unspecified political views (54.8%) would be particularly eager to grant powers to dispatching services [χ^2 (24, N=1001) = 77.61; p≤0.001; V=0.17; C=0.28]. The desire to limit the possibility of collecting data by corporations is particularly visible among people who define themselves as left-wing (64.3%), and also among the right-wing (40.5%) [χ^2 (32, N=1001) = 66.81; p≤0,001; V=0.13; C=0.25]. The remaining socio-demographic variables turned out to be statistically insignificant.

The General Data Protection Regulation (GDPR) is a legal act in force in the EU Member States. In Poland, it entered into force on May 25, 2018. Despite the

fact that it significantly protects privacy, it was initially viewed negatively, in particular by entrepreneurs. The sample was randomly divided into two parts: In the first group, question L4a (general assessment of privacy rights) was asked; in the second group, question L4b (direct reference to the provisions of the GDPR). Such a procedure was aimed at checking whether the current social attitude towards the GDPR has changed and whether the use of the trigger-word; i.e., "GDPR", is a reason for the occurrence of differences in the distribution of responses.

Table 3. Legal subaspects of attitudes towards privacy on the Internet – current law

	Response rate (in %)		
Statements	**The protection afforded by law is excessive**	**Undecided**	**The protection afforded by law is too weak**
L4a. The current legal provisions ensure adequate protection of people's privacy in their online activities	12.4	21.1	66.5
L4b. The current legal provisions on the protection of personal data, and therefore, above all, the GDPR, ensure adequate protection of people's privacy in their online activities	16.3	13.9	69.8

It was shown that the differences between the distribution of answers to both questions are statistically significant ($p \leq 0.05$), but the differences in the response rates are not large. In the case of the answer that the legal protection of privacy is too extensive, a difference of only slightly less than 4.0% was noted.

3.3. Behavioural aspects of privacy protection on the Internet

As shown in Tab. 4., the measures most often taken by Poles to protect privacy are not very effective or completely ineffective. Most of all, deleting cookies (which is done by more than half of the respondents (54.8%)), deleting documents or files so that they do not fall into the wrong hands (49.1%), and using web browsers in *incognito* mode (31.9%). Poles make little use of effective legal solutions, such as the right to be forgotten, or of effective IT solutions such as anonymisation tools, and thus ensuring almost complete security.

The analysis of sociodemographic variables showed that only one factor, that is age, correlates with the competences in the field of privacy protection on the Internet. The probability of taking counter-effective or only partially effective measures increases with age. This applies to deleting documents [χ^2 (5, N=1001) = 81.35; p≤0,001; V=0.29; C=0.28] and using the browser in *incognito* mode [χ^2 (5, N=1001) = 50.86; p≤0,001; V=0.22; C=0.21]. Education is an important predictor of undertaking most of the activities protecting privacy. The higher the education, the more actions are taken such as: document encryption [χ^2 (8, N=1001) = 53.14; p≤0,001; V=0.23; C=0.23], using a VPN [χ^2 (8, N=1001) = 37.85; p≤0,001; V=0.19; C=0.19], using web browser in *incognito* mode [χ^2 (8, N=1001) = 39.11; p≤0,001; V=0.20; C=0.19], and deleting cookie files [χ^2 (8, N=1001) = 57.56; p≤0,001; V=0.24; C=0.23]. Among other observations, it is also worth pointing out the gender variable – men have a statistically significantly higher tendency to use the browser in *incognito* mode [χ^2 (1, N=1001) = 12.40; p≤0,001; V=0.11; C=0.11] and using a VPN [χ^2 (1, N=1001) = 24.43; p≤0,001; V=0.16; C=0.16].

Table 4. Behavioural subaspects of attitudes towards privacy on the Internet

Statements	Response rate (in %)	
	Does not perform / does not use	Performs / uses
B1. Deleting documents/files so as not to fall into the wrong hands	50.9	49.1
B2. Using the browser in incognito mode	68.1	31.9
B3. Using aliases so not to be traced back to real name	72.5	27.5
B4. Delete cookies/Delete browser history	45.2	54.8
B5. Using a temporary username or email	78.6	21.4
B6. Encryption of files/documents	79.0	21.0
B7. Using a VPN	82.1	17.9
B8. Using the so-called "right to be forgotten"	99.4	0.6
B9. Using advanced anonymisation tools	90.4	9.6

3.4. Diversification of Poles' attitudes towards online privacy – segmentation

Variables were selected to create segmentation which enabled the most effective division of the surveyed Poles into clusters. The segmentation carried out using the cluster analysis method led to the identification of three types of attitudes towards privacy on the Internet. The obtained segmentation results turned out to be statistically satisfactory as measured by the coherence and distinctness measure (the so-called Silhouette coefficient). This coefficient indicates whether the division was made in such a way that observations are concentrated within the groups and separated between them. It takes values from -1 (very weak model) to 1 (perfect model). Fig. 1. shows the fit of the model graphically. The obtained result should be considered at least satisfactory, i.e. almost 0.4.

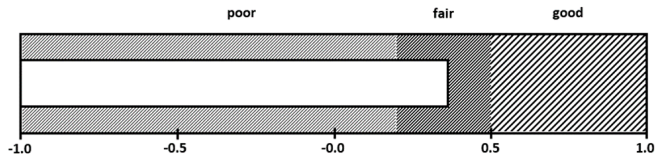

Figure 1. Silhouette measure of consistency and distinctiveness.

The most significant creative task in the procedure of segmentation is to give appropriate names for each of the segments identified. After analysing the characteristics, three descriptive names of the separate groups were created (in order of group size):

- Cluster 1. Skeptical or disappointed praetorians with low or medium IT competences (68.7%; n=668).
- Cluster 2. Moderate cyberlibertarians with medium or low IT competences (21.7%; n=217).
- Cluster 3. Moderate or extreme cyberlibertarians with high IT competences (9.6%; n=96).

The socio-demographic differences shown below are dominant; i.e., the characteristics are presented which make a specific group statistically significantly different from the average value for the population.

Cluster 1. Skeptical or disappointed praetorians with low or medium IT competences. They were called praetorians because they showed a significantly higher than the population average and lower than in other groups predilection towards legal restriction of privacy on the Internet. In particular, they advocate the need to verify with your name on the Internet and the possibility of law enforcement access to any data. Moreover, in the moral aspect, they mostly consider anonymity as being a cybercriminal or having malicious intent. The second premise for calling them praetorians was the fact that this group has the lowest intensity of negative attitudes towards state institutions. This group presents these attitudes as not too intense, and the differences between the other groups are small and in the above-mentioned aspects they do not exceed 15 percentage points. For this reason, the term skeptical or disappointed is used. This group generally equates their internet security with pseudonymisation. Nobody in this group uses advanced anonymisation tools. This group includes mainly women, they are people over 55, mostly inhabitants of rural areas and small towns up to 20,000 inhabitants. These people usually have secondary education, and consider their own material well-being to be moderate. From a psychographic point of view, we see an overrepresentation of practicing believers or non-practicing believers and representatives of the right-wing worldview.

Cluster 2. Moderate cyberlibertarians with medium or low IT competences. In this publication, cyberlibertarians are defined as those who oppose legal solutions to limit privacy on the Internet. The adjective "moderate" was used due to the fact that the differences, although statistically significant, are not so large in nominal terms. In this group, we see in the moral aspect, strong support for anonymity, stronger than in all other groups, and in the legal aspect, reluctance to impose the necessity to identify Internet users. In this group, we see the greatest consent to violating privacy by corporations. This consent is the greatest in comparison to the other groups and the average for the entire population. IT competences in this group are low, as in the first group, they consider pseudonymisation to be a sufficient way to protect privacy on the Internet. Also, no one from this group uses advanced anonymisation tools. This group is dominated by men, people from 25 to 44 years of age prevail. We see a positive high perception of economic welfare, which is also correlated with the highest actual wages. These people make clear political self-identification. They are of three groups in the following order: left, right, and center. Therefore, there are no undefined and undecided people in terms of worldview, as well as center-left or center-right people.

Cluster 3. Moderate or extreme cyberlibertarians with high IT competences. In this group, we see the highest aversion towards state institutions among other groups, although the aversion towards the second sector institutions in terms of violating the privacy of users on the Internet is similar to that in other groups. IT competences within this group are the highest, each of its representatives uses advanced nonymization tools. This group is dominated by men, they are people between 35 and 44 years of age. We see an overrepresentation of the inhabitants of cities with more than 500,000 inhabitants and more than 100,000 inhabitants, as well as the inhabitants of the Mazowieckie Voivodeship. These are people who generally have higher education, who are in cohabitation or who declare themselves as single. They positively assess their own material well-being. They consider themselves as non-believers and consider themselves off-scale left versus right. It is worth noting that in all three groups, the assessment of the phenomenon of mass surveillance by state entities (E. Snowden case) and moral attitudes towards corporations (and therefore consent to the claim that profiling and tracking on the Internet is a payment for free services) are the same.

4. Discussion

In the first place, it is necessary to answer the last of the research questions that were asked in the introduction. This question concerns whether Poles want to protect their privacy on the Internet on their own, or whether they expect protection from entities such as the state or corporations in this respect. It should be emphasized that the attitudes of Poles towards freedom are ambivalent. According to CBOS, freedom is in one of the last places among Poles' other values [32]. Poles primarily value health, family, and work; while only 3.0% of them spontaneously indicated freedom as an important value. A survey conducted by CBOS a year later reveals where the value of freedom was asked directly, reveals that for nine out of ten Polish citizens it is a key value in their lives [33] (this result can be partially explained by the strong political polarization of Polish citizens and the numerous protests that took place at that time). Therefore, this empirical study also posed the question of freedom, but in a different context. The study asked which is more important: freedom or security. However, more than a fourth of Poles (28.5%) indicate freedom, and an almost identical group (27.8%) claim that security is more important to them than freedom. Most importantly, one third of the respondents (36.2%) indicated that there is security only when people have freedom. As shown by the segmentation, partial values (such as privacy) and closely related to freedom, although undoubtedly valued, remain detached from reality. Firstly, Poles are not aware of the numerous threats to their privacy. Secondly, the behavioural aspect clearly shows that the respondents are not able to protect themselves against privacy violations on their own. Only one in ten respondents is able to effectively maintain privacy on the Internet using both adequate and advanced (effective in all situations) measures.

The conducted analyses showed that in the Polish society it is possible to distinguish groups that differ significantly in their attitudes towards privacy on the Internet. These differences are not of a fundamental nature, as the behavioural aspect resulting from competences turns out to be the most differentiating. Another important factor in distinguishing the group were different attitudes towards anonymity in the moral aspect and different attitudes towards the legal requirement to present one's real identity in online interactions. Moreover, the respondents shared the attitude towards state institutions as potentially violating their privacy on the Internet. The majority of Poles remain relatively skeptical about legal regulations concerning privacy on the Internet. In contrast, attitudes towards second sector entities that potentially breach privacy were slightly varied and only moderately critical. Research also indicates numerous differences in terms of gender and attitudes towards privacy on the Internet. They were taken into account in the conducted quantitative study. The discovered trends are the same for Western research. There is a visible slightly weaker protection of privacy by women than by men. At the same time, women are assigned higher care to not disclose such obvious elements as a telephone number or name and surname; however on the other hand, women reveal more of other data that can be deanonymised without being aware of it [13]. In the case of Polish society, this is true as long as we do not use the variable age as the control variable. We observe a stronger correlation between the lack of privacy competences and age than between the level of privacy protection and gender. We also know that in the over 55 years of age group, the females are overrepresented, so the differences can be explained in two ways; i.e., both age and gender. Differences in the perception of privacy as a value and age are widely recognized [34]. Moreover, in the literature on the subject, the differences between men and women are not taken as obvious [35].

The privacy paradox has also been confirmed to a limited extent for the Polish population. Susanne Barth and Menno D.T. de Jong identified three explanations for the privacy paradox [36] based on the analysed literature. First, the risks and benefits to privacy are rationally considered by actors, but the benefits outweigh the risks to privacy. Second, the threats and benefits to privacy are rationally weighed by actors; however, the result of the reasoning is distorted by irrational factors or limited rationality.

On the other hand, the third explanation indicates that threats to privacy are not considered by users at all. The first and the second hypothesis seem to be the most probable. The first hypothesis is supported by the low intensity of negative attitudes towards corporations in all surveyed groups in the entire Polish population of the country. The lack of systematic privacy protection behaviour, which is dictated by the lack of technical competences, speaks in favor of the second hypothesis. At the same time, the value of privacy is highly appreciated. The fact that there is a privacy paradox in Poland is supported by the correlation between education and the number of privacy protection measures used.

Relationships between political self-identification and attitudes towards privacy on the Internet are noticeable. In the moral aspect, the center-right and center-left are stronger than other political options against government surveillance. On the other hand, the right-wing highly value anonymity on the Internet and considers it unethical to limit it. The left-right, left, and right, to a large extent value all the elements of freedom in the moral aspect. In the legal aspect, the left and, to a slightly lesser extent, the right are against corporations that violate users' privacy. Behaviourally, the supporters of certain political options do not differ from each other. This diversity is not limited to Poland only [37].

5. Conclusions

In this article, we analysed the value system of Poles in terms of the phenomenon of privacy on the Internet. The following aspects were taken into account: privacy on the Internet as a moral value, privacy on the Internet as a subject of legal regulations (current or future), and actual actions taken by users to protect privacy. The differentiation of Polish society in terms of the three above-mentioned areas was also examined, creating its segmentation.

Freedom, including its component of privacy on the Internet, is valued by Poles. It is primarily verbal, because this value is, however, detached from reality and rarely translates into specific actions. There is a polarization of attitudes regarding privacy on the Internet as a subject of legal regulations. Poles are moderately willing to accept laws against tracking and profiling on the Internet. However, Poles remain significantly opposed to the legal regulation of the obligation to disclose their identity on the Internet and the legally guaranteed access to any information belonging to an ordinary user by law enforcement agencies. The basic observation is the low competence of Poles in the field of privacy protection on the Internet. Poles generally undertake ineffective forms of protection. The tools used are ineffective or mixed with ineffective or even counter effective (at most one in ten Polish users is able to effectively protect their privacy on the Internet).

A moderately strong, negative attitude towards state institutions was identified in the Polish society as a factor that could excessively limit privacy on the Internet. Although the negative attitude towards entities of the second sector prevails in Polish society, it is still lower than the negative attitude towards state institutions. Probable explanations of this phenomenon are a rational profit and loss calculation made by users (users receive benefits from Internet service providers, and therefore agree in exchange for tribute in the form of privacy violations) or insufficient knowledge about privacy violations by Internet service providers. Socio-demographic variables differentiating Poles in terms of attitudes towards privacy on the Internet were identified. These attitudes depend mainly on: age, education, and (to a lesser extent) gender, socioeconomic status, and the size of the place of residence. The self-identification of political attitudes on the left-right scale is also a differentiating factor. However, the basic factor differentiating attitudes turned out to be the behavioural aspect, i.e., the actual actions taken by individuals to protect their privacy on the Internet. Low trust in state institutions in the field of privacy protection on the Internet may lead to a situation of negative attitudes

towards all legal regulations and resistance to them. The issue of violations of privacy by Internet service providers, in particular social media, seems to be a dangerous and requiring awareness phenomenon; however, the lack of trust in state institutions may cause resistance to the reception of values conveyed by a potential social campaign. The level of the ability to protect privacy on the Internet by Poles is insufficient and far unsatisfactory, which may be important for maintaining the state of national security.

REFERENCES

[1] LeakLookup, *Data Breach Search Engine*. [Online]. Available: https://leak-lookup.com/. [Accessed: Oct. 28, 2022].

[2] A. Florek, "The problems with PRISM: How a modern definition of privacy necessarily protects privacy interests in digital communications," *UIC John Marshall Journal of Information Technology & Privacy Law*, vol. 30, no. 3, pp. 571–606, 2014.

[3] L. Rainie, J. Anderson. (2014). *The Future of Privacy*. [Online]. Available: https://www.pewresearch.org/internet/2014/12/18/future-of-privacy/. [Accessed: Oct. 29, 2022].

[4] D. J. Solove, *Understanding privacy*. Cambridge, MA: Harvard University Press, 2008.

[5] H. Nissenbaum, *Privacy in context: technology, policy, and integrity of social life*. Stanford, CA: Stanford University Press, 2010.

[6] L. Rainie, S. Kiesler, R. Kang, M. Madden. (2013). *Anonimity, Privacy, and Security Online*. [Online]. Available: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/. [Accessed: Oct. 29, 2022].

[7] Dell. (2022). *Dell Technologies Global Data Protection Index*. [Online]. Available: https://www.dell.com/en-sg/dt/data-protection/gdpi/index.htm. [Accessed: Oct. 29, 2022].

[8] Surfshark. (2021). *Wyniki ogólnopolskiego badania wskazują, że Polacy nie doceniają wartości swoich danych*. [Online]. Available: https://surfshark.com/pl/blog/polacy-nie-doceniaja-wartosci-swoich-danych. [Accessed: Oct. 29, 2022].

[9] M. Sadurski. (2022). *Wolność przede wszystkim, potem równość – to dla Polaków podstawowe wartości*. [Online]. Available: https://www.newsweek.pl/biznes/co-polacy-mysla-o-swoim-panstwie-wolnosc-przede-wszystkim-potem-rownosc/21hrn6q. [Available: Oct. 29, 2022].

[10] M. G. Hoy, G. Milne, "Gender Differences," in "Privacy-related measures for young adult Facebook users," *Journal of Interactive Advertising*, vol. 10, no. 2, pp. 28–45, 2010, doi: 10.1080/15252019.2010.10722168.

[11] K. Christopherson, "The positive and negative implications of anonymity in Internet social interactions: 'On the Internet, nobody knows you're a dog'," *Computers in Human Behavior*, vol. 23, no. 6, pp. 3038–3056, 2007, doi: 10.1016/j.chb.2006.09.001.

[12] K. B. Sheenan, "An investigation of gender differences in on-line privacy concerns and resultant behaviors," *Journal of Interactive Marketing*, vol. 13, no. 4, 1999, doi: 10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O.

[13] Y. Feng, W. Xie, "Teens' concern for privacy when using social networking sites: an analysis of socialization agents and relationships with privacy protecting behaviours," *Computers in Human Behavior*, vol. 33, pp. 153–162, 2014, doi: 10.1016/j.chb.2014.01.009.

[14] V. Steeves, P. Regan, "Young people online and the social value of privacy," *Journal of Information, Communication and Ethics in Society*, vol. 12, no. 4, pp. 298–313, 2014, doi: 10.1108/JICES-01-2014-0004.

[15] E.-M. Schomakers, Ch. Lidynia, L. Vervier, A. Gadeib, M. Ziefle, "Online privacy perceptions of older adults," *International Conference on Human Aspects of IT for the Aged Population*, 2017, doi: 10.1007/978-3-319-58536-9_16.

[16] A. Acquisti, „Privacy in electronic commerce and the economics of immediate gratification," Proceedings of the 5th ACM Conference on Electronic Commerce, 2004, pp. 21–29, doi: 10.1145/988772.988777.

[17] S. Barth, M. D. T. de Jong, M. Junger, "Lost in privacy? Online privacy from a cybersecurity expert perspective," *Telematics and Informatics*, vol. 68, 2022, doi:10.1016/j.tele.2022.101782.

[18] A. Deuker, "Addressing the privacy paradox by expanded privacy awareness: The example of context-aware services," in *Privacy and identity management for life*, M. Bezzi, P. Duquenoy, S. Fischer-Hüber, M. Hansen, G. Zhang, Eds. Berlin: Springer, vol. 320, 2010, pp. 275–283.

[19] Z. Benenson, O. Kroll-Peters, M. Krupp, "Attitudes to IT security when using a smartphone," Proceedings of the Federated Conference on Computer Science and Information Systems, 2012, pp. 1179–1183.

[20] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," Proceedings of the Conference on Human Factors in Computing Systems, 2014, pp. 2347–2356, doi: 10.1145/2556288.2557421.

[21] S. Barth, M. D. T. De Jong, M. Junger, P.H. Hartel, J.C. Roppelt, "Putting the privacy paradox to the test. Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics*, vol. 41, pp. 55–69, 2019, doi: 10.1016/j.tele.2019.03.003.

[22] S. D. Warren, L. D. Brandeis, "The right to privacy," *Harvard Law Review, no. 5*, pp. 193–220, 1890.

[23] Y. Tsukada, K. Mano, H. Sakurada, Y. Kawabe, "Anonymity, privacy, onymity, and identity: A modal logic approach," *Transactions on Data Privacy*, no. 39, pp. 177–198, 2010.

[24] J. Assange, J. Appelbaum, M.-M.J. Zimmermann, *Cypherpunks: Freedom and the future of the Internet*. New York, London: OR Books, 2016.

[25] J. Waksberg, "Sampling methods for random digit dialling," *Journal of the American Statistical Association*, vol. 73, pp. 40–46, 1973.

[26] R. F. Potthoff, "Some generalisation of the Mitofsky-Waksberg technique for Random Digit Dialling," *Journal of the American Statistical Association*, vol. 82, pp. 409–418, 1982.

[27] H. E. Driver, A. L. Kroeber, "Quantitative expression of cultural relationships," *University of California Publications in Amer. Archaeology*, vol. 31, pp. 211–256, 1932.

[28] J. Czekanowski, "Objectiv kriterien in der ethnologie," *Korrespondenzblatt der Deutschen Gesselschaft fur Anthropologie, Ethnologie, und Urgeschichte*, vol. 47, pp. 1–5, 1911.

[29] R. B. Cattell, "The description of personality: Basic traits resolved into clusters," *Journal of Abnormal and Social Psychology*, vol. 38, pp. 476–506, 1943, doi:10.1037/h0054116.

[30] R. R. Sokal, P. H. Sneath, *Principles of numerical taxonomy.* San Francisco-London: Freeman 1963.

[31] R. K. Blashfield, "The growth of cluster analysis: Tryon, ward, and johnson," *Multivariate Behavioral Research*, vol. 15, no. 4, pp. 439–458, 1980.

[32] CBOS. (2020). *Wartości w czasach zarazy*, no. 160. [Online]. Available: https://www.cbos.pl/SPISKOM.POL/2020/K_160_20.PDF. [Accessed: Oct. 30, 2022].

[33] CBOS. (2021). *Młodzi Polacy o zasadach demokracji*, no. 120. [Online]. Available: https://www.cbos.pl/SPISKOM.POL/2021/K_120_21.PDF. [Accessed: Oct. 30, 2022].

[34] N. Demertzis, K. Mandenaki, Ch. Tsekeris, "Privacy attitudes and behaviors in the age of post-privacy: An empirical approach," *Journal of Digital Social Research*, vol. 3 no. 1, pp. 119–152, 2021, doi:10.33621/jdsr.v3i1.75.

[35] T. Dienlin, S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours," *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[36] S. Barth, M.D.T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics*, vol. 34, no. 7, pp. 1038–1058, 2022, doi: 10.1016/j.tele.2017.04.013.

[37] C. Neill. (2021). *Politics of Privacy: The Role of Individual Political Views in Consumer Data Privacy Concerns*, Honor Theses. [Online]. Available: https://egrove.olemiss.edu/hon_thesis/1697. [Accessed: Oct. 30, 2022].