Inimõiguste Instituut
Estonian Institute of Human Rights

TARTU ÜLIKOOL

2014 STUDY BY THE INSTITUTE OF HUMAN RIGHTS

"THE RIGHT TO PRIVACY AS A HUMAN RIGHT AND EVERYDAY TECHNOLOGIES"

SUMMARY

The focus of the 2014 Human Rights Institute study is on the protection of the right to privacy in relation to the use of everyday technologies. The right to privacy has been included as a human right in many significant international conventions, such as the UN Universal Declaration of Human Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union and the Constitution of the Republic of Estonia. The right to privacy as a human right encompasses a number of interests and rights, such as privacy of the home, protection of personal data, secrecy of the message and so on. The fundamental right to control information about oneself, the right to informational privacy or informational self-determination, forms the basis for the principles of data protection both in the legislation of the European Union as well as the Republic of Estonia.

This study focuses on informational privacy and its protection in the context of modern everyday information and communication technologies – primarily the Internet, computers, smart phones, tablets, various software applications, social networks and web environments. Our starting point in the study was the so-called discourse of threat. Our assumption was that the right to privacy is endangered when using the technologies listed above and therefore in need of protection. The authors of the study concentrated on the perceived threat to one's privacy, not the identification of objective privacy violations (pursuant to applicable laws). In the course of a survey, we asked people how they felt about the protection of privacy and how they perceived different potentially privacy-invading situations.

The III part of the study consists of the theoretical and empirical bases of the study as well as an overview of the concept of privacy, interdisciplinary debates linked to the concept and main terminology. In this part, we looked at the potential examples of privacy invasion in an individual's relationships with the state, private businesses, employers and other people. We also described the attitudes of Estonians in comparison to the average European on the basis of previously conducted studies.

The most important part of the study is its IV part, which consists of the results of the public opinion survey. The main objective of the study was to use a survey to determine the following:

- which situations are deemed to invade privacy;
- how much do the respondents know about what kind of data is processed in relation to them;
- where would the respondents turn in order to protect their data or where have they turned;
- trust in data processors;
- who should protect the data and be responsible for it;
- what kind of privacy protection strategies are used.

The public survey covered all of Estonia and involved 959 respondents in the 15-74 year-old age group; the results can be extended to the whole Estonian population. We believe that the use of digital media affects our attitudes towards privacy. Therefore, we have provided an overview of the respondents' digital media use, which shows that in the past month, 83% of respondents had used the Internet, whereas 13% had never had any contact with the World Wide Web. As was to be expected, the most active Internet users come from the age group of 15-50 year-olds. Based on people's Internet use frequency and the variety of activities carried out in the web, we distinguished between three types of users: Internet non-users, active Internet users and moderate Internet users. Differences between the groups become particularly apparent in how much time they spend on entertainment and communicating.

The study results show that only 18% of people assess their knowledge on what kind of data is collected about them to be good or extensive. 36% considered their knowledge to be sufficient and 43% poor or completely lacking. Older people are more likely to give a negative assessment of their knowledge. As the study also suggested that respondents mostly consider people themselves to be responsible for their data protection, a question arises as to what extent responsibility is possible in such circumstances.

We also examined the respondents' general views on data gathering and protection. The majority (53%) claimed that the worry about personal data is relevant, while a significant number of participants (41%) also found that the issue of personal data protection is exaggerated. Both this study and previous similar studies indicate that Estonians tend to be passive and accepting in connection with data collection. The respondents believed that the acceptance of data gathering is unavoidable if one wants to use certain services or enjoy certain benefits (88% of respondents). A prevalent opinion was that data is collected anyway; there's nothing that could be done about it (83% of respondents). 74% of participants agreed with the claim that "they had nothing to hide", which could also allude to a sense of inevitability. More active, i.e. younger, Internet users tended to disagree with this statement a bit more often. Despite the common myths to the contrary, younger people (15-24 year-olds) view the protection of personal data as somewhat more important than other age groups.

In the case of perceived threats to privacy, a significant factor is trust in the parties that are processing data. In the questionnaire, we asked which parties that collect data could endanger privacy. It was interesting that all listed parties (state, other states, employers, private businesses, smart devices, acquaintances and strangers) were seen as potential threats to privacy when they process data. The biggest perceived threat is information gathering by smart devices and applications. One of the questions was to what extent people trusted different parties in relation to the purposeful use and protection of data. Medical institutions, the state as a general institution, educational establishments, local governments and financial institutions were trusted the most. Less trust was placed on private companies (online shops, etc.) and Internet service providers.

In general, it was seen as equally problematic when the data was accessed or collected without a person's consent by the state, private businesses or other people. At the same time, in the light of recent NSA and Wikileaks scandals, it was surprising that the respondents (61%) agreed with the statement that the state should have more rights to process personal data without consent in order to ensure people's security. Estonians are characterised by a positive and trusting attitude towards the protective role of the government and state.

Additionally, we were interested in what kind of situations bothered people and which situations and consequences thereof were considered a threat. To generalise, the threats were the following: the use of collected data without the person's consent and for another (unintentional) purpose; the interference with a person's private matters and freedom of choice; identity thefts; and combining data to learn things about a person that the said person would like to keep a secret.

The perception of privacy largely depends on the context or situation, which was why, in addition to more general questions, we asked about more specific potentially privacy-invading situations. Some studies have shown that the attitude towards privacy in a specific situation could be quite different from the overall views in relation to personal data gathering and use. We listed 21 situations, some of which were only asked about from Internet users. The most disturbing situations for respondents were linked to children, such as when a kindergarten displays a photo of the child on its website (bothered 44%) or when a teacher follows the students' activities on Facebook (38%). For Internet users, the disturbing situations were the following: a service provider collects and analyses a user's data and behaviour for targeted advertising or some similar purpose; email service providers analyse the content of e-mails (65%); mobile phone and Internet applications request personal data (54%). Situations linked to security – surveillance cameras in the city and on the roads (bothered 13%), security cameras in schools (17%), examination of travel behaviour and history to guarantee the safety of flights (19%) – were found less disturbing. Situations concerning direct personal gain, such as data accessibility for doctors in the case of medical services (15%), sharing of location data to obtain restaurant and parking recommendations in the vicinity or to find a taxi quickly (31%) were also not as bothersome for people.

In the study, we asked people who they thought should be responsible for the protection of data on the Internet. Similarly to the pan-European Eurobarometer study, it turned out that 84% of respondents agreed that the protection of personal data on the Internet is primarily the responsibility of the individual person. Surprisingly, 55% thought that the responsibility fell on the European Union and only 24% thought the same about the Estonian state. It is likely that the results have been influenced by media coverage of the ruling of the European Court of Justice about "the right to be forgotten" or the data protection reform of the European Union.

Another noteworthy result was that 47% of people claimed to read the privacy policy of a service before using it, 22% do it sometimes and 22% rarely or never. Experts who discussed the results were very sceptical about this answer. They mostly agreed that people had probably given a "socially acceptable" answer at this point. The controversy mainly arises because the privacy statements are usually long and complicated documents from where it is rather difficult to find which data will be processed and what the associated risks are. Therefore, it is doubtful that we can really refer to "informed consent" in this respect.

The respondents were asked to what extent they had felt that their privacy had been violated in the past 12 months. 16% of respondents said that their privacy had been violated by strangers, 15% blamed Internet service providers, 11% private businesses and 11% friends and acquaintances. An important question posed was where people would turn in the case of the violation of privacy. The list also contained authorities that fulfil some data protection tasks but who do not directly handle complaints on data protection issues (e.g., the Information System Authority, the Ministry of Justice) as well as authorities that are linked to this area more indirectly (e.g., the Consumer Protection Board). The respondents answered most often that they would turn to the Data Protection Inspectorate (77% in total), whose statutes specify that it is their task to process such complaints. Many of the respondents (73%) thought that the person or organisation that invaded the privacy should deal with the violation. People would also turn to the company that owns the problematic website (58%) or to the Internet service provider (54%). A rather large share of people would go to the police (77%), the Consumer Protection Board (68%), the court (55%) and the Information System Authority (53%). These results indicate that people are not really sure where to turn in the case of data protection violations.

According to the study, people employ several strategies simultaneously to protect their privacy; 10-12 activities out of the listed 19 were mentioned most frequently. The most common strategy is the limited sharing of information, followed by more technical solutions – using passwords and security software. A large part of the respondents (69%) named social steganography – the sharing of information in a way that the information only makes sense to selected people. The least applied strategies are disclosing false information about oneself, encrypting messages and using several identities. People show the least familiarity with technology-based strategies, such as encryption, deletion of a browser history and cookies, modification of privacy settings in a web environment or applications. Women tend to use social strategies, while men prefer technology-based solutions. Younger people have the widest variety of strategies in use, which probably comes from the fact that their activities on the web are also the most diverse. Active Internet users are more familiar with the existence of various strategies and use different activities to protect their privacy to a larger extent than moderate users.

The V part of the study deals with the legal aspects of the right to privacy and data protection. This chapter summarises the development of the right to privacy as a human right as well as some of the more significant principles in the protection of personal data and regulations adopted in order to protect informational privacy. Modern information and communication technologies have introduced some serious issues in the field of data protection laws, and so far there are no solutions about how to deal with the problems.

The last, VI part of the study contains suggestions and recommendations for public authorities on various ways to protect the right to privacy. These recommendations were compiled by the authors of the study with noteworthy input from the experts who participated in the discussion on the results of the survey. The amendment of legislation is important; however, laws do not stop people from sharing all sorts of information about themselves nor do they make people realise threats and assess risks to privacy in different situations. Therefore, our suggestions and recommendations stress the need to raise awareness about data protection and improve overall digital literacy among the population from childhood onwards.