2014 STUDY BY THE INSTITUTE OF HUMAN RIGHTS

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

RECOMMENDATIONS AND SUGGESTIONS TO AUTHORITIES

INTRODUCTION

The main objective of the Human Rights Institute 2014 study was to use a public survey to determine the following:

- which technology related 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 suggestions and recommendations brought out here thereby stem from the results of the survey and not from legal or political analysis on the efficiency of the protection of the right to privacy.

RECOMMENDATIONS

Awareness of data collection and personal responsibility

The results of the study showed that most respondents found that their knowledge about what kind of data was collected about them was sufficient or poor. Older people are more likely to give a negative assessment of their knowledge. At the same time, the majority of respondents agreed that the protection of personal data on the Internet is primarily the responsibility of the person him or herself. This responsibility can be carried out in several ways and through different privacy protection strategies. Nevertheless, a question arises –

how can people be responsible if they don't really know what kind of data is being processed in relation to them?

Almost half of the respondents claimed that they always or usually read the privacy policies. Experts who discussed the results were very sceptical about this answer. Mostly they agreed that people had probably given a "socially acceptable" answer at this point. This means that people are aware that they should read the privacy policy, but to what extent they actually read it remains unclear. It is likely that the text of most privacy policies is long and complicated and does not answer the question regarding the data that is gathered and processed about a person. Therefore, it is arguable to what extent the consent given to the terms and conditions is "conscious" and informed.

In the case of state technologies, services and solutions, a person's consent is not necessary if the collection of data is carried out pursuant to law. Databases have statutes, which provide for the access of third persons to the data, and similar requirements. Unfortunately, this information is often not easily accessible and comprehensible to an ordinary citizen. The experts who participated in the discussion found that public authorities should at least inform people in a simple and understandable manner regarding which data is collected about them and how this data is being used.

Recommendation

1) We suggest that clearer rules or instructions be adopted about privacy policies, which would easily and shortly summarise what kind of data is processed and how. If necessary, a standard form or template should be developed to exemplify the rules or instructions.

2) State authorities should introduce good practices on how to inform people in a simple and understandable manner regarding their data being collected and used.

Awareness of one's rights in the event of an violation of privacy

In the survey, people were asked where they would turn to protect their rights in the event that their privacy had been violated in an Internet environment. The list 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 deal with data protection more indirectly (e.g., the Consumer Protection Board). Most often, the respondents would turn to the Data Protection Inspectorate, whose statutes specify that it is their task to process such complaints and whose website contains information on how to request assistance, different sample templates and guidelines. People would also turn to the person or organisation that violated the privacy, also to the company that owns the problematic web page or to the Internet service provider. A rather large share of people would go to the police, the Consumer Protection Board and the Information System Authority. The police only processes informational privacy violations in a few instances, such as identity theft. People always have the option of turning to the court, and about half of the respondents would do exactly that according to the questionnaire. Referring to the

Information System Authority or Consumer Protection Board to protect one's privacy would be of no use whatsoever.

To the authors of the study these results indicate that people are uncertain as to where to turn in the event of data protection violations and what the exact role is of the listed authorities. Hence, this topic should be covered more in society at large.

Recommendation

We need to raise awareness about where to turn for the protection of one's rights in the event of data protection violations and what the roles are of different state authorities. The Data Protection Inspectorate should compile some clear sample cases, which would help clarify data protection violations and instruct on who to turn to if you have a problem.

Raising public awareness to improve overall digital literacy

The general opinion was that campaigns and events to raise awareness among different target groups as well as the preparation of data protection instructions in the Data Protection Inspectorate were extremely useful, and such activities should certainly continue. It is also important to improve existing legislation, but counting on such amendments could create the false security that an individual is not responsible for his/her behaviour.

Awareness needs to be raised from childhood. In recent times, there have been many outstanding campaigns on Internet safety that have mostly been directed at the most active Internet users – young people; such campaigns are usually organised by foundations and non-profit associations, such as the foundation Vaata Maailma SA with their project "NutiKaitse 2017"; MTÜ Lastekaitse Liit coordinated the project "Targalt internetis" (Smart Behaviour on the Internet); the foundation Hariduse Infotehnoloogia Sihtasutus has held a number of projects, events and media campaigns. All these organisations have wider goals – to improve society's (primarily young people's) digital literacy and security awareness – while data protection is one aspect of this competence. Public authorities, such as the Data Protection Inspectorate, the Police and Border Guard Board, the Information System Authority, the Ministry of Social Affairs and others, have been involved in the events and campaigns as funders and as active participants.

With sample scenarios, it would be easier to explain how personal data is used in different contexts and of what kinds of dangers people should be aware. This could possibly make people think more about the value of information and who and to what extent should get access to their personal data. Some of the most successful examples of awareness raising have been the Data Protection Inspectorate's comic strips for young people, a Safe Day on the Internet videos completed in the framework of the project "Targalt internetis", and the Vaata Maailma SA project "Päriselt ka või?" ("Really?!") (päriseltkavõi.ee).

Recommendation

To continue with the campaigns and events directed at increasing society's general digital literacy and awareness. To support different interested parties in their activities through financing and active involvement.