THE RIGHT TO PRIVACY AS A HUMAN RIGHT AND EVERYDAY TECHNOLOGIES

Theoretical and empirical bases of the study

Maria Murumaa-Mengel
Pille Pruulmann-Vengerfeld
Katrin Laas-Mikko

TABLE OF CONTENTS

INTRODUCTION

PRIVACY AS A FOCAL ISSUE. In modern society, **challenges related to privacy are perceived larger than ever before** in the history of humankind. On the one hand, the loss of privacy may not seem greater compared to earlier times, when people lived in small communities or extended families and secrets were probably harder to keep. On the other hand, digital technologies and new media have altered the ways in which information is shared, received and recorded, setting a huge challenge for our privacy. This study focuses primarily on **informational privacy**. The possibilities to look data up quickly, forward it instantly, keep it eternally and copy it endlessly are only a few phenomena to accompany digital technologies and endanger privacy by making it difficult to draw a line between what is public and what is private. Although most of the public discussion has centred on situations in which privacy has been violated by other parties (e.g. the spying scandals that shocked Europe, WikiLeaks, the control that large corporations, such as Google, Facebook and Amazon, exert over a person's data and behaviour), violation of privacy can also be seen in cases where people themselves share content without full awareness or give consent to the use of their data in various situations. Therefore, in the context of defending privacy as a basic human right, we should pose the question **to what extent should we protect a person from him- or herself?**

THE SIGNIFICANCE OF CONTEXT. As we started with the study on the right to privacy, we faced a complicated decision as to what to examine in the first place – there is an unlimited supply of situations that violate or infringe the right to privacy. These situations make up kaleidoscopic patterns of contexts, actors, messages and time, while they are always viewed through the filter of social norms and values (see Figure 1). All the elements are closely linked and constantly changing. Therefore, the information of our being away from home might be necessary for our neighbour so he or she can keep an eye on our house, whereas it would infringe on our privacy if a stranger knew this, because he or she could be a potential threat. One can be pleased when a doctor shares information on one's physical state with other doctors so that they can make better treatment decisions; however, one's rights would be violated if such medical data would become available to an employer who could then decide to change the status of the professional relationship. In Estonia as well as elsewhere, people often ask about the extent of the rights of the employer; for instance, are work-related e-mails private or public? Is it acceptable to look up an applicant's social media account in addition to their CV before a job interview? To paraphrase Pille Runnel, who said that each person has "their own Internet, which is linked to their skills, habits and needs" (Runnel 2010), it could be said that **each person also has their own unique situational privacy**. As no one exists in a social vacuum or separate from society, we should take into account that a person's "own" privacy has been influenced in various ways by the context – what is considered private has been entwined with context (social mores, contemporary and historical peculiarities, etc.).

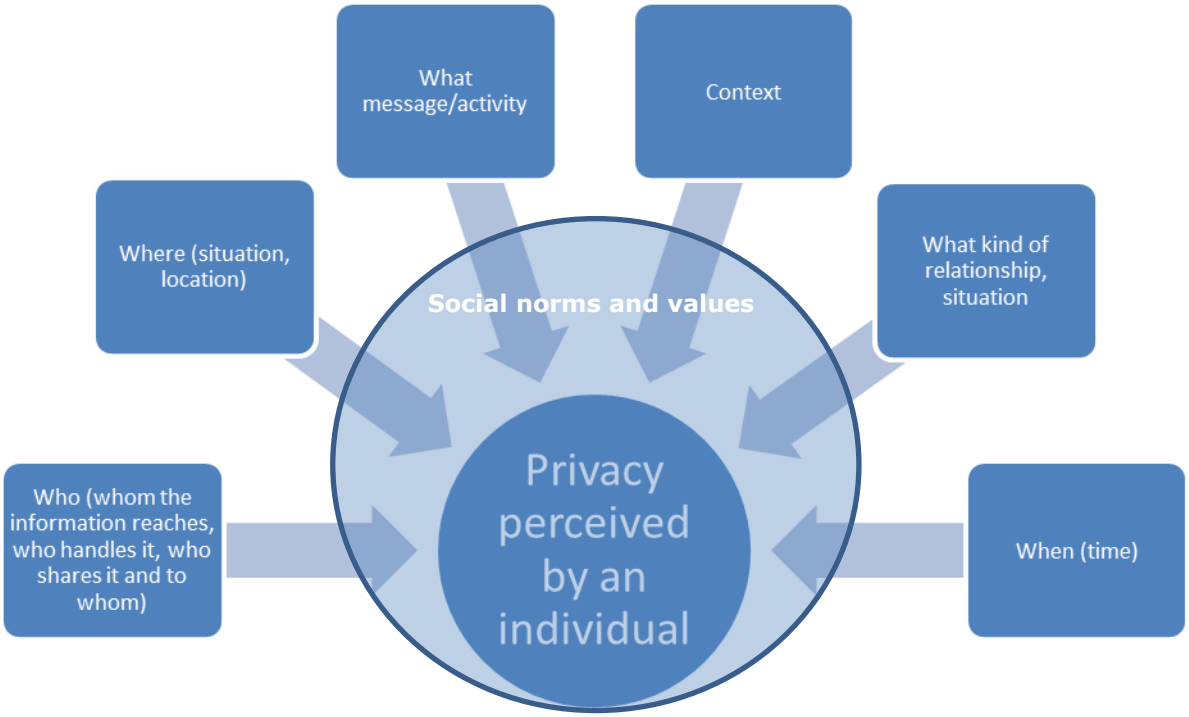

Figure 1: Factors that influence contextual privacy

Some authors are of the opinion that privacy in the modern information society can be described in a simple way: it does not exist! This report is based on the assumption that there are several strategies that can be applied to protect privacy. When speaking about informational privacy we can distinguish between an **objective violation of privacy** and a **perceived threat to privacy** – these two may but do not have to be linked; in this study, we concentrate on the perceived threat. For instance, legally everything is in order when a person has agreed to the conditions of use of a service – it is considered informed consent. Nevertheless, certain clauses of a contract could be perceived as an invasion of privacy, even if legally no violation has occurred. The purpose of the present study is not to determine whether a specific situation can be considered an violation of privacy in an ethical or legal sense; instead, we will look at how people perceive different situations and which situations, in their mind, could potentially violate privacy.

This part of the study will give an overview of the theoretical key concepts, issues and studies related to privacy, and it will explain the theoretical and empirical bases of the study.

Below, we will:

- give an overview of the general understanding of privacy as well as online privacy specifically;
- summarise the main perceived violations of privacy;
- highlight the problems that an individual has when communicating with the state, employer, service providers and other people;
- describe the views of Estonians on privacy-related matters in comparison to the rest of Europe.

THE CONCEPT OF PRIVACY

ASPECTS OF PRIVACY, DIFFERENT PERSPECTIVES. The concept of privacy can include a wide variety of interests, rights and aspects. For instance, David Solove (2002) names **six aspects of privacy**: the right to be left alone; restricted access to one's person (physical person) or possibility to protect oneself from unauthorised access; right to hide certain things from others; control over personal information; protection of one's dignity, individuality and persona; and intimacy – the right to control and limit access to information that concerns intimate relationships and aspects of life.

Several authors who have dealt with privacy issues (Allen 1997, DeCew 1997, Rössler 2005) have distinguished between **three spheres of privacy**: informational privacy; physical, local or spatial privacy, and decisional privacy. In this report, we focus primarily on informational privacy, which concerns the data collected, recorded and shared about a person.

Various thinkers and scholars (e.g., Gross 1967, Miller 1971, Bennett 1992, Post 2001) have claimed that it is not possible to reach a clear consensual agreement on what exactly privacy means. **The concept of privacy is complex and controversial.** The complexity stems from the fact that in defining privacy people also talk about the value of privacy, that is the role of privacy for an individual and for society at large, as well as about the scope of the concept of privacy and how it could be morally weighted with other values.

A large share of privacy theoreticians (Westin 1967, Rachels 1975, Fried 1984, Rössler 2005, et al.) consider the central notion in terms of privacy to be **control over personal information**. One of the best known privacy scholars Alan Westin (1967: 7) defined privacy as the right of individuals, groups or institutions to decide when, how and to what extent the information related to them is communicated to others. This means that the extent of privacy or the feeling of whether privacy has been violated or not depend on the data subject's choice as to how well and what kind of information he or she wants protected. This is based on the liberal idea of self-determination – a person determines his or her self and decides freely the values that he or she holds dear.

The idea of control seems all-encompassing and absolute, which is why the modern concepts of privacy tend to narrow the scope of the term and emphasise **a person's right to decide who and to what extent can access and use information concerning him or her** (Rössler 2005, Moore 2008 *et al.*). In this respect, the right to privacy includes control over access as well as over information usage rights. In the core of this right is the person's (informed) consent to have his or her personal data collected/accessed for a specific purpose, such as purchasing something from an online store. This consent does not automatically mean that the data can be used in some other context or circumstances for some other purpose.

PRIVACY ON THE INTERNET

PERSONAL RESPONSIBILITY IN PROTECTING ONE'S PRIVACY. A person has the right to exert control over access to his or her personal information and how this information is used. Helen Nissenbaum (1998) stresses that this right does not necessarily apply in cases where the person has disclosed the information him- or herself and has not taken any specific measures to have the information removed from the public space. In the era of social media environments, the latter causes the most problems, as a significant share of information that ends up on the Internet has been uploaded by the people themselves. Terence Craig and Mary Ludloff (2011) claim that as much as 70% of the digital world has been created by people through the use of Facebook, Twitter, LinkedIn, Flickr, YouTube and other similar services.

THE SPREAD OF ICT AND PRIVACY. The fast development and wide accessibility of information and communication technologies (ICT) has caused technology, by which we primarily mean the Internet, computers and mobile phones, to be **domesticated**, accepted and integrated into our everyday life. In Western society, this has happened to such an extent that we can now speak about the ICT-rich "bedroom culture" (Bovill & Livingstone 2001). In case of everyday technologies, we need to pay attention to their **potentially extensive usage opportunities** (from banking to porn), **constant readiness to be used** (mobility, fast connections), **large number of users** (critical mass) and the **social rituals and routines** that come with these technologies (e.g., Googling your date, Skyping your grandmother on Sundays, creating a personal audio space in a public place with the help of earphones, and so on). Technology has become an extension of our physical self and has turned invisible because of its constant presence, thereby making the potentially privacy-violating situations sometimes also invisible. If Michel Foucault (1991) spoke about the society as a panopticon (the few observe/watch the many) and Thomas Mathiesen (1997) described television as a synopticon (the many watch the few), then Jakob Linaa Jensen (2010) and Jeffrey Rosen (2004) have talked about an omnopticon - the constant observation of each other, the so-called joint surveillance, which is characteristic of new media environments. The process that happens in social networks has also been called participatory surveillance (Albrechtslund 2008) - the many watch the many via links and networks of relationships and friendships. None of the users ever knows who is watching them at any given time. **Borders between the public and the private have been considerably blurred because the public is intermediated through social networks.** When we compare networked publics to the classical understanding of the public sphere (parks, streets, cafés, etc.), we can see four unique properties (boyd 2007):

1. Persistence. Anything done or said at the age of 15 is still accessible and visible as one grows older, even if one's attitudes and ideas have changed.
2. Searchability. Published information can be found on the Internet with minimum effort.
3. Replicability. Digital information can be easily copied and thereby transferred from one context to another or unnoticeably modified.
4. Invisible audiences. In intermediated public, we cannot see who observes us and the previous three traits give the voyeurs access to the time and space into which they had not been invited.

The problem is that a person's life can be divided into different social situations with specific audiences and context (boyd 2008). In professional relations, people share one kind of information, with close friends they communicate in a different way and with their children in yet another way. In a medical institution, one has to share one's medical history but during a job interview this kind of information should not be requested (Baghai 2012). **New media has merged different contexts that used to be separate; the audience remains invisible and the content persistent**.

STRATEGIES TO PROTECT ONLINE PRIVACY. Nevertheless, danah boyd [sic!] (2008) indicates that our current situation is not as unique as we like to stress – we could bring several examples from history where despite an over-controlling regime trying to insinuate itself into the private sphere, people have developed strategies to maintain their privacy to at least a certain extent. There are several strategies to protect online privacy. The simplest methods are moderate use, self-censoring and deleting accounts and information (Oolo & Siibak 2013). However, the actual efficiency of such strategies is doubtful, as people tend to underestimate the size of their audience and by the time information is deleted it could have been replicated to other sites. Web environments allow users to apply various privacy settings through which one can restrict the size of the direct audience of a message. At the same time, modifying the settings takes time and effort, and it might be too complicated for some web users. We should keep in mind that default settings often leave as much of the user's information public as is possible – privacy is something that requires extra effort, not something set by default. The European Union has turned its attention to exactly that aspect in reviewing its laws on data protection: **measures and settings to protect data should be inherently designed into services and products and, as opposed to the currently prevalent situation, it should take special attention and effort to publish information, not to protect it** (Progress on EU... 2014).

EXAMPLES OF PRIVACY PROTECTION. Other strategies available to people are to use several identities on the web, to selectively post false information and to act anonymously (Oolo & Siibak 2013). Another method to maintain at least partial privacy is social steganography – knowingly sending ambiguous messages, which can be understood one way by part of the audience and in another way by the rest (boyd & Marwick 2011, Siibak & Murumaa 2011). Steganography is a historical technique used to hide messages in plain sight by using invisible ink, writing with milk, rebuses and secret languages (boyd 2010). In social networks, similar techniques are used; for instance, a person can post a sentence that says nothing to part of the audience, but to a limited target group, who is familiar with the context and possesses the correct interpretative lens to decode the message, this sentence has a deeper meaning and speaks about the sender's mental state, recent developments in his or her life or certain attitudes (boyd 2010). The Eurobarometer that studied attitudes and practices related to privacy (Special Eurobarometer 359... 2011) showed that Europeans prefer strategies that include the moderate sharing of information as well as various technical and procedural strategies, such as limiting access to information by applying tools offered by the environment, by using web pages with secure connection and using security software.

Some more radical authors, such as Simson Garfinkel (2001) and David Brin (1998), have even claimed that privacy is dead and that we should get used to the thought that our society is extremely transparent. Brin (1998) also warns that the greatest threat is the

availability of surveillance technologies, which is modern-day reality – **if everybody has access to the same information, then the power relations are equal and total surveillance ensues.** Mark Zuckerberg, the founder of Facebook has said (Kirkpatrick 2010) that the era of privacy is over and that only those people who have something to hide worry about the lack thereof. That same argument has previously been used by feminist theoreticians and communitarianists, who stress that privacy as an individualistic value supports anonymity and covers socially unacceptable behaviour and freeriding. The inherent logical error of this argument has been pointed out by Solove (2007), who says that the claim is based on the false presumption that privacy means hiding bad deeds and wrong behaviour. Everyone has something to hide from others. It seems that **the debate on privacy has become stuck in the context of concealment and restrictions**, as used to be the case with the pioneers of privacy (Warren & Brandeis in 1890 and Cooley in 1880). The people who play the I-have-nothing-to-hide card often mean that they do not have anything to hide from a particular audience whom they imagine while posting, and not from absolutely anyone who could potentially read the post on the Internet (Siibak & Murumaa 2011).

VALUE OF PRIVACY AND INVASION THEREOF

POSITIVE ASPECTS TO LOSS OF PRIVACY. It is clear that a more transparent, always remembering information society has created many new opportunities for people, and in this light the loss of privacy could be viewed as positive: sharing information about oneself plays an important role in maintaining friendships; sharing information about oneself in the virtual world is to an extent a demonstration of trust in your network (Marwick, Murgia-Diaz & Palfrey 2010). Malene Charlotte Larsen (2007) has highlighted the following positive aspects about disclosing personal information, presenting oneself on the Internet and about the impact of such activities: The Internet is the place of continuous (re-)construction of the identity of oneself and others, of the reassurance of the sense of community, and of the implementation of democracy through expressing one's opinions and having one's voice heard.

PRIVACY AS A VALUE THAT NEEDS PROTECTION. Discussions over privacy that take place in the public and academic spheres mainly include the discourse of danger – privacy is a constantly bombarded value and undoubtedly needs protection. First of all, we should actually ask ourselves what privacy protects. Why is privacy valued in the first place and why do people want to limit access to information regarding themselves or restrict the use thereof? The term privacy does not really define what exactly it is that the limited access and use are supposed to protect.

FUNCTION OF PRIVACY AS AN INSTRUMENTAL VALUE. Privacy is generally considered an instrumental value, which is important because it protects other, possibly more significant values. There is no consensus on the matter, but quite many authors say that **the main function of privacy is to protect an individual's autonomy and the development of person's self-image** (Gavison 1980, Schoeman 1984, Kupfer 1987, Rössler 2005, Steeves 2009 *et al*.). Privacy gives us the **right to decide** about the context in which we act or operate to defend it against interferences and to allow us shape our life and self-image. **Respect for another's moral autonomy** presumes that we try to fit in someone else's shoes and understand his or her personal goals, values, attitudes, ideas and desires from his or her point of view (Williams 1973). **Informational privacy** signifies a person's right to decide in the information sphere who gets access to information regarding him or her and to what extent. According to Valeria Steeves (2009), privacy helps us create **meaningful relationships with others**. She thinks that striving for privacy is a social practice, which allows social actors to draw a line between themselves and others, thereby being open or closed to social communication. In accordance with this theory, social actors are capable of choosing what is the most important for them and defining themselves in relationships.

VIOLATION OF THE RIGHT TO PRIVACY. Violation of the right to privacy can result in many undesirable consequences for a person, such as identity theft and access to person's property or benefits; injustice caused by misuse of certain information; unequal treatment or harm to one's dignity. Risks to society are difficult to assess because as a rule we are dealing with so-called **soft impacts**. We cannot say exactly how many people need to feel that their

privacy has been invaded and in which context it needs to happen so that people would lose trust in government institutions or that democracy would be endangered.

Privacy advocates often speak about privacy as a right, which leaves the impression that we are dealing with an absolute right or value that should not be given up in any case, and that a conflict with competing values, such as solidarity, security and freedom of speech, is unavoidable and irreconcilable. More recent treatments presume that value conflicts and choices between different values are a natural part of the pluralist society and privacy should be weighed against other important, and sometimes incomparable values. We risk daily the invasion of our privacy by publishing sensitive information about ourselves in significant relationships or social environments; generally, we do not want "perfect privacy" – that is, complete separation, anonymity or exclusion from social relations. Therefore, as mentioned earlier – context matters.

PRIVACY AS AN ENDANGERED VALUE. The foundation of our study consists of the questions: to which extent is privacy perceived as an endangered value and in which context is it valued? By posing these questions, we leave aside the possibility that people are quite happy to give up their informational privacy. Although we cannot exclude the possibility that this might be the case, theoretical and empirical results, as well as the results of this study indicate that privacy is generally viewed as something that needs protection.

The currently still valid European Union data protection directive (EU Directive 95/46/EC) regulates certain areas of data use; in summary thereof, we can specify **six main ways in which privacy can be invaded**:

1. Insufficient informing – a person whose data is being collected has not been informed thereof;
2. Non-purposeful data processing – collected data is used for a different purpose than declared;
3. Lacking consent – personal information is published or shared with third parties without the person's consent;
4. Security holes and information leaks – collected data is not processed safely enough (abuse, misuse, theft and loss of data);
5. Limited access to own data – a person has no access to the data collected about him or her and therefore no opportunity to correct or withdraw erroneous and false information;
6. Responsibility – data collectors are not responsible for following the above-mentioned principles.

The European Union is currently looking for new solutions to renew the said data protection act of 1995; one of the key points of discussion is the protection of online privacy rights. Although the Internet is characterised by a lack of universal rules due to its global nature, the EU hopes to develop a General Data Protection Regulation by the end of the year that would satisfy all member states. A key concept to guide debates on legislative amendments is **"the right to erasure"** (European Parliament legislative... 2014) – this means that people are given the right to demand that information about them be deleted from the Internet. This spring, the Court of Justice gave a decision on the basis of which people can request a search engine (e.g., Google) to delete incorrect data about them, thereby making the search

engines, in effect, official data processors (Rebane 2014). The Court was of the opinion that a search engine should, as a rule, prefer the right to privacy to the public's right to information (Streitfeld 2014). Critics have said that the decision restricts freedom of speech and initiates an era of private censorship (Mayes 2011, Index Blasts EU... 2014).

PRIVACY IN DIFFERENT RELATIONS. In the following sections, we will discuss different relationships and privacy in various spheres of life, an individual's relations with the state, businesses and other people. Such discussions seldom focus on the fact that the invasion of privacy often happens perfectly legally; invasion is perceived in cases where a person has actually disclosed the information him- or herself. Here, it ought to be stressed that **a person him- or herself often poses the biggest threat to his or her privacy** by publishing all kinds of information in different environments, which can then be used for a purpose different from what the person who disclosed the information had imagined. For instance, information published in social media is of interest to commercial enterprises (more on this below) as well as to the authorities that maintain law and order and national security (Wigan & Clarke 2013). The police uses Twitter and Facebook to keep an eye on a suspect's activities (Knibbs 2013), a Facebook account can help assess a person's credit profile (Nergi 2013, Parksepp 2014), and there have been debates on the possibility for courts to contact people via Facebook (Teder 2012).

THE STATE AND INDIVIDUAL

When we speak about the relationship between the state and the individual, we can safely say that it is extremely multifaceted because of the wide spread of e-services and digital information transfer, and that the six above-mentioned ways of invasion potentially exist in this relationship. Once again, we need to distinguish between the objective violation and perceived threat – technically, data can be protected, but people still feel that their privacy has been invaded. This study (as well as the Special Eurobarometer study 359 which dealt with privacy) mostly covers phenomena related to perceived privacy, not with specific measurable and objective ways of privacy violation.

ESTONIAN EXAMPLE. Estonia has earned positive recognition in the world for its diverse and widely used national e-solutions (electronic tax returns, e-voting, paperless government, e-health, e-commercial register, e-school, education information system EHIS, etc.). Estonian Internet users find that services have had a clearly positive impact on their lives by helping them save time and making paperwork easier to handle (Kalvet, Tiits & Hinsberg 2013). These two factors – perceived usefulness (with a focus on the objective) and perceived ease-of-use (with a focus on the process) have a central position in the technology acceptance model (Davis 1989). Although data is nowadays collected, processed and stored in many databases, most people pay little attention to this or find it insignificant – only 40% of Estonians agreed with the Eurobarometer claim that the government is asking for more and more personal information, whereas the European average was much higher – 64% (Special Eurobarometer 359... 2011). Estonians use the possibility to submit online income tax returns and get digital prescriptions most actively; the latter was also often mentioned by those who did not consider themselves Internet users at all (mostly older people). Therefore,

we cannot really say that digital prescriptions are used as an e-service (Kodanike rahulolu riigi... 2012). On the basis of the special Eurobarometer study on data protection and privacy (Special Eurobarometer 359... 2011), it can be said that the most often used areas are also the ones that people consider the most private (both in Estonia and in the rest of Europe). The results of the study commissioned by the Ministry of Economic Affairs and Communications (Kodanike rahulolu riigi... 2012) indicate that people's discontent with e-services generally stems from the complicated and time-consuming usage of the service; the fact that the service is not secure (incl., in relation to an individual's privacy) was mentioned as a reason for discontent the least often. The issue of data gathering and privacy is approached with certain passivity or even fatalism in Europe; for instance, 74% of European citizens believe that disclosing personal information is an increasing part of modern life (Special Eurobarometer 359... 2011).

SECURITY PRINCIPLES OF STATE DATABASES. State databases generally follow three security-related principles, which form the basis for assessing the data security level and setting security requirements – confidentiality (data can be accessed by authorised persons only), integrity (data is based on the original source, it cannot be changed without authorisation and all changes can be traced) and availability (data can be accessed and used on time and easily) (Haas *et al.* 2011). We can also add the aspect of responsibility – people have the right to criticise and request information (Fernández-Alemán *et al*. 2013). Databases that contain such sensitive information are in great danger of information leaks and data thefts. In case of the digital medical history used in Estonia, the state has taken different security measures to make the system secure and transparent; for instance, all actions (adding, modifying and looking up data) leave a trace, a complex attack is needed to create serious harm, there is no "super administrator", data is encrypted and for log-in you need to authenticate yourself with an ID-card, mobile-ID or by some similar method (Süsteemi turvalisus 2014).

FINANCIAL DATA. The publication of financial data usually means everyday banking activities, which is mostly the domain of private businesses but could be considered a relationship between the state and the individual because the state exercises control over it and bank login is used as a common authentication method. In comparison to the EU average, Estonians are very avid Internet banking users (the EU average is 47% of all Internet users; in Estonia it is 69%); there was a separate question about income tax return and other e-services, and once again the European average (23% have ever used any) was much lower than the popularity of such services in Estonia (68%) (Special Eurobarometer 359... 2011).

COMBINATION OF DATA. Various data is nowadays often combined for big data administrators and for people's own use; for instance, a couple of years ago, every second Estonian had used the state portal eesti.ee (Kodanike rahulolu riigi... 2012), which combines state and municipal e-services, information on various areas of life and the contact data of public authorities. As new registries and databases are created and the old ones are updated, modern (democratic) states need to pay attention to different aspects in relation to citizens' privacy. When we speak about people's **health**, we should mention the unique Estonian Gene Bank (biobank, with voluntary membership of approximately 5% of the Estonian adult population), which contains data that can help with genetic research and forms the basis for

the introduction of the personal medical treatment approach in Estonia (Tartu Ülikooli Eesti Geenivaramu 2014). The personal approach to medicine and extra thorough databases that contain sensitive data are one of the main issues when talking about privacy risks.

Discussions on **Internet privacy** often concentrate on the freedom of speech and censorship, but in the world of permanent intermediated publicity, copiability, searchability and availability to the invisible audience, information that can be deleted or lost in the real world is easily available to the state. Globally, we have seen several cautionary examples of how the state aggressively interferes with people's freedom of speech and informational self-determination, thereby invading individuals' privacy; in India, for example, one can get sentenced to 90 days in prison for liking inappropriate content on Facebook (Cooper 2014) and the Chinese government employs two million people (so-called public opinion analysts), who, among other things, check that people do not post opinions critical of the government (Hunt 2013). Due to cultural differences, we can see different approaches in Western cultures as well – in the US, the (self-)regulation of privacy-related issues is led by the private sector while citizens see the state and the government as threats to their privacy and wish to curb their power (Belanger & Hiller 2006), whereas in Europe, including Estonia, the government is perceived to lay down regulations to protect privacy and is therefore seen as a trustworthy saviour (Titiriga 2011, Special Eurobarometer 359... 2011).

EMPLOYMENT RELATIONSHIPS

In recent years, the public has seen many problematic cases linked to an individual's privacy and employment relationships. Two of the more noteworthy cases from abroad: a woman posted in Twitter how she hated her job and her boss, to which the boss replied with a tweet "No worries. You're fired." (Dietrich 2013); a doctor's social media account contained an old photo of his student days, in which the doctor was drunk and hugged a strip-tease pole, which led to a patient filing a complaint (Sibicca & Wesson 2012). There was also a case in which a person in a leading position justified her absence from work with jury duty although her Facebook profile showed that she had been busy with much more entertaining activities (Slattery 2010). Of similar cases in Estonia, we can point out how customer representatives in a bank used Orkut and juice bar workers used Facebook to make fun of their customers (Šmutov 2007, Tigas 2013); how a nurse in the intensive care unit of Tartu University Hospital posted a photo on Facebook of a dying child and a description of her work (Puuraid 2012); or how an officer of the Defence Forces abused a soldier who died in Afghanistan on Facebook (Kaitseväe ohvitser sõimas... 2012). An employee of an Estonian company used the word "codenigger" („koodineeger") in his blog; a potential business partner from abroad was doing a background search, could not understand the context of the term used and ended the business relationship (Eslas & Koch 2012). Against the background of such cases, it is good to analyse how the private half of an employment relationship has become merged with the public half – employees have invaded the employer's privacy and vice versa. As we can see, many new situations that need to be regulated have emerged.

BACKGROUND CHECK WHEN APPLYING FOR A JOB. When a person applies for a job, there is a high probability that all the information that a person has publicly shared in social media reaches the employer, but in a context that was not originally planned (Nicolaisen

2010). Public posts in social media, blogs and e-mails have led to several cases in which the working life and the company's public image have suffered because of the private life of an employee (Umphress *et al*. 2013); therefore, we can see the constantly growing interest of recruiters and personnel managers in background checks conducted in online environments. About 70% of personnel managers who participated in the studies (Rosen 2010, Preston 2011) regularly claim that they use social media in the recruitment process and that they have rejected a candidate because of the information (inappropriate pictures, forum posts, etc.) that they unearthed during the background check on the Internet. On the other hand, a well-compiled self-presentation in social media, e.g., Facebook or LinkedIn, can actually help in finding a job (Siibak & Suder 2013).

In Estonia, this topic has been studied by Greete Kempel (2014), Eva-Liis Ivask (2013) and Katriin Visamaa (2012), who all found compelling evidence that Internet background checks of job applicants are common practice despite the fact that it might seem like an invasion of privacy. The most popular option is to look for additional information on a candidate on Facebook, but search engine (e.g., Google) results and other web environments are also checked. Applicants are not, as a rule, informed of the background check beforehand and their consent for this is not asked. Employers have listed the following as inappropriate social media use: rude language, uploading photos with sexual innuendo, party pictures, slander of the employer and colleagues, and leaking confidential work-related information (Kempel 2014). A rather usual situation is that colleagues (in spite of the power hierarchy in the organisation) are "friends" in social media environments. Tension arises when the friend request is sent by a superior or personnel manager, for example. Globally, there have been some extreme cases where during a job interview an applicant has been asked for his Facebook login data or to log in to his account and have the superior or recruiter look through it (van Dijck 2013, Roth *et al*. 2013).

LEGAL REGULATION. Kempel (2014) states that the legislation of the Republic of Estonia is not of much help in matters of social media: it does specify the term of "inviolability of private life" and provides that in case of any kind of processing of personal data the data subject has to be notified. However, anything related to social media has to be read between the lines, and there are many contradictory regulations. An employer should not process the personal data of an (potential) employee without the latter's consent, but without evidence and supervision it cannot be stopped (Siibak & Suder 2013).

BUSINESS RELATIONSHIPS

B2C COMMERCE: INTERNET AND CUSTOMER CARDS. When we speak about business relationships, we should distinguish between relationships that allow the provision of e-services and e-commerce (primarily online stores) and Internet content providers, primarily Facebook and Google. The Government Office held a survey in 2013, which showed that 86% of questioned Estonian citizens had purchased goods or services through e-channels (E-äri ja e-kaubanduse...2013); according to the Eurobarometer conducted last spring, 46% of Estonians aged 15 and older had bought something from the Internet in the past 12 months (Special Eurobarometer... 2013). TNS Emor study added a couple of percentage points to that result, reaching 49% (Voog 2014). In the case of e-commerce, people could be

encouraged by the fact that dissatisfied clients can submit complaints quickly and easily, and that the consumers have more power in business relationships than they used to, since entrepreneurs are afraid of negative experiences spreading in social media (Jasper & Waldhart 2013). However, we should not forget shops in the physical space, which also collect data about people. Stores widely use the system of customer cards and Estonians are avid users of such cards – 71% of Estonian respondents said that they use at least one customer card, while the European average indicator is considerably lower – 47% (Special Eurobarometer 359... 2011). On the basis of a person's **buying patterns**, we can learn a lot about him or her; one of the more drastic examples comes from the US, where the Target chain store used "predictive statistics" to analyse their customers' purchases and to learn who is probably in the last trimester of pregnancy, when their buying habits become more flexible (Duhigg 2012). In one instance, Target sent advertisements and vouchers for pregnancy and baby products to a young girl, and because of that other members of her family learned about her state. In public discussions, this case was viewed as an extreme invasion of privacy, even if companies like to stress that if an individual wants to protect his or her privacy (e.g., by limiting access to his or her information, restricting ways that he or her can be monitored, sharing minimum information, asserting the right to be left alone) he or her cannot enjoy personalised experiences at the same time (Titiriga 2011).

PERSONALISED RECOMMENDATIONS. Providers of different services are interested in making personalised recommendations. One of the most common options is behavioural targeting (Titiriga 2011), which could be described as making offers to masses based on stereotypes (choices and recommendations displayed in the web are influenced by sex, age, location, etc.). A great example is Google AdWords – it monitors what the user searches for and clicks on, and follows this to display different sponsored posts. The most efficient way to make recommendations is based on collaborative filtering recommendation system. If the probability of clicking on a Google AdWords link is 1% on average, then the more context-sensitive recommendation system that takes into account the user's (and his or her friends') profile raises the probability to 3-4% (Titiriga 2011), which is one of the main reasons for Google creating its own communication network, Google+.

REASONS FOR SHARING PERSONAL INFORMATION. Why should a person give out so much information about himself and his friends? In the case of business, we speak of perceived benefit or the **trade-off** between the service provider and consumer. The most common motivator for a trade-off is tied to the consumption of a product or service – to use a web environment one needs to disclose personal data. A step further – in order to use the service or product even more easily or efficiently, one needs to provide more information. Personalised web use is popular on social networks (Facebook, Instagram, Pinterest, etc.), where a user leaves a visible digital trace of his or her interests through friendships, likes, followings, recommendations and group memberships. The Eurobarometer study on privacy (Special Eurobarometer 359... 2011) shows that the most significant reason as to why people disclose personal information is to use a service in either a social network or e-commerce (61% and 79% respectively).

SPECIAL CASES OF MAJOR SERVICE PROVIDERS. Public attention has focused mainly on two Internet giants – Facebook and Google. Reproaches against Facebook are linked to disclosing private information to third parties without the users' informed consent (MacMillan

2010) – data has been given to commercial enterprises and advertising networks in order to profit from the information and offers made on the basis thereof (Youn 2009). We can also debate the aspect of "being informed"; when Google harmonised the privacy policies of its various services and platforms in 2012 and made significant changes to the conditions of use, the majority of people (90%) had no idea of any of this even though the information had been made freely available (Moscaritolo 2012). For people, the decision (whether you agree to the conditions of use or not) has been made easy – new conditions are applied even without the user's informed consent and this has made users more passive.

OTHER PEOPLE'S INFLUENCE ON AN INDIVIDUAL'S PUBLIC IMAGE

Besides the person him- or herself, the state, employment and business relations, an individual's privacy could be threatened by another person – a friend or an acquaintance. Katrin Laas-Mikko (2010) has emphasised that **privacy has a social nature**; that is, without other people privacy would hold no value. "Others" are active participants in the creation of our identity and image in new media environments. The most active role is, naturally, played by the person himself; users can create free profiles in different environments, to which they can add infinite photos and videos, their interests, contact data, political views, sexual preferences, relationship status and an abundance of other information. In photos and videos, you can tag the people depicted and such tagged images show up on those people's profiles; therefore, we can say that a person's Facebook image is a collective project to a certain extent. Researchers (Walther *et al*. 2008) have pointed out how problematic this is in relation to the formation of an image – a person does not have much control over what others post, though the posted content can potentially affect the image of the page owner. Even if the user does not upload photos of him partying, his friends can still do it and thereby endanger his privacy (McLaughlin & Vitak 2012).

INTERNET LITERACY AND PRIVACY. The violation of privacy can occur because of the individual's or other people's insufficient knowledge. Internet literacy includes many different skills (information search, critical evaluation of information, use of services, application of security settings, netiquette, involvement, etc.) but researchers think that civil education does not pay enough attention to this: "on the level of action, more attention has been paid to the creation of information technological infrastructure" (Runnel 2010). For regulators and legislators, it is easy to see the individual as responsible (for digital literacy as well as privacy) and people have adopted this point of view: in various privacy-invading situations, the active responsibility falls onto the person himself (Special Eurobarometer 359... 2011). Additionally, people have to consider that applicable privacy norms are never universal and therefore the violation of privacy in each case depends on a particular situation – what is public for one person is private for another (Siibak & Suder 2013) and as a rule these opposing points of view emerge in a conflict situation in which someone perceives that their privacy has been invaded.

POSSIBILITIES AND LIMITATIONS OF PROTECTING PRIVACY. When we speak of privacy in Europe, we speak about the right to be forgotten, or more specifically the *right to erasure* (European Parliament legislative... 2014); however, the efficiency of such a solution is doubtful as one of the basic characteristics of information on the Internet is its replicability. Information may already have spread in several ways and to many channels; for instance, a screenshot of a social media post with shameful content will be sent by members of the network to the pages that focus on such content, such as Lamebook or Failbook; from there the post is copied to various blogs, often automatically by a parasite page. Sometimes, the most curious cases end up in online news in the media of different countries and as an example in academic analyses, books and so on.

PRIVACY-RELATED ATTITUDES AND PRACTICES OF ESTONIANS IN COMPARISON TO EUROPEANS

As has been referred to earlier, 2011 saw the publication of a large-scale study that was conducted in the member states of the European Union and was unique in its thoroughness and comprehensiveness – the Eurobarometer on data protection and privacy (Special Eurobarometer 359... 2011). One of the motivators for carrying out our study was the fact that the Eurobarometer data were collected in 2010 and, in view of the privacy-related scandals and developments in the web in the meantime, we felt that there was a need for more up to date data. Below, we will highlight some of the more significant findings about Estonians in comparison to the rest of Europe.

Estonians consider the most private information to be the following (see Table 1): data on identification documents (personal code, ID-card and passport number), followed by medical information and financial data (above all, salary, credit card history and bank account details).

Table 1: What is considered private information – Estonia in comparison to the European average (data from Special Eurobarometer 359... 2011).

Area	Considered private in Estonia	Considered private in the EU on average
Personal code, ID-card and passport data	85%	73%
Medical information	81%	74%
Financial information	79%	75%
Fingerprints	66%	64%
Home address	58%	57%
Mobile phone number	54%	53%
Name	44%	46%
Photos of oneself	41%	48%
List of one's friends	22%	30%
Nationality	22%	26%
Work-related information	19%	30%
Personal opinions and preferences	19%	27%
Activities (hobbies, sports, places)	18%	25%
Visited web pages	18%	25%

The general rule is that **the higher the education and socio-economic status the more private Europeans consider their personal information to be**.

Privacy-related attitudes involve a lot of acceptance or passive subservience: 77% of Estonians agree to the claim that disclosing personal information is increasingly more important and common in modern life (European average is 72%); people also think that there is no escape from disclosing personal information if you wish to consume certain services and products (Estonia 54%, EU 58%). Additionally, 47% of Estonians do not consider the disclosure of personal information a problem at all; Europeans on average are

more cautious and distrustful – 33% of them did not see the disclosure of personal information as a problem.

Estonians are noticeable in their high level of trust in many questions: they trust the state as well as the public and private sectors, banks and Internet service providers more than the European average (see Figure 2).

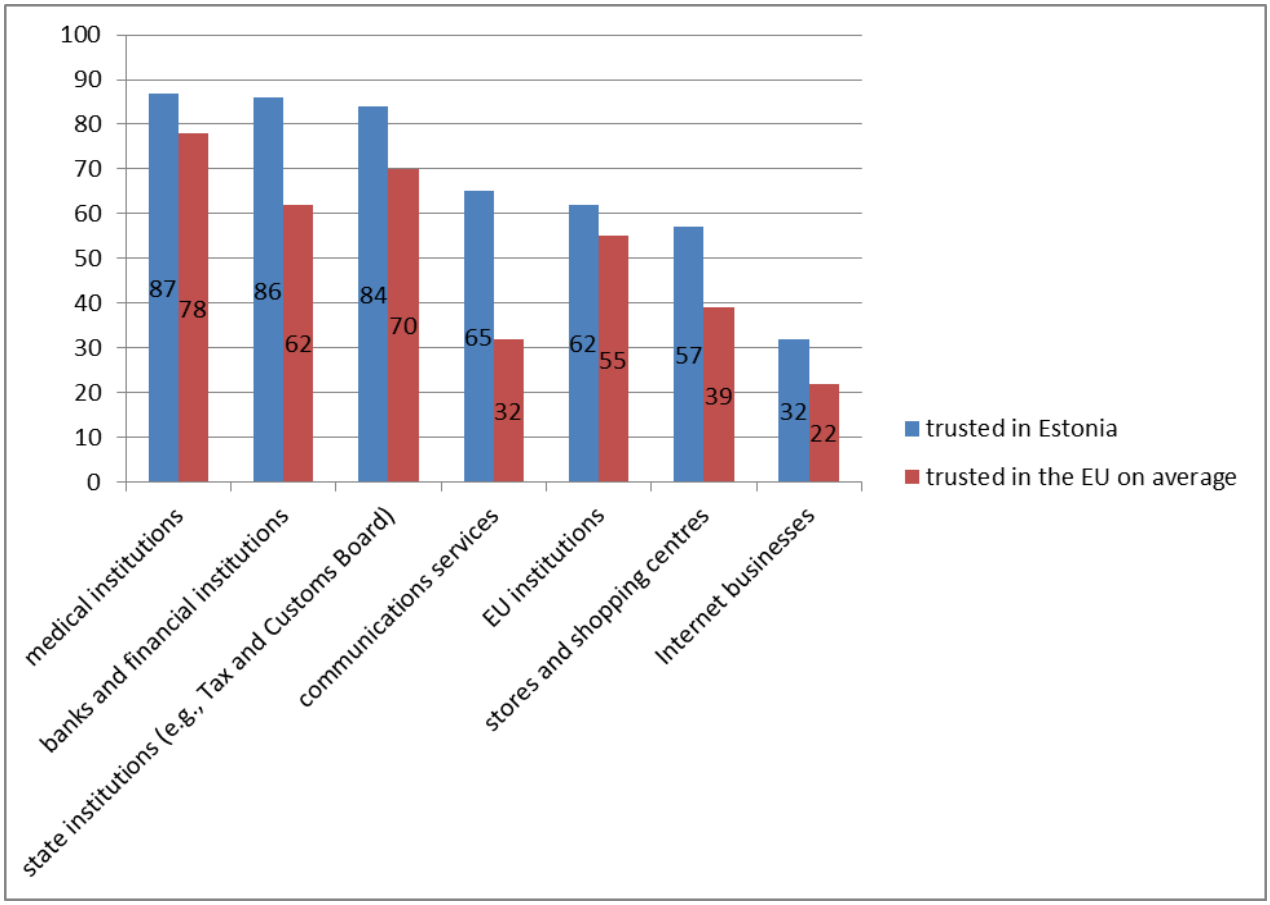

Figure 2: Trust in institutions in Estonia and in Europe on average (data from Special Eurobarometer 359… 2011).

In general, Estonians are less disturbed and worried than the rest of Europe about the collection and storage of their data (see Figure 3); in all the categories, Estonian indicators are approximately 15% lower than the European average. Likewise, our people do not worry about their data being used for other purposes than for what they were originally gathered (51% of Estonians are worried about that while in Europe the average is 70%); only the Swedes are more carefree than us in this respect.

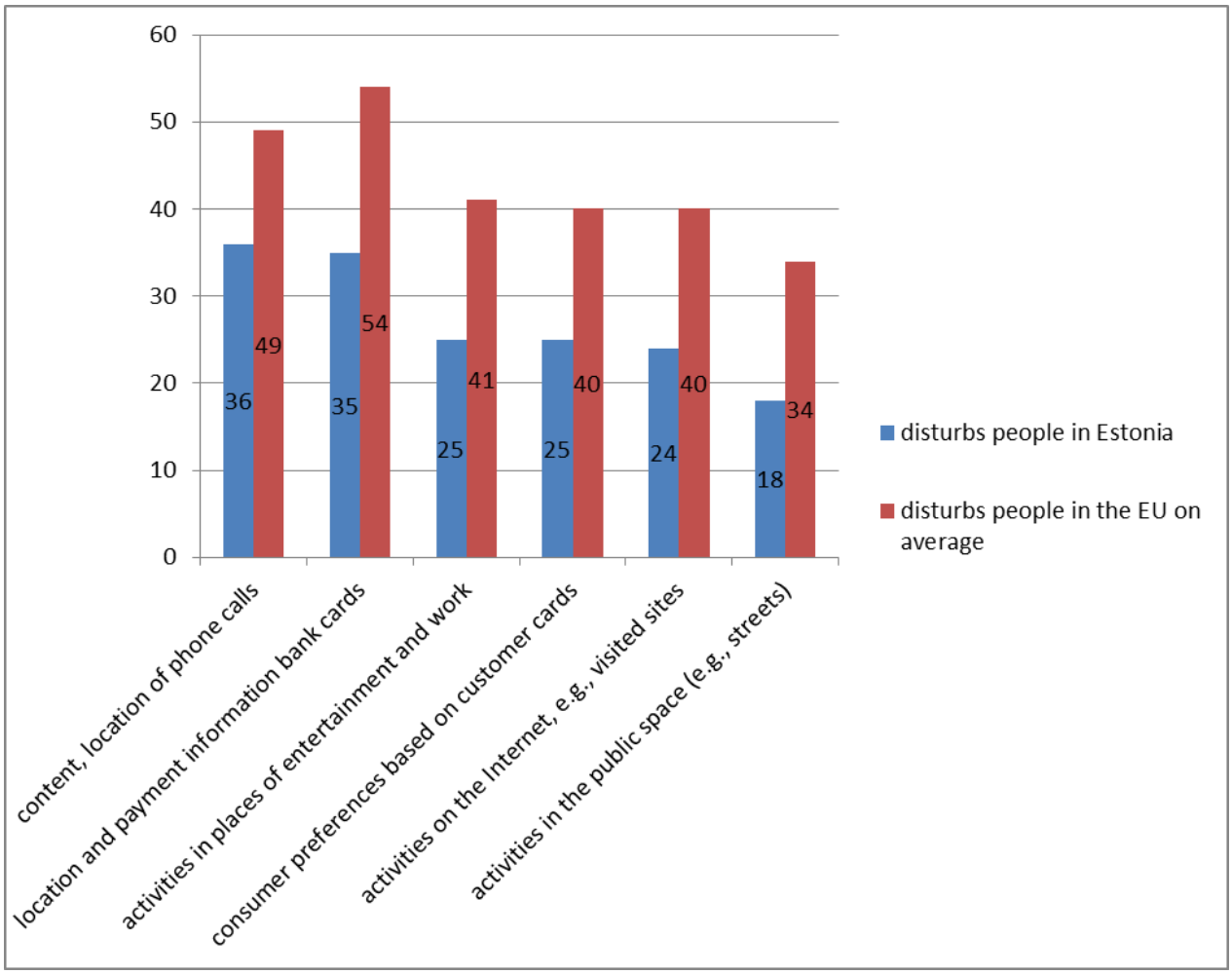

Figure 3: Estonians being disturbed about different activities being monitored in comparison to the European average (data from Special Eurobarometer 359... 2011).

Estonians use fewer strategies and tools to protect their privacy and identity than the European average (see Figure 4). Note that the options provided in the Eurobarometer study were limited and the list was incomplete. Nevertheless, it is obvious that Estonians claim to use mostly technical, not social, strategies and tools.

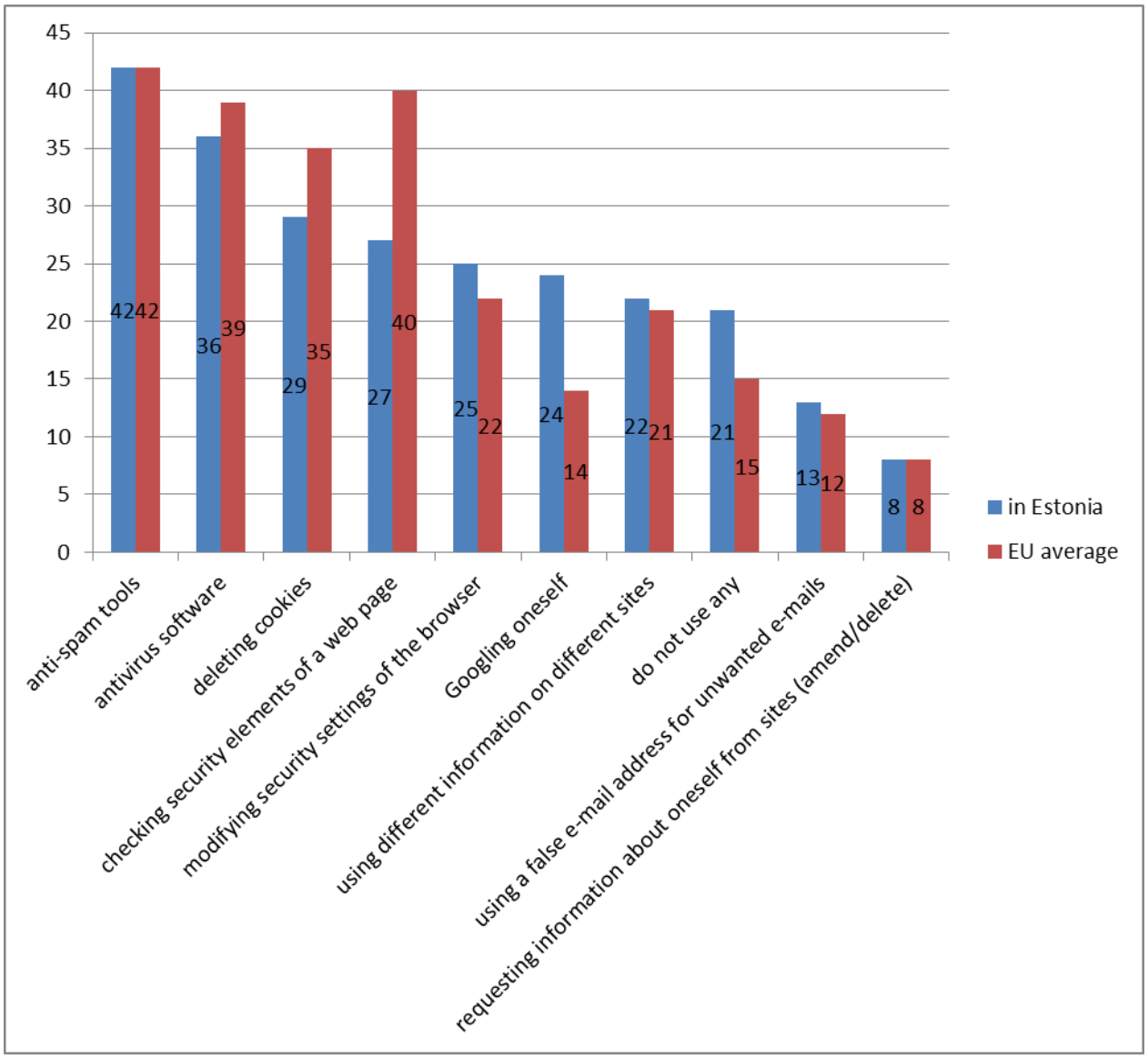

Figure 4: Strategies and tools that Estonians use to protect their identity (and privacy) on the Internet in comparison to the European average (data from Special Eurobarometer 359… 2011).

The questioned Europeans most often think that a person him- or herself is responsible for his or her information. A person's responsibility for the protection of his or her privacy is linked to awareness and consideration of one's activities. It is notable that the lack of necessary knowledge is admitted by Estonians more often than by Europeans on average. 54% of Estonians say that they read the terms of privacy and use of various services, which is close to the European average (58%), but a discrepancy becomes apparent with the option "I don't know where to find them" – Estonians gave that answer in 10% of the cases, which is the highest result among European countries (the European average was 5%). Estonian social media users are more active than Europeans in setting the privacy settings of different environments to their requirements (60% vs 51%) and they consider it relatively easy to do (90% of those Estonian social media users who have changed the settings; the EU average is 82%). Among those social media users who have not changed their privacy settings, Estonians once again rank the highest in Europe with the reply "I don't

know how to do this"; a big percentage of respondents also replied: "I did not know it was possible" (see Figure 5).

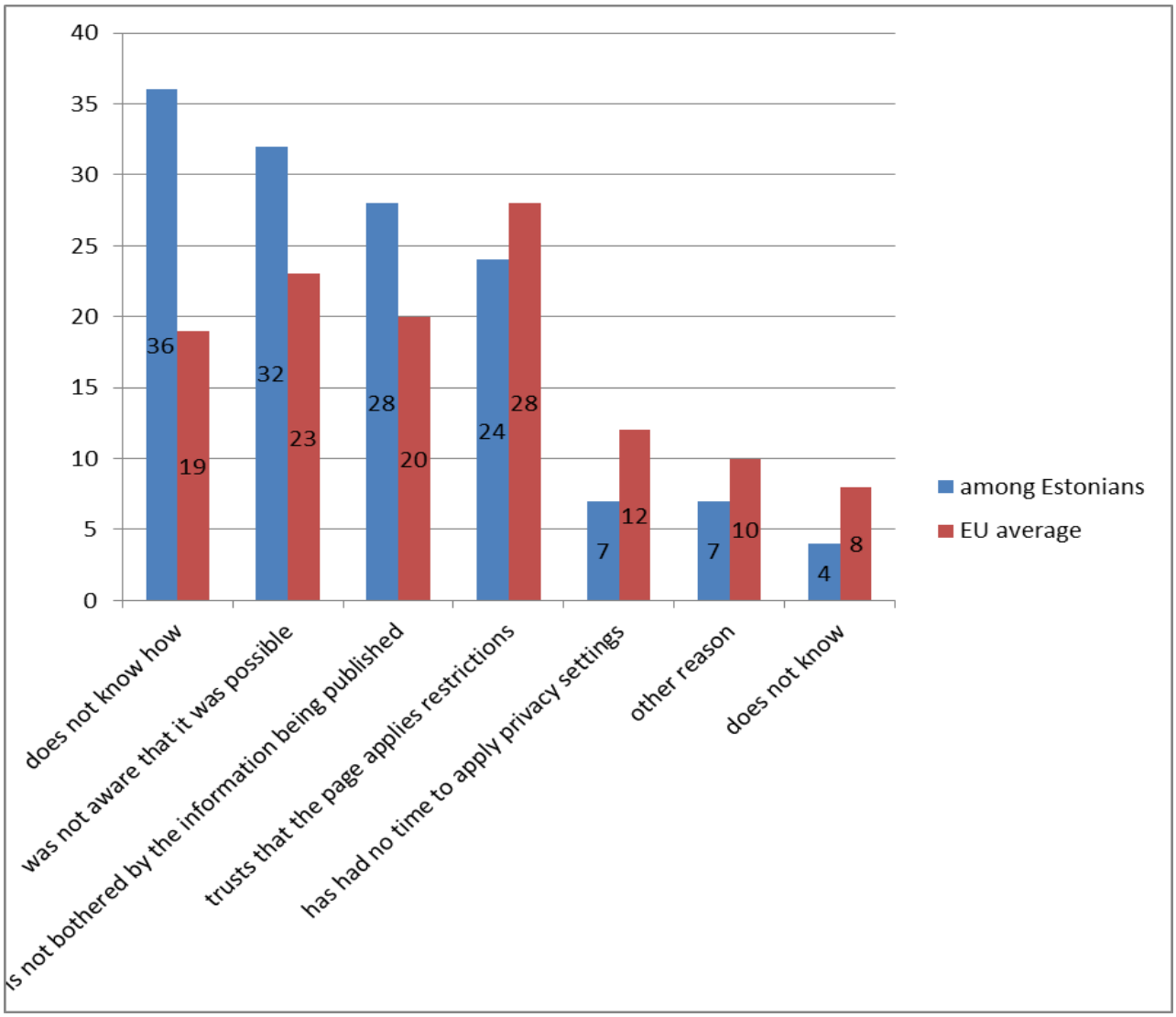

Figure 5: Reasons why privacy settings are not applied; comparison of Estonian and European average indicators among the social media users who have never changed privacy settings (data from Special Eurobarometer 359… 2011).

The results shown on the last Figure indicate how important it is, on the one hand, to raise individuals' digital literacy and competences, but on the other hand it shows that until these skills are limited it would not make sense to rely on the individual's responsibility.

CONCLUSION

The objective of this part of the study was to give an overview of the concept of privacy and related debates, to summarise possible violations of privacy in different contexts and to describe the attitudes of Estonians in comparison to the average European.

The study primarily focuses on informational privacy, which concerns the data collected, recorded and shared about a person. The concept of privacy is a complex notion that has given rise to many heated arguments. The right to privacy gives a person the right to decide who gets access to and to what extent, as well as the use of information concerning the said person. In the study, we look at what kind of situations are perceived by people as private and potentially privacy-invading. What is perceived as private depends on and is influenced by the context.

The rapid development of information and communication technologies has changed our everyday life: there are more usage possibilities, more mobility, more users, social rituals and routines. New media has mixed different, erstwhile separate audiences and contexts, blurring the borders between public and private life. At the same time, new technologies and environments create new solutions and enable different online strategies for retaining privacy, starting with moderate use and self-censoring and ending with more complicated strategies, such as social steganography and the use of multiple identities or pseudonyms.

Although some sceptics are of the opinion that "privacy is dead", the public and academic debates still emphasise the need to protect privacy. Why is it recommendable to protect privacy? There is no consensus in this matter. It is thought that the main task of privacy is to protect a person's autonomy and the formation of self-image. Privacy gives us the right to decide how to shape our lives and self-image and how to protect them from interference from other people. Privacy facilitates the establishment of socially meaningful relationships, as it makes it possible for social actors to draw a line between themselves and others, being thereby open or closed to social communication, depending on the context.

We have distinguished between the six main ways to violate privacy: insufficient informing, unpurposeful use of information, missing consent, security holes and information leaks, limited access to (own) data, and data collectors' lack of responsibility. The perception of privacy depends on the context and relationships that define the context. In the study, we looked at privacy-related problems in four distinct areas: 1) relationships between the state and the individual; 2) employment relations; 3) business relations and 4) relationships with other people.

We also highlighted some attitudes that characterise Estonians in comparison to the citizens of other European countries on the basis of earlier public opinion polls. In general, Estonians are less disturbed and worried about their data being gathered. The typical attitude of Estonians is one of acceptance or even passive subservience in relation to data disclosure. Estonians more often agree to the claim that disclosing information about oneself is increasingly more important in modern life. They also think that there is no escaping from disclosure if you want to use certain services and goods. Estonians are characterised by

above average trust in the state and private sector in relation to data processing. Similarly to Europeans in general, Estonians consider individuals to be responsible for the protection of their personal information. At the same time, more Estonians than Europeans admit that they lack the relevant skills to do this.

REFERENCES

1. Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, 13(3). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949
2. Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, California: Brooks/Cole.
3. Baghai, K. (2012). Privacy as a Human Right: A Sociological Theory. *Sociology*, 46(5), pp. 951–965.
4. Belanger, F. & Hiller, J. (2006). A Framework for E-Government: Privacy Implications. *Business Process Management Journal*, 12(1), pp. 48–60.
5. Bennett, C. J. (1971). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press.
6. Bovill, M. & Livingstone, S. (2001). Bedroom Culture and the Privatization of Media Use. Livingstone, S. and Bovill, M. (Ed.). *Children and their Changing Media Environment. A European Comparative Study*. New Jersey: Lawrence Erlbaum Associates, Inc. Pp. 113–140.
7. boyd, d. m. (2007). Social Network Sites: Public, Private, or What? *Knowledge Tree 13*. URL: http://www.zephoria.org/thoughts/archives/2007/05/07/social_network-3.html
8. boyd, d. m. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics*. Dissertation. University of California, Berkeley. URL: http://www.danah.org/papers/TakenOutOfContext.pdf
9. boyd, d. m. (2010). Social Steganography: Learning to Hide in Plain Sight. *danah boyd's blog,* 23 August. URL: http://dmlcentral.net/blog/danah-boyd/social-steganography-learning-hide-plain-sight
10. boyd, d. & Marwick, A. (2011). Social Steganography: Privacy in Networked Publics. *Presentation. International Communication Association Conference.* Boston, MA. URL: http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf
11. Brin, D. (1998). *The Transparent Society.* Reading, MA: Perseus Books.
12. Cooper, D. (2014). India Makes 'Liking' Blasphemous Content Illegal. *Engadget.com*, 22 August. URL: http://www.engadget.com/2014/08/22/india-censorship-blasphemy-laws-digital/
13. Craig, T. & Ludloff, M. E. (2011). *Privacy and Big Data: The Players, Regulators, and Stakeholders.* Sebastopol: O'Reilly Media.
14. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), pp. 319–340.
15. Dietrich, G. (2013). Social Media Policy: When Are Your Own Opinions Not Okay? *Social Media Today*, 26 September. URL: http://socialmediatoday.com/ginidietrich/1765916/social-media-policy-when-are-your-own-opinions-not-okay
16. van Dijck, J. (2013). You Have One Identity: Performing the Self on Facebook and LinkedIn. *Media, Culture & Society*. 35(2), pp. 199–215.
17. Duhigg, C. (2012). How Companies Learn Your Secrets. *The New York Times*, 16 February. URL: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp&pagewanted=all
18. Eslas, U. & Koch, T. (2012). Sõna «neeger» seadis ohtu tööpakkumise. *Postimees,* 1 November. URL: http://www.postimees.ee/1025662/sona-neeger-seadis-ohtu-toopakkumise
19. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P.A.O. & Toval, A. (2013). Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, 46(3), pp. 541–562.

20. Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison*. London, etc.: Penguin Books.
21. Fried, C. (1984). Privacy. Schoeman, F. D. (Ed.). *Philosophical Dimensions of Privacy: An Anthology.* Cambridge: Cambridge University Press, pp. 203–222.
22. Garfinkel, S. (2001). *Web Security, Privacy and Commerce*. Sebastopol, CA: O'Reilly.
23. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), pp. 421–471. URL: http://courses.ischool.berkeley.edu/i205/s10/readings/week11/gavison-privacy.pdf
24. Gross, H. (1967). The Concept of Privacy. *New York University Law Review*, 42, pp. 34–53.
25. Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N. & Müller, N. (2011). Aspects of Privacy for Electronic Health Records. *International Journal of Medical Informatics*, 80(2), pp. 26–31.
26. Hunt, K. (2013). China 'Employs 2 Million to Police Internet'. *CNN Asia*, 7 October. URL: http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/
27. Ivask, E-L. (2013). *Facebooki kasutamine tööle kandideerijate taustauuringu tegemisel teenindussektori asutuste näitel*. Bachelor's thesis, supervisor A. Siibak, Tartu University, Institute of Media and Communication. URL: http://dspace.utlib.ee/dspace/handle/10062/31312
28. Jasper, C. R. & Waldhart, P. (2013). Internet and Distance Channel Use and European Consumer Complaint Behavior. *The International Review of Retail, Distribution and Consumer Research*, 23(2), pp. 137–151.
29. Kalvet, T., Tiits, M. & Hinsberg, H. (2013). *E-teenuste kasutamise tulemuslikkus ja mõju*. Tallinn: Institute of Baltic Studies and Poliitikauuringute Keskus Praxis. URL: http://www.ibs.ee/et/publikatsioonid/item/116-e-teenuste-kasutamise-tulemuslikkus-ja-moju
30. Kempel, G. (2014). *Sotsiaalmeedia töösuhtes: tööandjate hinnangud ning kogemused*. Master's thesis, supervisor A. Siibak, Tartu University, Institute of Social Studies. URL: http://dspace.utlib.ee/dspace/handle/10062/42383
31. Kirkpatrick, M. (2010). Facebook's Zuckerberg Says the Age of Privacy is Over. *Readwrite*, 9 January. URL: http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php
32. Knibbs. K. (2013). In the Online Hunt for Criminals, Social Media is the Ultimate Snitch. *Digital Trends*, 13 July. URL: http://www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks/#!bNLp76
33. Kupfer, J. (1987). Privacy, Autonomy, and Self-concept. *American Philosophical Quarterly*, 24: 1, pp. 81–89.
34. Laas-Mikko, K. (2010). *Privaatsuse filosoofilise kontseptsiooni piiritlemine.* Master's thesis, supervisor M. Sutrop, Tartu University, Institute of Philosophy and Semiotics. URL: http://dspace.utlib.ee/dspace/bitstream/handle/10062/15048/laas-mikko_katrin.pdf?sequence=1
35. Larsen, M. C. (2007). 35 Perspectives on Online Social Networking. *Social Computing Magazine*, 5 July. URL: http://vbn.aau.dk/files/17515817/35_Perspectives_on_Online_Social_Networking_by_Malene_Charlotte_Larsen.pdf
36. Linaa Jensen, J. (2010). The Internet Omnopticon - Mutual Surveillance in Social Media. *Presentation. Internet Research 11.0: Sustainability, Participation, Action*. Gothenburg, Sweden, 19–21 October 2010.
37. McLaughlin, C. & Vitak, J. (2012). Norm Evolution and Violation on Facebook. *New Media Society*, 14(2), pp. 299–315.
38. MacMillan, D. (2010). Facebook's Washington Problem. *Businessweek*, 17 May, pp. 33–34.
39. Marwick, A. E., Murgia-Diaz, D. & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review). *Berkman Center Research Publication No. 2010–5; Harvard Public Law Working Paper No. 10–29*. URL: http://ssrn.com/abstract=1588163

40. Mathiesen, T. (1997). The Viewer Society: Michel Foucault's "Panopticon" Revisited. *Theoretical Criminology,* 1(2), pp. 215–234.
41. Mayes, T. (2011). We Have No Right to Be Forgotten Online. *The Guardian*, 18 March. URL: http://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet
42. Miller, A. R. (1971). The Assault on Privacy: Computers, Data Banks and Dossiers. Ann Arbor: University of Michigan Press.
43. Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, 39, pp. 411–428.
44. Moscaritolo, A. (2012). Most Users In the Dark About Google's New Privacy Policy. *PC Magazine*, February.
45. Nergi, A. (2013). Facebooki konto kaudu saab hinnata laenaja maksevõimet. *Eesti Päevaleht*, 8 May. URL: http://arileht.delfi.ee/news/uudised/facebooki-konto-kaudu-saab-hinnata-laenaja-maksevoimet.d?id=66090580
46. Nicolaisen, N. (2010). *Getting StartED with Netbooks*. New York: Springer.
47. Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17, pp. 559–596.
48. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(30), pp. 101–139.
49. Oolo, E. & Siibak, A. (2013). Performing for One's Imagined Audience: Social Steganography and Other Privacy Strategies of Estonian Teens on Networked Publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 7 (1). URL: http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501&article=7
50. Parksepp, A. (2014). Bigbank kasutab krediidianalüüsis Facebooki. *Majandus24.postimees.ee*, 12 August. URL: http://majandus24.postimees.ee/2885015/bigbank-kasutab-krediidianaluusis-facebooki
51. Post, R. (2001). Three Concepts of Privacy. *Georgetown Law Journal*, 89, pp. 2087–2089.
52. Preston, J. (2011). Social Media Becomes a New Job Hurdle. *The New York Times*, 21 July. URL: http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html
53. Puuraid, P. (2012). Haiglaõde riputas intensiivravile sattunud sureva lapse pildi Facebooki. *Eesti Päevaleht*, 28 June. URL: http://epl.delfi.ee/news/eesti/haiglaode-riputas-intensiivravile-sattunud-sureva-lapse-pildi-facebooki.d?id=64603328
54. Rachels, J. (1975). Why Privacy is Important? *Philosophy and Public Affairs*, 4, pp. 323–333.
55. Rebane. M. (2014). Google'it andmeid kustutama sundiva kohtuotsuse Eestis rakendamine võib olla keeruline. *ERR Uudised*, 18 May. URL: http://uudised.err.ee/v/eesti/8f7b6216-e0a6-4a91-be87-5eb644f76953
56. Rosen, J. (2004). The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. *Workshop, Florida State University web page*. URL: http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf
57. Rosen, J. (2010). The Web Means the End of Forgetting. *The New York Times*, 21 July. URL: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1
58. Roth, L. P., Bobko, P., van Iddekinge, C. H. & Thatcher, J. B. (2013). Social Media in Employee-Selection-Related Decisions: A Research Agenda for Uncharted Territory. *Journal of Management*, 20(10).
59. Runnel, P. (2010). Digitaalsest kirjaoskusest kodanikuaktiivsuseni. *Postimees*, 23 January. URL: http://arvamus.postimees.ee/215402/pille-runnel-digitaalsest-kirjaoskusest-kodanikuaktiivsuseni
60. Rössler, B. (2005). The Value of Privacy. Polity Press.
61. Schoeman, F. D. (1984). Privacy: Philosophical Dimensions of the Literature. Schoeman, F. D. (Ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1–34.
62. Sibicca, A. J. & Wesson, S. K. (2012). The Dermatologist and Social Media: The Challenges of Friending and Tweeting. Bercovitch, L. & C. Perlis (eds.*). Contemporary*

Ethics and Professionalism in Dermatology Dermatoethics. London: Springer. Pp. 77–83.
63. Siibak, A. & Murumaa, M. (2011). Exploring the 'Nothing to Hide' Paradox: Estonian Teens Experiences and Perceptions about Privacy Online*. Conference article. A Decade In Internet Time: OII Symposium on the Dynamics of the Internet and Society*, Oxford, 21–24 September. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1928498
64. Siibak, A. & Suder, S. (2013). Ülemus kui "suur vend". *Kommunikatsiooniajakiri Kaja*, 4, pp. 13–14.
65. Slattery, J. (2010). S.I. Woman Allegedly Faked Jury Duty to Take Vacation. *CBS New York*, 28 October. URL: http://newyork.cbslocal.com/2010/10/28/s-i-woman-allegedly-faked-jury-duty-to-take-vacation/
66. Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review,* 90, pp. 1087–1155. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103
67. Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 44, pp. 745–772. URL: http://ssrn.com/abstract=998565
68. Streitfeld, D. (2014). European Court Lets Users Erase Records on Web. *The New York Times*, 13 May. URL: http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html?_r=2
69. Šmutov, M. (2007). SEB Ühispanga töötajad mõnitasid räigelt kliente. *Postimees Online*, 8 February. URL: http://e24.postimees.ee/1628091/seb-uhispanga-tootajad-monitasid-raigelt-kliente
70. Steeves, Valerie (2009). Reclaiming the Social Value of Privacy. Kerr, I., Steeves, V. and Lucock, C. (eds.). *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. New York: Oxford University Press, pp. 191–208.
71. Teder, M. (2012). Kohtud saavad õiguse Facebookis inimesega ühendust võtta. *Postimees*, 25 March. URL: http://www.postimees.ee/783758/kohtud-saavad-oiguse-facebookis-inimesega-uhendust-votta
72. Tigas, K. (2013). Noored müüjad sõimavad Facebookis avalikult kliente! *Õhtuleht Online*, 6 November. URL: http://www.ohtuleht.ee/552584/noored-muujad-soimavad-facebookis-avalikult-kliente
73. Titiriga, R. (2011). Social Transparency through Recommendation Engines and Its Challenges: Looking Beyond Privacy. *Informatica Economica*, 15(4), pp. 147–155. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1944728
74. Umphress E. E., Tihanyi, L., Bierman, L. & Gogus, C.I. (2013). Personal Lives? The Effects of Nonwork Behaviors on Organizational Image. *Organizational Psychology Review*, 3(3), pp. 199–221.
75. Visamaa, K. (2012). *Veebipõhiste sotsiaalvõrgustike kasutamine töötajate värbamisel*. Bachelor's thesis, supervisor A. Siibak, Tartu University, Institute of Media and Communication. URL: http://dspace.utlib.ee/dspace/handle/10062/28010
76. Voog, A. (2014). Internetipoodidest ostmine on Eestis seni arvatust populaarsem. *Eesti Päevaleht*, 7 March. URL: http://kasulik.delfi.ee/news/uudised/internetipoodidest-ostmine-on-eestis-seni-arvatust-populaarsem.d?id=68188085
77. Walther, J. B., Van Der Heide, B., Kim, S. Y., Westerman, D. & S. Tom Tong. (2008). The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep? *Human Communication Research*. URL: https://www.msu.edu/~jwalther/vita/pubs/facebook_hcr.pdf
78. Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.
79. Wigan, M. R. & Clarke, R. (2013). Big Data's Big Unintended Consequences. *Computer*, 46(6), pp. 46–53.
80. Williams, B. (1973). Problems of the self. Cambridge: Cambridge University Press.
81. Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, 43(3),

pp. 389–418. URL: http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2009.01146.x/full
82. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (2014). *European Parliament*. URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN
83. E-äri ja e-kaubanduse kasutamine Eestis ja kasutamise laiendamise võimalused. (2013). *Government Office*. URL: http://www.itl.ee/static/files/37.Lopparuanne_-_E-ari_ja_e-kaubandus_1_6_avalik_2013.pdf
84. Index Blasts EU Court Ruling on "Right to be Forgotten". (2014). Index on Censorship, 13 May. URL: http://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/
85. Kaitseväe ohvitser sõimas Afganistanis hukkunud kaitseväelast (2012). *Delfi*, 13 August. URL: http://www.delfi.ee/news/paevauudised/eesti/kaitsevae-ohvitser-soimas-afganistanis-hukkunud-kaitsevaelast.d?id=64813704
86. Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega 2012. (2012). Ministry of Economic Affairs and Communications. URL: https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/uuring_kodanike_rahulolu_riigi_poolt_pakutavate_avalike_e-teenustega_2012_emor.pdf
87. Progress on EU data protection reform now irreversible following European Parliament vote. (12 March 2014). *Europa.eu press releases database*. URL: http://europa.eu/rapid/press-release_MEMO-14-186_et.htm
88. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. (2011). *European Commission*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
89. Special Eurobarometer 398: Internal market. (2013). *European Commission*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_398_en.pdf
90. Süsteemi turvalisus. (accessed in 2014). *Estonian e-health Foundation*. URL: http://www.e-tervis.ee/index.php/et/uudised/uudiste-arhiiv/48-eestikeelsed-kategooriad/sihtasutus/tervise-infosysteem/251-systeemi-turvalisus
91. Estonian Gene Bank of Tartu University. (accessed in 2014). *Estonian Gene Bank of Tartu University homepage*. URL: http://www.geenivaramu.ee/et/geenivaramust