INIMÕIGUSTE KESKUS
HUMAN RIGHTS CENTRE
ЦЕНТР ПО ПРАВАМ ЧЕЛОВЕКА

HUMAN RIGHTS, THE INFORMATION SOCIETY AND ESTONIA: A PRELIMINARY MAPPING

AUTHORS: KARI KÄSPER, LIINA RAJAVEER
TRANSLATED BY: KARI KÄSPER

ESTONIAN HUMAN RIGHTS CENTRE 2019

The mapping was completed thanks to the financial support from the Civil Liberties Union for Europe's "Digital Empowerment of Members" project, which is supported by the Ford Foundation. The mapping does not necessarily reflect the views of Liberties or the Ford Foundation.

Cover photo: Bernard Hermant, Unsplash

TABLE OF CONTENTS

INTRODUCTION

Estonia is known all over the world as a digital society. Estonia is indeed one of the most forward countries when it comes to e-governance, but the reputation is somewhat further than reality and the mantra of "move fast and break things" might no longer apply. Everywhere around the world, risks and challenges to human rights related to information technology are more and more recognised, especially after the revelations of the United States whistleblower Edward Snowden about the mass-surveillance by intelligence agencies and the Cambridge Analytica scandal, which concerned the use of Facebook micro-targeting to influence democratic decision-making (Brexit referendum in the United Kingdom, elections in the US and elsewhere). There is also a wider, more mature understanding forming that innovation is in its essence a matter of political choices and that the development direction of technologies can be directed with smart policies and laws.

Technology does not have specifically positive, negative or neutral impact. This is the same with the impact of information technology on human rights. New technologies like artificial intelligence or social media are a good opportunity to minimise human rights breaches, for example by eliminating the share of human biases in decision-making or by allowing to rapidly and easily share information about human rights violations. Privacy-enhancing technologies, encryption and anonymisation are spreading, which allows individuals to better protect their rights themselves. On the other hand, the rapid adoption of information technology solutions threatens human rights, by making it easier to violate rights using digital means or by crystallising and deepening the injustice that is already existing (such as when using artificial intelligence, the biases in historical data are not taken into account, or when it comes to incitement of hatred). All kinds of mass personal data processing are also a potentially severe breach of the rights to privacy and to data protection. Therefore, it is important that before information technology solutions are adopted, their potential impact on human rights is evaluated and negative impacts are mitigated.

Estonian Human Rights Centre investigated in autumn 2019 the impact of technology to human rights in Estonia. It is a preliminary mapping, which intended to get a better understanding of the digital rights topics, threats and possibilities in Estonia, an overview of the important actors in terms of people and institutions, to raise awareness of Estonian Human Rights Centre as a human rights advocate and centre of expertise, and to get a deeper understanding of three topics.

In the frames of the mapping, we looked through important documents, but the main emphasis was on group and individual discussions. We met with people who deal with digital

rights related topics both in the private sector as lawyers or entrepreneurs, in the public sector as officials responsible for policymaking or oversight. Civil society activists, researchers and a journalist also contributed. In total, we met with 19 individuals, who gave their view on the topic in semi-structured focus group or individual interviews. This mapping is based on the summaries of the interviews and separate desk research.

THE MAPPING OF TOPICS

THE MAPPING OF TOPICS

As an exercise to start the discussion, we offered a number of topics to the experts which they evaluated based on their relevance. General Data Protection Regulation (GDPR) related issues were considered most important: its full and proper implementation. Also, profiling and artificial intelligence solutions in the public sector were considered problematic. As an important topic, freedom of expression online was emphasised. For these three topics, we provide a more detailed overview in this mapping.

The other group was formed by topics such as mass-surveillance and the use of communications and other data by intelligence and security agencies, as well as profiling in the private sector. Face recognition was specifically pointed out as a technology that potentially severely breaches human rights. The digital divide and the exclusion and deprivation caused by this were already mentioned, with which there has been little action in Estonia.

Less relevant were: smart city solutions, smart border solutions, the use of drones for surveillance and cross-border cooperation of security authorities. It was mentioned that the topic of machine behaviour could create a conflict with universal rules and local customs and laws. For those topics, there is likely little knowledge in Estonia, or they were too narrow. It is possible that these topics were considered already covered by wider topics.

This mapping cannot by any means be considered comprehensive. The area of digital rights is rapidly developing and new issues can quickly appear and disappear. At the same time, it can be said that the same discussions came up in the mapping in Estonia that are also taking place in Europe and the rest of the world. In addition to those, there are topics that touch upon the specifics of Estonian e-governance, which other countries have less experience in, such as proactive public services that use profiling and artificial intelligence.

It is interesting that the main threat was seen in the actions of the state, the potential impact of private sector actors was not mentioned much. It can be related to the fact that the world-wide platforms of large corporations such as Google, Facebook, YouTube and Twitter that threaten human rights have not given special attention to Estonia and perhaps are also considered not something that could be handled by a small country like Estonia. Local companies are quite invisible in their activities when it comes to threatening digital rights, so the threats posed by them are not considered much.

THE SITUATION IN ESTONIA

“In Estonian digital area regulation, there is the habit to regulate things so that it is convenient for the state — a cyber-seal is attached so that a person would immediately forget about it.”

– an expert that took part in the focus group

THE SITUATION IN ESTONIA

PUBLIC DISCUSSIONS AND AWARENESS

There is a lack of informed discussion about the impact of technology on human rights. Its possible reasons are manifold: the issues are technical in nature and complex and there have not been a lot of efforts to clarify them. The area is relatively new and rapidly developing, so there are few experts and thought leaders who could discuss the issues in a way that the public can understand.

The wider public is not generally aware of the different topics related to digital rights. It can thus be said that many are excluded and deprived when it comes to this topic, which is caused by the digital divide. Many Estonians do not have enough knowledge and skills regarding technical solutions. It is more of a problem that many lack even the vocabulary and basic understanding to engage in discussions about these issues. Therefore, it is easy to spread fears and rumours, but this also raises questions about the democratic legitimacy of the decisions made in this area.

A separate grave issue is that information technology solutions make life easier for those who are not in vulnerable groups. More attention should be given to how to create IT-solutions in a way that reaches vulnerable groups better.

Individuals cannot protect their rights because of lack of awareness; they also do not frequently understand the value and need for human rights on the Internet. Usually, the false "I have nothing to hide" argument is followed when it comes to the Internet. Privacy is sometimes not considered even suitable to ask for online.

The topics are not considered frequently in the human rights frame, but usually are framed in other ways, such as cybersecurity. This is not necessarily bad, in case the rights of individuals are in an important place when talking about cybersecurity. In this context, the security authorities might be allies in terms of data protection, if the dangers of too wide access to personal data are emphasised. It is also true that the rights of individuals are sometimes viewed in a too negative context, for example, when it comes to data leaks.

The media also does not fulfil its usual role, in many cases because there are few journalists who are able to orientate well in the area. In the issues of data protection and privacy, the media might also have a self-interest to have as low protections as possible. On the other hand, technology journalists are usually also IT-enthusiasts and might not be interested in covering these topics in a way which limits the use of technologies. When the GDPR came into force, some in the private sector used the lack of awareness to spread fears and confusion and thus sell trainings or products.

"The digital world got started very slowly: there was an e-mail address and not much else. But then suddenly it grew like an explosion and suddenly was so foreign that it was impossible to adjust in peace.."

– an expert that took part in the focus group

It is a Catch-22 situation: among politicians there are few who support human rights in the digital field, because it is not a vote winner due to the disinterest and lack of awareness among the voters. This means that there is no motivation to change this for the better and there are no politicians or opinion-makers, who would explain these topics. Also, in Estonia, public authorities are generally well trusted, so there is a lack of concern that they could threaten human rights in some way.

One expert pointed out the differences of approach among the US and Europe. In the US media, there is quite an active discussion regarding the impact of digital issues on human rights, but there is no such discussion in Europe. This might be caused by the more active grassroots activism in the US.

A role could also be played by history. In Soviet Estonia, human rights were not respected, including the right to privacy. On the contrary: surveillance was pervasive and people were called upon to snitch about dissidents. The fact that human rights could in the same way be threatened by an independent and democratic Estonia, or even less, the private companies, is not considered likely. Also, for a small state, the understanding of private life might be different from larger countries where there is more anonymity.

PROMISING INITIATIVES TO PROTECT HUMAN RIGHTS

Many experts brought out the personal data tracker, which allows individuals to see who has accessed their data in the state portal. Unlike paper documents, for which no such records are generated. At the same time, it was found that the implementation of data tracking is different in different databases and there is often not much information about it: for example, the option to add or see a reason for accessing data is missing. Also, the traceability of data access is not, in itself, sufficient justification to start collecting personal data. There are circumstances when personal data should not be collected at all.

Accessibility of information and public services was also brought out, as something that empowers those left behind and worse off, as well as those with a disability. The money saved by the use of e-services allows to lower the fees on regular public services, which increases their availability.

Crypto parties are a good example during which people can learn how to protect their data: encrypt files, browse the web without surveillance, learn how to create strong passwords and so on.

Digital state has also increased transparency, which helps to prevent and discover potential corruption and to guarantee uniform application of laws.

LEADERS AND ACTORS

The experts were not very well able to name persons or institutions who can or could handle issues related to human rights and information technology: raising awareness or protecting the rights of individuals. There are statutory roles for Chancellor

“It would be good for the state if there was a partner that points out discrimination, profiling, engage in algorithm-critique.”

– an expert that took part in the focus group

“Dealing with data is a new social order. One thing, which I personally miss, is third sector data activism — people who use open data, do the same predictions as scientists and offer solutions to the society.”

– an expert that took part in the focus group

of Justice and Estonian Data Protection Inspectorate. From the state, the round table of legislative managers was given as an example of a place were debates take place among techno-optimists and -conservatives. From the ministries, the topic is more often dealt with by the Ministry of Economic Affairs and Communications and the Ministry of Justice.

The role of private companies was considered so far quite minimal, because Estonian technology companies rarely value ethical or human rights considerations. There are opportunities here to create economic incentives (new business opportunities, better reputation, more effective oversight), so that they take human rights more seriously. The private sector will show initiative only when not dealing with these issues becomes “painful” to them. At the same time, the private sector was seen as an important channel to reach individuals (customers, employees).

It was considered important to have closer and more wide-ranging cooperation between the data protection authority, other state institutions and civil society organisations to deal with gaps.

THE ROLE OF REGULATION

Almost all of the experts said that further regulation is not necessary, they hoped for some relief from adoption of new laws. It was emphasised that specific gaps in existing legal frameworks should be tackled, as and when these come up. Some of the experts also noted that laws are sometimes contradictory, which allows for multiple interpretations. Definitions should also be made

more uniform, as different laws use different terminology. The GDPR should be implemented and its actual and effective application guaranteed. The issue of renewal of communications data retention and usage laws was also considered important.

Instead of new laws, there is a need for ethical frameworks and general principles, which could be used when adopting new technologies. These exist in different human rights catalogues, such as the Constitution and other legal acts, but applying these to new technologies proves difficult. As an example of good practice, the initiative of the Ministry of Justice in drafting principles of ethical data processing was highlighted.

THE ROLE FOR CIVIL SOCIETY

Civil society organisations were mostly seen as those pointing out gaps and issues, gathering data about various related topics, and bringing them to the public. They could also be partners to the state and the private sector. It was also thought that civil society could lead quality, science-based discussions.

Today not many activists are seen in the Estonian civil society that could orientate well in the area of technology and data. The role of civil society organisations could be to join up and mobilise such activism.

The experts also mentioned that making complaints, giving advice and helping with litigation could be something that civil society organisations could do.

TOPIC 1

PROFILING AND THE STATE

“It is so cool to make yet another registry etc, instead of thinking that perhaps the result could be achieved in another way.”

– an expert that took part in the focus group

TOPIC 1: PROFILING AND THE STATE

The state uses profiling more and more, by cross-using personal data from different state databases. This is done in different situations, such as for proactive services, for analysis that supports policy-making, but also in the area of national security.

Proactive (also predictive) services are a new type of public services, which state institutions offer at their own initiative. This means that, as opposed to traditional public services which require the person to submit an application, this is no longer necessary. Proactive services are said to be useful, because they make it easier and less time-consuming to use public services. They function “invisibly” to the citizen and activate in case of specific life-events (such as the birth of a child).

According to the Principles for Managing Services and Governing Information, proactive public services are “the direct public services provided by an authority on its own initiative in accordance with the presumed will of persons and based on the data in the databases belonging to the state information system. Proactive services are provided automatically or with the consent of a person.” In Estonia there are still few such services, but there is a trend to make more use of them, especially using artificial intelligence.

As an example, the Social Insurance Board starts to offer automatic child birth benefits, which the parent just needs to accept. Proactive services are also planned by the Unemployment Insurance Fund for labour market services.

Topics such as big data and state databases concern more than just proactive public services. Experts also brought out the lack of oversight when it comes to state databases, especially when they are copied to “data silos”. It has also happened that information technology developments that might use personal data are already under development before the possibility has been “made legal” by law.

Profiling in the area of national/internal security is even more hidden and thus proper oversight over it is even more important.

OPPORTUNITIES AND THREATS

In terms of human rights, public services provided with the use of profiling could reach more people than before, especially those who might not have been aware of the possibility to use such a service. This presumes that the system is fully automatic in a way that does not require the consent or acceptance of a person. Even though such analysis does not exist, it is likely that marginalised groups have less access to public services. If profiling is used in a way that enables to bring public services to those who need them, but were left out previously, then this helps to protect the right to equal treatment.

“Should the state tell you that you should get new skills and retrain, or when to give blood tests. How proactive should the state be?”

– an expert that took part in the focus group

“IT solutions could amplify and make existing problems structural.”

– an expert that took part in the focus group

At the same time, any new dataset threatens the right to privacy and the right to data protection. Questions need to be answered, such as under which conditions and if a person could refuse a proactive service. Human autonomy and choice will be under threat.

The right not be discriminated could also be impacted by profiling, if the data that is used is incorrect or incomplete. Often, when profiling with the use of artificial intelligence, it is forgotten that historical data could already include bias, and biases could also be introduced by the programmer.

SOLUTIONS AND RECOMMENDATIONS

1. Create a holistic solution for the use of personal data by the state. In this solution, the citizen could easily and clearly see (by use of visualisation), which state services use their personal data and in which they could consent or refuse consent for data processing or object to automated processing. Private companies could also be added to this. In this way, everyone could get a “big picture” of the use of their personal data.

2. Analyse the use of any kind of decision-making that uses artificial intelligence from human rights perspective, by setting the goal that AI-assisted decision-making should decrease, not crystallise discrimination.

3. Ban profiling based on special categories of personal data for national security purposes.

4. Analyse the existing and planned databases in terms of compatibility with the principle of data minimisation.

TOPIC 2

APPLYING THE GDPR

TOPIC 2: APPLYING THE GDPR

The General Data Protection Regulation of the European Union became in force 25 May 2018. It brought new options for enforcing data protection rules and specified the existing rules. The GDPR is directly applicable, which means that Estonian law only regulates those aspects of data protection, which fall outside of the scope of the GDPR or which the GDPR enables to regulate in national law. The GDPR as an EU legal act has primacy over Estonian law.

At the same time, proper application of the GDPR has been problematic in Estonia and other countries.

First, the Estonian supervisory authority Estonian Data Protection Inspectorate is underfunded to fulfil the responsibilities it has according to the GDPR. It received no additional funding or staff compared to the situation prior to the GDPR coming into force, although the powers and competences were considerable expanded. The capacity of Estonian Data Protection Inspectorate to ensure effective oversight is therefore doubtful. The Estonian supervisory authority did not also have a properly appointed head during much of the period following the deadline for applying the GDPR.

On the other hand, GDPR required Estonia to review its current law. The implementing act of the Personal Data Protection Act,

"I think that the well informed and aware citizens are missing. Where the state cannot go, is the private sector, and for research - but in research activities ethical issues are doubtful."

– an expert that took part in the focus group

"The state listens to academic expertise, but there is no clarity with the GDPR, how to interpret it, fears of making decisions, by delegating it to the [data protection authority], which is not very interested, by delegating it to the ethics committee... There is very little knowledge by different institutions, there are still no practices of interpretation of GDPR in specific contexts. The data have moved forward, law is left behind."

– an expert that took part in the focus group

which entailed changes in large number of other laws and which applied both the GDPR and implemented the Police Directive, was rushed through the legislative process and without sufficient analysis. Most problematic might be the numerous exceptions made under Article 23 of the GDPR, which allow Member States to derogate from the GDPR for public order, public security and other reasons. At the same time, these derogations need to respect the essence of the fundamental rights and freedoms and be necessary and proportional in a democratic society.

Finally, the awareness of the GDPR is low in general, because the Estonian authorities have not fulfilled their obligation to raise awareness about the new rules among citizens and companies. Also, there are no CSOs in Estonia today which would actively work on effective application of the GDPR and thus help individuals to protect their rights. Article 80 of the GDPR enables such action.

Processing of personal data for research purposes also entails a high risk, and it is not clear today whether and to what extent it is in compliance with the GDPR. Although the GDPR allows as an exception to process personal data for statistics, historical and research purposes, there is a high risk that personal data that is used for research initially (such as mobile positioning data, gene and health data) is commercialised by companies attached to research institutions in ways which breach human rights. Such breaches are hidden, but with a potentially grave consequences, because they touch upon the most private

personal data. In addition to the use of public databases, private databases could be linked in this context.

OPPORTUNITIES AND THREATS

The GDPR is a leap forward in guaranteeing high level of protection of personal data. It is a possibility for both the public sector and companies to bring their activities into compliance with human rights and guarantee that information technology solutions respect privacy. This respect for the principles of data protection will, in turn, contribute to greater trust in information technology solutions which allow them to be adopted more widely and used more voluntarily. Therefore, the effective application of the GDPR protects the right to data protection and the linked right to privacy.

Effective application of personal data protection also has a positive effect on other human rights, such as the freedom of expression (the so-called chilling effect that comes with surveillance is prevented).

Effective application of the GDPR might at the same time need balancing with other human rights and somewhat limit the right to conduct a business or freedom of the media.

SOLUTIONS AND RECOMMENDATIONS

1. Review Estonian law in terms of compliance with the GDPR and follow the principle of data protection by default and by design.

2. Raise awareness about the rules of data protection in a broad and easy to understand way among entrepreneurs, public sector employees and citizens, by use of conferences, training programmes, public awareness campaigns and other activities.

3. Regulate more clearly and precisely the use of personal data for research purposes (for example using Codes of Conduct) and strengthen the supervision over the use of sufficient safeguards.

4. Create a funding mechanism for civil society organisations, with which they could assist with the effective implementation of the GDPR, including by representing data subjects in judicial proceedings according to Article 80.

TOPIC 3

FREEDOM OF EXPRESSION ONLINE

TOPIC 3: FREEDOM OF EXPRESSION ONLINE

One of the bigger challenges in the area of digital rights is to ensure freedom of expression in social media in a way that does not at the same time increase the spread of false information, terrorism, abuse of children or incitement to hatred.

On the one hand, social media platforms have created extraordinary possibilities to communicate with each other and to be in constant contact with persons who might live thousands of kilometres away. They have helped people to organise, and established and helped to promote business activities. The level of access to information and its scope has become extremely far-reaching.

Social media platforms have not done enough to ensure that rules are followed on their platforms. Facebook has been accused of helping the genocide of Rohingya in Myanmar. Facebook, Twitter, YouTube and others give a platform without distinction to those, whose objectives undermine human rights.

Further issue is the outsourcing of human rights related decision-making to big corporations such as Facebook and Google, which consider their reputation and business most important, not human rights of the users. Only a handful of giant corporations, mostly headquartered in the US, control the platforms where most people use their freedom of expression. They have an enormous power to silence or amplify voices.

Currently, the removal of inappropriate content takes place with the help of tens and tens of thousands of workers, who review the notifications made by the users and either remove or not according to internal rules of the companies. These rules might be or appear to be discriminatory or unfair because of lack of clear criteria. On the one hand, they need to check the compliance with their own terms, but also with the legal requirements in the jurisdictions where their platforms are used, and, finally, also with universal human rights norms.

OPPORTUNITIES AND THREATS

Social media has created new opportunities to use freedom of expression, also for freedom of association and access to information. It is possible to react easily and quickly to human rights violations.

Social media threatens the right to life, freedom and security, when it enables spreading of terrorist content, sexual abuse of

children, incitement to genocide or hatred. The rights to health and fair working conditions are also threatened, because working as a content moderator might not be good for mental health. The right to equal treatment might also be impacted negatively.

SOLUTIONS AND RECOMMENDATIONS

1. Turn more attention to how well social media platforms comply with human rights. Use the means that other countries have done to pressure the platforms to comply with human rights, the Constitution and other laws.

2. Raise awareness about the threats of use of social media and ways to protect themselves, especially among youth and children.

"If we want to improve the situation, then using the example of medical metaphors, we should give simple recommendations (not to train everyone to be immunologists, but to advise to wash hands). Very practical recommendations should come first, then human rights, then technical side."

– an expert that took part in the focus group

SOLUTIONS AND IDEAS TO RAISE AWARENESS

There were also many good ideas to raise awareness and protect human rights in the digital rights area.

Ideas to raise awareness:

- information campaigns in a simple language and using stories that use a visual language and are not about prohibitions or directives, but about positive stories.
- articles and stories in non-traditional places, such as women's journals
- talk about these topics already starting from basic education
- MOOC for high school students (already planned)
- "change your password day"
- the need for an alternative narrative
- disseminate open source platforms, use "fair trade" technologies
- create simple software bundles for use by people
- recognise ethical companies that respect human rights and shame those that do not

ESTONIAN HUMAN RIGHTS CENTRE AND DIGITAL RIGHTS

Estonian Human Rights Centre is an independent non-governmental human rights advocacy organisation with a mission to work with supporters for Estonia that respect everyone's human rights. By 2020, Estonian Human Rights Centre is the influential and competent leader of Estonian non-governmental human rights movement.

EHRC develops its activities according to the needs of the society. Our focus is currently on the advancement of equal treatment of minority groups and diversity & inclusion and the human rights of asylum seekers and refugees. EHRC coordinates the Estonian Diversity Charter. We also monitor the overall human rights situation in Estonia and publish bi-annual independent human rights reports about the situation in Estonia. We are NGO partner for UNHCR (the UN Refugee Agency) in Estonia.

EHRC activities in the area of digital rights have so far been limited, but this mapping is the first step to finding ways for strategic interventions.

Since 2014, we have been intermittently working with the issue of communications data retention. We have studied the situation and repeatedly asked for information from different authorities and companies in order to get a better overview of the issue. We have asked the Estonian government to stop illegal retention obligations and regulate the use of communication data more clearly and precisely. Partly because of our work, the Ministry of Justice initiated at the end of 2018 the drafting process for amendments to the current regulation.

We have also worked with the Civil Liberties Union for Europe on the issue of behavioural advertising on the Internet, on which we submitted together with other human rights organisations complaints to data protection authorities (in Estonia, the Estonian Data Protection Inspectorate) to start investigation into the compliance of behavioural advertising with data protection rules.

In order to limit hate speech online, we work with the European Commission and social media platforms to regularly monitor the process of removal of illegal content which incites hatred. In addition, we are partners in the project Op-Code, which aims to broaden and strengthen the coalition of civil society organisations working systematically on monitoring online hate speech, and to develop open source solutions that allow to moderate hateful content.

We have also covered technology related issues in our human rights reports "Human Rights in Estonia," especially in chapters that deal with protection of private life.

Support the activities of the Estonian Human Rights Centre on our website:

https://humanrights.ee/en/act-now/donate/

ESTONIAN HUMAN RIGHTS CENTRE 2019