Rule of law in Cyberspace – focusing on police methods to detect and investigate crime in digital networks

1. The content of rule of law in Cyberspace

The classical and basic idea in legal theory has been that the government shall be ruled by the law and subject to it.[1] The purpose of the rule of law has been "to make it possible to foresee with fair certainty how the authority will use its coercive powers in given circumstances, and plan one's individual affairs on the basis of this knowledge".[2]

This implies that the rule of law also should impose limitations and obligations on the powers of how the police enforce law in nations governed by the rule of law. Common for the different notions of the rule of law is that they were developed in a world where the citizens in most cases interacted directly with each other and where crimes were committed within one national jurisdiction. The rule of law protects typically the citizen against infringements of their fundamental human rights, from arbitrariness and misuse of power.[3] The exact limits and content of the rule of law will tend to vary between the national jurisdictions.

The closest we get to a common understanding of the rule of law is probably the regulations in the international law and international human rights, at least on an abstract level. An example of content not different from what initially described as the rule of law is article 17 in the International Covenant on Civil and Political rights states in article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." Article 6 in the European Convention of Human rights gives everyone, in the determination of his civil rights and obligations or of any criminal charge against him, the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal, while judgments. These are two examples of codification of the rule of law. The project will concentrate on the latter aspect; the principle of accountability, i.e. to hold someone responsible for interventions. An important question is to understand how the European Court of Human Rights interprets the principle in its case law.

2. The operationalization of the rule of law in Cyber Space

The project is intended to focus on whether the rule of law can and should be applied on cyberspace. Cyberspace can be defined as "the interactional space or envi-

[1] The rule of law and its virtue, Joseph Raz, 1977
[2] The Road to Serfdom (London, 1944) p. 54, F.A. Hayek
[3] Rettsfilosofi (Oslo,2007), Svein Eng

adfa, p. 1, 2011.

ronment created by linking computers together into a communication network."[4] Cyberspace differs from the world where the rule of law was developed. Inter alia can cyberspace be viewed as "anti-spatial" i.e. the interaction between computers in digital networks makes it difficult to locate different physical locations.[5] Another difference is for example that the communication might not be between living organisms, but between computers.[6]

The project will be based on the rule of law, as applied and operationalized by the police in relation to law enforcement in cyber space for the purpose of preventing and investigating crime connected to financial transactions. To be able to this the project will use the principle of holding the state accountable as a tool. Does this tool contribute to the protection of the individuals when analyzing policing on financial transactions? When implementing new measures as the Data Retention Directive it was discussed how to operationalize privacy concerns.[7] However the rule of law has not to the same extent been discussed when operationalizing measures. A relevant question is whether privacy concerns are enough when developing algorithms to collect data in cyberspace. Hopefully the research can find the nexus between the rule of law and algorithmic accountability when collecting data from a financial transaction. Software and algorithms to enforce law on in digital networks might have biases. They might be unjust. Who and how do we hold someone responsible for the mistakes made by the state but operationalized through software and algorithms?

3. The relationship between privacy concerns and the rule of law

When analyzing how to handle cyber risks it's common to build the assessment on the relationship between the interests of privacy and the governments need for effectiveness in its protection of its subjects. An important question to ask is whether privacy is enough? Do we need the rule of law in addition to measures to protect the privacy of the citizens?

The concept of due process of law is often stated on a principle level as a requirement to the decisions made by official authorities.[8] However, firstly, it might not be clear how the concept is applied on a specific measure. E.g. when the police will seize and inspect a very large volume of data, how can a court decision where the judge is supposed to review the material be operationalized? Secondly, it might not be clear whether the application fulfill its purpose. Some researchers have claimed that the judicial control just gives legitimacy to the authorities and there is often no reality in the control of the authorities.

My hypothesis is that research and studies have mainly focused on privacy issues for the citizens when implementing measures the police are using to collect infor-

[4] Cybercrime and Society, second edition (London, 2013), Majid Yar
[5] Mithcell, W.J. (1995) City of Bits: Space, Place and Infobahn. Cambridge, MA: Mit Press
[6] Datakriminalitet (Bergen,2016) p. 15, Inger Marie Sunde
[7] Prop. 49 L for 2010-11
[8] NOU 2009:15 Skjult informasjon – åpen kontroll DEL II og NOU 2015:13 Digital sårbarhet – sikkert samfunn kap 3.1

mation from cyberspace to investigate crime. The objective of this article is first of all to explore this hypothesis and eventually see, using juridical dogmatic methods, if the concept of the rule of law i.e. the principle of holding the state accountable for interventions can contribute to the understanding of what tools the police can use to investigate crime related to financial transactions in cyberspace in an efficient way. If the principle has a contribution to the protection of the individual and to a just investigation, the project will explore how this contribution can be operationalized in the surveillance and investigating measures in the financial sector of cyberspace.

4. Collecting information from third parties like FinanceCERT

To investigate efficiently in cyberspace, the police need to cooperate with third parties which are experts in the field that is investigated. In the financial marked FinanceCERT (Finance Computer Emergency Response Team) is a nonprofit stock company established in 2013 to handle the surveillance and the cyber risks in the financial sector.[9] It is owned by Finance Norway.[10]

To a large extent the effectiveness of the legal guarantees hinges on actual technical design and implementation, information flow and reporting procedures, oversight and control mechanisms etc. implemented. Interesting questions for the research is to understand what information FinanceCERT possess and what tools they use to collect it. At the outset technical monitoring and surveillance measures are implemented on the digital network in order to maintain security and prevent crime by third parties like the FinanceCERT who is in the position to do so. FinanceCERT is in dialogue with external contacts from the national and supranational authorities. Such actors are inter alia NorCERT and other regulators (ie. FSA) and public controllers. In addition FinanceCERT is in dialogue with contacts in the financial sectors (ie. Banks, insurance companies and Bank ID). The law enforcement must connect to the measures and get information pursuant to access provided by such third parties. This may lead to unclear attribution of responsibility and accountability seen from a rule of law point of view. Hopefully the findings can be operationalized into how the police can interact with third parties like FinanceCERT to police financial transactions in an efficient way that protect the individuals from abuse from the state.

5. The vulnerability of financial transactions

The committee of Digital Vulnerability in Society has identified several challenges related to the way transactions are performed today, both for private persons and the financial sector. The committee concludes that the sector has a high conscience of the potential risks compared to other sectors. However the services for financial transac-

[9] NOU 2015:13 Digital sårbarhet – sikkert samfunn side 170

[10] Finance Norway is the industry organisation for the financial industry in Norway. See www.finansnorge.no

tions are developing quickly. Both effectiveness and user-friendliness are important drivers. The most practical solutions might be beyond national control. This implies that financial institutions in the future might be involved in developing solutions that are more vulnerable. This means that the risks to perform financial transactions in cyberspace might increase while the individuals at the same time will be more and more dependent on these transactions. For the police to do surveillance to prevent crime and to investigate crime the measures to collect information need to steadily increase in effectiveness. In order to develop software and algorithms that are not only effective, but also protect the individuals, it is important to ask the right legal questions at an early stage when starting to build the tools. To be able to this it is interesting to understand the actors in the financial sectors and how the monitoring of the financial transactions can protect the citizens in reasonable way, both the victims of the crime and the people under police investigation.