TALLINN UNIVERISTY OF TEHCNOLOGY
School of Business and Governance
Department of law

Markus van der Ende

DRONES AND PRIVACY

Master's thesis

Programme HAJM08/15 - Law, specialisation European Union and international law

Supervisor: Katrin Nyman-Metcalf, Adjunct Professor

Tallinn 2019

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 20800 words from the introduction to the end of summary.

Markus van der Ende ……
(signature, date)
Student code: 156490HAJM
Student e-mail address: vanderende.markus@gmail.com

Supervisor: Katrin Nyman-Metcalf:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee: / to be added only for graduation theses /
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

This master's thesis discuss about consumer camera drones and privacy. The research questions are "What kind of privacy issues are drones causing and are the issues covered by law?" and "Are there any measures how to ensure privacy concerning drones?" There are few main privacy issues that drones are causing and these are the use of different recognition devices and software's to recognise specific persons, tracking and recording persons without their consent. Most of these are found out to be covered by law in but not exactly regarding drones. The drone filming and surveillance is a relatively new thing and the laws and regulations are few steps behind the development of the drones. At the moment of writing this master's thesis, many new laws are under reviews and there are plans of new regulations by the EU and the Finnish authorities. The authorities are regulated relatively well in Finland what it comes to use of drones and surveillance, but the consumers and other private drone flyers and regulated very loosely if at all. The main regulations and laws concerning drones are mostly about flying it. The privacy issues the drones are causing cannot be totally being handled with laws and regulations, but needs also technical measures to be able to ensure the privacy because there are persons who do not follow the laws and regulations. Furthermore, if the authority use of drones is not regulated, it can cause threats to privacy in the future in EU and Finland.

Keywords: drone, privacy, surveillance, facial recognition

LIST OF ABBREVIATIONS

ATM	Air Traffic Management
CAA	Civil Aviation Authority (UK)
CCTV	Closed-circuit television
EEA	European Economic Area
EU	European Union
FAA	Federal Aviation Administration
GDPR	the European General Data Protection Regulation
GEO	Geospatial Environment Online
GPS	Global Position System
MAV	Micro Aerial Vehicle
MTOM	Maximum Takeoff Mass
POW	Prisoners of War
ROA	Remotely Operated Aircraft
RPAS	Remotely piloted aircraft systems
RPV	Remotely Piloted Vehicle
SCS	Social Credit Score
SESAR	The Single European Sky ATM Research
SUPO	Safety Police
TRAFI	Finnish Transport Safety Agency
UAV	Unmanned Aerial vehicle
UMA	Unmanned aircraft

1. INTRODUCTION

Flying has always been one of the biggest dreams of the human, but being able to fly an air vehicle safely from the ground is in many cases more convenient and safer. After the invention of the motor driven air plane, also the UAVs (unmanned aerial vehicles), ROAs (Remotely Operated Aircrafts), UMAs (unmanned aircrafts), RPASs (remotely piloted aircraft systems) or drones as we know them better, have been developed slowly from unstable big air vehicles to small precise and technically advanced drones. The early stage flying drones has been used since 1918 mostly for military purposes such as surveillance, targeting and bombing.[1] The first commercial drone with four propellers as most of the non-military drones has, was designed in 1991, but the first commercial drone was sold first in 1999 with a $350 price tag.[2] From the first consumer drone it took around 10 years before they started to be more common. Since 2010, the camera drones have become popular and during the last years the amount of civilian used drones has grown with an exponential speed. In Finland it is estimated to be tens of thousands of drones in 2017. The authorities do not know how many drones there are in Finland, because there is no mandatory registration for the drones that are under 25kg.[3] In the USA the authorities made it mandatory to register civilian drones starting from December 2015, and between January 2016 and March 2017, 770,000 drones were registered. The Federal Aviation Administration (FAA) estimated in 2017 that the amount of drones will increase from around 1,1 million drones to about 3,5 million drones by 2021.[4] The increase of civilian used drones is not a simple thing and authorities in Europe, USA and other places are trying to draft new rules and laws concerning civilian drone flying. The drone flying is not the only issue and the question about privacy is also a big concern.[5] The drones have good cameras and other censors and can take sharp pictures from a long distance. Furthermore, also facial recognition can be used in drones and this is one reason why the privacy concerns have to be taken seriously. There is a wide range of drones in different sizes, prices and with different features. There is almost for everyone a drone that meets the needs. For civilians the drones are usually equipped with a camera to take aerial footage and

[1] Sullivan, J. M.. (2006) "Evolution or Revolution? The rise of UAVs", IEEE Technology and Society Magazine, vol. 25, no. 3, pp. 43-44. Accessible: https://ieeexplore.ieee.org/abstract/document/1700021
[2] Drone, Object lessons series, Adam Rothstein, Bloomsbury Academic, Jan. 29, 2015, pp. 37
[3] STT, Yle News 18.7.2017. Suomessa on arviolta kymmeniä tuhansia droneja - EU kiristää Suomen löyhää lennokkilainsäädäntöä. Accessible: https://yle.fi/uutiset/3-9727680 (8.3.2019)
[4] CNN (Cable News Network), U.S. drone registrations skyrocket to 770,000, 28.3.2017, https://money.cnn.com/2017/03/28/technology/us-drone-registrations/index.html
[5] Luppicinia, R., Sob, A.. A technoethical review of commercial drone use in the context of governance, ethics, and privacy, Rocci Luppicinia, Technology in Society
Volume 46, August 2016, Pages 109-119, pp. 109-111

it has become very popular whereas for companies and authorities there are more heavy-duty drones that can be equipped with different sensors or carry other equipment to places where it has earlier been difficult or impossible to take them. One of the privacy concerns is surveillance, and to be more precise, drone surveillance. This kind of surveillance with drones can pose a threat to privacy when drones are flying high above the streets and filming citizens without their knowledge.

This master thesis will go through different questions about privacy and drones. The author will concentrate to discuss how the privacy is affected by the drones used by authorities, mostly the police, and is the civilian drones also a threat to privacy and how the law sees the filming with drones. Moreover, there is also discussion about possibilities to ensure privacy or if it is possible and is the European and Finnish law up to date regarding drones and privacy? The current situation is taken into account and the future and upcoming laws and regulations are discussed and how they will influence the drones. This master's thesis leaves the military drones outside the discussion because it is more of an international law matter and the purpose of military drones and consumer / commercial drones is totally different. Even though the military drones are left outside the discussion, it is necessary in some degree to talk about them for the reason that military industry has driven the development of drones, and there are some aspects that have to be taken into consideration even if it is not in the focus. These are e.g. different kind of surveillance such as facial recognition. Furthermore, the governments, police and other authorities can use downgraded military drones for surveillance in areas where large areas have to be covered.

Because the new technology and new phenomenon of drones, we are not yet familiar with all the possibilities they can bring or how to be able to control the increasing drone flying. This is also one topic that will be discussed because it is important to get a good picture of the subject to be able to determine how to regulate the drone to ensure the safety and privacy, but also how the authorities can protect citizens from illicit recording or in worst case, against terror attacks. Because the drones are new, there are still many questions regarding the safety and privacy and this master's thesis tries to find the answers to these questions. Some of the issues are probably going to need further research, because there are new laws and regulations under review, and they will probably not be passed during the writing of this master's thesis.

1.1 Aims and research question

The development of drones has been fast during the last decade but now it is developing at an accelerating speed and when the technology is developed further, there are endless possibilities how to use drones. When cameras, GPS (Global Position System), facial recognition and other features are inserted to the drones it may create a threat to privacy and even health and life. The facial recognition is developing even faster than the drone industry and drones combined with facial recognition raises a lot of questions and concerns about privacy. The aim of this master thesis is to research the privacy issues with drones in Finland and EU and how the legislation sees it now and how the legislation may be developed and changed to meet the new challenges with drones. Furthermore this master's thesis tries to come with possible proposals how to ensure the privacy with the drones. There are few main points that will be discussed in more detail and these are the facial recognition, illicit recording and storing and processing the collected data. Even though this master's thesis is focusing on Finland and EU, there will be examples and discussion also from other countries, but the main research area will be Finland and EU.

The research questions are:
What kind of privacy issues are drones causing and are the issues covered by law?
Are there any measures how to ensure privacy concerning drones?

1.2 Methodology

To this master's thesis was used empirical analysis and analysis of legislation as well as academic commentary about it. The material was gathered from libraries, websites and news sites. The books are mainly eBooks because the topic of drones is relatively new and there are not enough printed versions available in the libraries. The websites included different researches, study papers, reports, governmental sites, organisation and company websites to mention few. This master's thesis used also news for the research because, as mentioned, the topic is new and the development is fast so new researches, books or papers do not keep up with the speed of new developments. The scientific material was read through, analyzed and combined with the news that was written about the topic. The author had also to follow the legislative procedures because new laws and regulations about drones and laws related to drones and privacy are under review and also new laws were passed during writing of this master's thesis. The message in most of the

material was that drones might be a threat to privacy, but there were also positive aspects with the increase of drones. This master's thesis is discussing about drones and privacy mostly in Finland and EU, and for that reason there are some news and other material only in Finnish. The author always tried to find the same news or other material also in English, but in some cases there were no English version.

1.3 Legislation used

The legislation used for this master's thesis consists of the Finnish and EU legislation. From the Finnish legislation at least the following laws are used; Henkilötietolaki 22.4.1999/523 (English: Personal Data Act), Laki sähköisen viestinnän palveluista 7.11.2014/917 (English: Information Society Code 917/2014), Suomen perustuslaki 11.6.1999/731 (English: The Constitution of Finland 11 June 1999, 731/1999), Suomen Rikoslaki 39/1889 (English: The Criminal Code Of Finland 39/1889) and Poliisin henkilötietolaki SM064:00/2015 (English: the Finnish Police Personal Data Act) that is under review at the time of writing this masters´ thesis. Besides these laws and acts also some aviation and other laws are used.[6]

The EU legislation includes the Regulation EU 2016/6790 (the European General Data Protection Regulation) (hereinafter the GDPR), The European Convention on Human Rights and Fundamental Freedoms (ECHR), Regulation 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency and the Opinion 01/2008 that will be implemented to the Regulation 216/2008 when it has been reviewed, Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, but also other EU laws, directives or regulations are used.

These are the main laws that will be discussed and used to discussion about drones and privacy but also other laws, also from other countries or regions are used to get a better picture of the topic.

[6] The Finnish law is accessible at: Finnish: https://www.finlex.fi/fi/ and English: https://www.finlex.fi/en/

1.4 Other sources and materials

Because the topic about drones and privacy is relatively new and there are not so much of academic books, the author of this master's thesis has used journals, articles, researches, news and authority reports to get a better picture and understanding about the topic. Most of the articles, journals and researches are pre-viewed and the author was careful when using news from different websites. The author tried to his best knowledge use trusted news sites and double-checked from other sites the news. Because the topic is about drones in Finland and EU, there are also some Finnish news, reports and researches that could not be found in English. Furthermore also both Finnish and EU authority websites were used as well as websites about drones, privacy facial recognition and other topics that is covered in this master's thesis.

2. DEVELOPMENT OF DRONES

To the long development of drones have been included many new inventions, many failures and success stories. As to any new device, the first ones are usually not so practical or they do not work as planned. The civilian, consumer and commercial drones we are familiar with today, have gone a long path from the first remotely piloted air vehicles. The first "drones", if we can call them that, were actually airplanes that were controlled remotely, from there the development went to military drones which rout could be programmed in advance or remotely piloted. After many decades of drones belonging only to the military, the civilian, consumer and commercial drones started to be developed. The first drones were as we can imagine, difficult to fly and relatively expensive. When the developers noticed that there might be a big market for the non-military drones, they started to develop them more and now, in 2019, there are a huge variety of drones in different kinds, sizes and prices.

2.1 History and development

The development and history of drones from ancient times to today has been really slow until the last decade and now the development is really fast and the legislators have a full work to keep the laws and regulations up to date. The development of drones has been slow in the beginning, and the first flying objects were not drones, but kites. The first kites are estimated to be

developed in China around 2300 years ago.[7] It took some 2200 years of development from the first kites to the firs flying vehicles with engine. The development has started with flying kites to kites carrying objects and slowly moved to balloons and continuing to motor driven flying vehicles. From the first motor driven flying vehicles in 1903 when the Wright Brothers managed to do the first flight with a motor[8], it took only 15 years to the first unmanned airplane flight. It was the Kettering Bug developed by Charles Kettering in 1918 and it used a gyroscope to control it. It was planned for military purposes.[9] Later during the World War II the V-1 "Buzz Bomb" created by the Nazis was similar but it was more of a flying bomb rather than a drone.[10] The ROA´s or as drones as we are familiar with today, have been developing basically since 1918, when the Kettering Bug took off. Even though the first engine driven airplane was made in 1903 and the first unmanned flight with an airplane was in 1918, the inventor and scientist Nikola Tesla started to develop on the first remotely controlled device in 1892, but a fire destroyed his laboratory and the first models. Later in 1897 Tesla continued with the remotely controlled devices and more precisely with a radio controlled boat even that he was imaging it to work also even with an airplane. This was the start of the remotely controlled vehicles.[11] The development of remotely operated vehicles was slow in the beginning and first they were designed and made mainly for military purposes but since 2010 the technology and development concerning drones has taken huge steps and now the drones are available for everyone and the development continues.

The history of drones includes many names such as UAV, UMA and ROA. Also many other names have been used to describe the flying objects at the same time as it has been debated how to characterise UAV's in the past.[12] Even if the origin of the name Drone has a military background and the name Drone has mainly been used to weapons, it has been adopted to the everyday language to describe camera UAV's. The name UAV is the formal name for the flying unmanned, remotely controlled small aerial vehicles, but if we are talking about the camera

[7] http://chinakites.org/htm/fzls-gb.htm
[8] Banner, S. (2009) Who Owns the Sky? : The Struggle to Control Airspace from the Wright Brothers On, Harvard University Press. pp.11
[9] Sullivan, J. M. "Evolution or Revolution? The rise of UAVs", *IEEE Technology and Society Magazine*, vol. 25, no. 3, 43-49, 2006. pp. 43 Accessible: https://ieeexplore.ieee.org/abstract/document/1700021
[10] Gross, C. J. (2002) American military aviation : the indispensable arm, College Station : Texas A & M University Press. pp.116-117
[11] Bernard, C. W. (2013) Tesla : Inventor of the Electrical Age, Princeton, New Jersey : Princeton University Press. pp. 225 - 227
[12] Newcome, L. R. (2004) Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles, American Institute of Aeronautics and Astronautics, Inc., Reston, Virginia. pp.1-5

UAV's, we often refer to it as a drone.[13] The most significant difference with the military and civilian drones are of course the weapons, but when not taking the weapon aspect into account, the military and civilian drones are often of different size. The civilian and consumer drones are often in the size that they can fit in a normal backpack with a weight up to few kilograms, whereas the military drones are often big and many of them weight around 1700kg and with length of around 10 meters and with a wingspan of over 15 meters they can be even considered almost like airplanes.[14]

The first records of camera drones can be reached as early as 1887 when an English meteorologist called Douglas Archibald attached a camera to his kite and took the first aerial photographs from the sky,[15] and later the pictures were published and Corporal William Eddy saw them and understood that aerial photographs would be useful in combat and he used the same idea during the Spanish - American war in1898 when he took aerial photographs during combat. This was probably the first time a UAV has been used in war.[16] Some sources suggest that cameras were used and attached to balloons already in 1858 in France, but as the camera kite as well as the camera balloon, both are without engine and are just the first steps into drones as we know them today able to carry objects. The first drones carrying weapons, mainly explosives, was already 1918 in the USA but the UAV´s were used mainly in the 1930 as targets to military trainings.[17] The big issue at the beginning was how to control the drone when it is flying. There was another English scientist named Montgomery Low Archibald who worked with data links. He managed to develop the first data link that was not interfered by the engine of the UAV that had been a problem. After many attempts to radio control an UAV resulted in a crash, he finally managed to make the world's first successful radio controlled UAV flight in September 1924.[18]

In many fields the war industry push for new technologies and drones are not an exception. Even if the drone technology and development was driven by the military industry, engineer John W. Clark from the United States of America came up with an idea of a remotely operated machine

[13] Dvorkin, D. (2013) Dust Net: The Future of Surveillance, Privacy, and Communication: Why Drones Are Just the Beginning, David Dvorkin. pp.6
[14] Kaag, J. Kreps, S. (2014) Drone Warfare, Polity Press, Oxford. pp.40
[15] Bartsch, R. et al. (2016) Drones in Society: Exploring the strange new world of unmanned aircraft. Routledge. pp.22
[16] Fahlstrom, P. Gleason, T. (2012) Introduction to UAV Systems, John Wiley & Sons, Ltd. pp.4
[17] Clarke, R. Understanding the drone epidemic. Computer law & security review 30 (2014) 230-246. Xamax Consultancy Pty Ltd. Published by Elsevier Ltd. pp.231
[18] Fahlstrom, P. Gleason, T. (2012) Introduction to UAV Systems, , John Wiley & Sons, Ltd. 11.7.2012. pp.4

could work and go to hostile places instead of a human being in 1964. His vision was that the remotely operated machine could work e.g. as miner, fire fighter or in the deep sea. His idea with the remotely controlled machine was to make the human work in hostile environment but not as a weapon in war. The idea of the remotely operated machine was not at this stage a drone as we know it, but more of a non-flying machine. None the less, the idea was clear, that a machine could be operated from distance from a safe place. Clark had planned it for friendly, nonviolent use, but as the military industry heard about it got interested about it.[19]

The next step was during the Vietnam War, when RPV´s (Remotely Piloted Vehicles) were introduced to the U.S. Air forces to minimize casualties and avoid POW´s (Prisoners of War). In Vietnam the drones were mainly used to gather information and for surveillance.[20] After the war, the drone project was abandoned in the United States of America by end of the 70´s. The Israeli Air Forces then again had continued developing drones and used RPV´s in war against Egypt and Syria. They used the drones to mislead the antiaircraft defence and the real bombers and fighter planes came after them. They were also used as surveillance and the U.S military got an introduction of it when an U.S. military officer went to Beirut after a terrorist attack in 1983, and an Israeli drone had filmed him in Beirut even if he had came there secretly without anyone knowing of it. The film was aired and the U.S. officer was shocked over the image. This was the turning point of the U.S. drone project. After this event the drones have been developed but was used mainly for surveillance until 2001 when the first drone launched a rocket to its target with live footage from the field.[21] Even though the first missile shot from a drone was as early as 1971, but at this time, there was no live footage so it had to be programmed ahead before the flight, so it is not exactly the same kind of drone as the newer where the target can be chosen from the live footage during the flight.[22]

After the start of killer drones in 2001, the technology has developed a lot in a short time and also commercial drones has become more common, smaller and easy to fly.

[19] Chamayou, G. (2015) A Theory of the Drone, , Translated by Janet Lloyd, New Press. pp.21-23
[20] Sullivan, J. M. "Evolution or Revolution? The rise of UAVs", *IEEE Technology and Society Magazine*, vol. 25, no. 3, 43-49, 2006. pp.43. Accessible: https://ieeexplore.ieee.org/abstract/document/1700021
[21] Chamayou, G. (2015) A Theory of the Drone, Translated by Janet Lloyd, New Press. pp.27-29
[22] Rothstein, A (2015) Drone, Object lessons series, , Bloomsbury Academic. pp. xi

2.2 History of drone law

During the relatively short time drones have been filling up our skies, there have basically not been laws or regulations regulating the drones until recently. The humanitarian and international law have covered the large military drones, but also some aviation law has been involved. The use of civilian, consumer and commercial drones was relatively Wild West in many countries before legislation was updated to cover drones. In the U.S.A the first "drone laws" came into force in 2015. In Finland, consumers have been able to buy drones in Finland since 2011, when the first drone shop opened.[23] Before that one could order a drone from abroad. Even if there were not exactly laws on consumer type of drones, the Finnish aviation legislation has mentioned UAV´s at least since 2005 in the Finnish Ilmailulaki 1242/2005 (aviation act). In the aviation act are mentioned that UAV´s may get exceptions from the law that applies to airplanes, helicopters etc but there are not any exact laws how and where to fly.[24] Basically the first time the RPAS´s or drones has been mentioned by the Finnish authorities in terms of regulations, was according to Salmisalo on the 6th of May 2015 when TRAFI gave its firs proposal OPS M1-32 to regulate drones.[25] After this, a new regulation issued by TRAFI regarding RPAS´s came into force the 7th December 2018 that replaced the previous OPS M1-32.[26]

As described above, there has not been many laws or regulations regarding civilian drones until around 2015. The EU Directive 216/2008[27] came out in 2008, but it was regulating only those drones which were heavier than 150kg, and these heavy drones are usually only for authority or company use, not for civilian leisure use. Since 2015, the European Parliament and the Council of the European Union have been working on EU wide regulations regarding drones[28]. In March

[23] https://multicoptercenter.fi/pages/miksi-ostaa-meilta (7.6.2019)
[24] Ilmailulaki 1242/2005. Accessible: https://www.finlex.fi/fi/laki/alkup/2005/20051242#Pidp445886336 (19.3.2019)
[25] Salmisalo, V. (2015) Taivaalla surisee, Multikopterit ja niiden yleistyminen. Metropolia Ammattikorkeakoulu Medianomi (AMK) Bachelor Thesis. Accessible: https://www.theseus.fi/bitstream/handle/10024/95819/Opinnaytetyo_Salmisalo.pdf?sequence=1&isAllowed=y (8.2.2019)
[26] Kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun OPS M1-32 (TRAFI/334638/03.04.00.00/2017)
Accessible: https://www.finlex.fi/fi/viranomaiset/normi/498001/44667 (15.3.2019)
[27] Regulation (EC) No 216/2008 Of The European Parliament and of The Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008R0216 (8.3.2019)
[28] http://dronerules.eu/en/recreational/eu_regulations_stakeholders

2015 the *Riga Declaration on Remotely Operated Air Systems*[29] were made where a discussion about the importance of EU wide regulation took place. Later the same year in September, the *Resolution of the European Parliament on the safe use of remotely piloted aircraft systems (RPAS), commonly known as UAVs, in the field of civil aviation (2014/2243(INI))*[30] came out, where the European Parliament suggested that a common European legislation regarding civilian and commercial drones that weight under 150kg has to be made to ensure the safety of aviation and that RPAS´s should be integrated to SESAR as soon as possible. Now there are new amendments on their way when the Directive 216/2008 is reviewed and the new Directive should come into force during 2019 and there also the civilian drones are included. These are the laws that are related to the privacy and drones. Besides these, there are many other EU, international and national laws and regulations that are regulating and protecting privacy and these are applying also to drones.

2.3 Surveillance from war to peace

Surveillance is not a new thing and military forces have used it as long as wars have been fought, but before it was the human eye that made the surveillance and it was limited to places where the human could go or climb. After 1850´s also cameras were started to be used for surveillance on the battlefield. The cameras were attached to a balloon and the area could be photographed from above and get larger areas covered and a bigger and better picture of the enemy.[31] After the development of the first UAV´s in the 1918 and in the 1960s when camera equipped UAV´s started to be used more widely, the surveillance technology on UAV´s or drones as more often called, has developed enormously. The drone technology developed rapidly during the millennium and the amount of drones the US military had grown from 167 military grade drones in the 2002 to around 7000 in 2010. During the years of 2001 - 2008, also the surveillance hours increased by 1431 per cent. The use of drones and surveillance was for military purposes in Afghanistan, Pakistan Yemen and Iraq, and already in 2010 the surveillance hours reached 250,000 hours during one year, which is more than all combined US drone surveillance during

[29] Riga Declaration on Remotely Piloted Air Systems: Framing the future of aviation, of 6 March 2015 Accessible: https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf (8.3.2019)
[30] Resolution of the European Parliament on the safe use of remotely piloted aircraft systems (RPAS), commonly known as UAVs, in the field of civil aviation (2014/2243(INI)) Accessible: http://www.europarl.europa.eu/doceo/document/A-8-2015-0261_EN.html?redirect (8.3.2019)
[31] Clarke, R. Understanding the drone epidemic. Computer law & security review 30 (2014) 230-246. Xamax Consultancy Pty Ltd. Published by Elsevier Ltd. pp.231

the period of 1995 - 2007[32]. As mentioned, this surveillance was earlier mainly for military purposes but since 2011 also police forces have been using drones for surveillance, and probably the first drone assisted arrest by the US police forces was in 2011.[33] Ever since that, also police forces have used drones for surveillance and not just in the US, but also all over the world.

Before the drones came there were already surveillance but not from the skies. Video surveillance is not a new thing and the first video surveillance was already in 1960s when the first recordings on video cassettes was possible to store.[34] After that the video surveillance has been used to prevent crimes, help police investigations and to make people feel safer. As most people who live or have visited bigger cities, have probably noticed the amount of video surveillance in public places, shopping malls, streets, public transport and almost everywhere else as well. At the same time as video surveillance should protect us, normal citizens, it has risen fears of loosing privacy.[35] From fixed surveillance cameras since 1960s, the video surveillance have raised to the next level, namely to the air. Nowadays almost all countries police forces use drones to help them do their job. Usual tasks to use drones are e.g. to search for missing people from the forest, to monitor big events or protests, get footage from a crime scene or to get real time footage from a police force siege. In 2018 the Finnish Police Department has totally around 130 drones[36] whereas over 900 public safety agencies in the US use drones, but The New York State Police has only 18 drones in its use.[37] In the end of 2018 the Finnish Police Department should have already around 200 drones in its use. The last big police drone mission was during the Finnish Independence Day 6.12.2018 when the police had 23 pilots operating 10 drones doing surveillance on demonstrations and the traffic. During the surveillance the police

[32] Neocleous M. (2014) War Power, Police Power. Edinburgh: Edinburgh University Press. pp.153-154
[33] Hiltner, P. J. (2013). The drones are coming: Use of unmanned aerial vehicles for police surveillance and its fourth amendment implications. *Wake Forest Journal of Law Policy* 3(2), 398-399.
[34] Kremer, J. The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space. Doctoral dissertation, Faculty of Law University of Helsinki, 2017. pp.20 Accessible: https://helka.finna.fi/Record/helka.3052131
[35] Senior, A (ed). (2009) Protecting Privacy in Video Surveillance, Springer-Verlag London Limited, Springer. pp.35
[36] Helminen, L. Suomen poliisin käyttämistä suosituista kuvauskoptereista löytyi haavoittuvuus – samoja koptereita käytössä tavallisilla kuluttajilla ja yrityksillä. Helsingin Sanomat 8.11.2018, Accessible: https://www.hs.fi/teknologia/art-2000005892603.html
[37] NYTIMES, Rise in US police use of drones triggers backlash over spying and other abuses 6.12.2018, Business Times, https://www.businesstimes.com.sg/technology/rise-in-us-police-use-of-drones-triggers-backlash-over-spying-and-other-abuses (12.3.2019)

caught also eight drones flying on restricted areas.[38] The year before, during the Independence Day 6.12.2017, the police was using 22 drones for the same purpose as in year 2018 and it is one of the biggest police drone operations so far.[39]

The development from military surveillance drones to civilian use drones took some time, but for the last 5 - 7 years, the development has been exponential and now we are in the situation that the military, the police forces, the governments, companies and private persons can do video surveillance relatively easy from the sky with drones. This has raised concerns about the privacy when the laws regulating the drones are one step behind the development of drones.[40] In the EU, the surveillance is not yet an extremely major problem, but in the United Kingdom there are already concerns about public space surveillance and the privacy of legal persons because of its large-scale surveillance and the use of facial recognition. It is estimated that there are around 6 million surveillance cameras and 100.000 publicly operated surveillance cameras in the UK.[41] This makes the UK one of the most surveyed countries in the world. Also the increased amount of drones the UK police use has risen concerns because many of the drones us AI to recognise people who behave in an un-normal way, such as fighting, kicking or shooting.[42] Also facial recognition has started to develop but is not yet used in drones in a large scale. The use of drones for surveillance to detect fights or other criminal activity is in general a good thing but, when it is constant surveillance, it creates a huge register of normal people who just happens to be recoded. This kind of mass surveillance is a big threat to the privacy that is a human right in every European country.

The surveillance technology is developing and there are already developments of even more sophisticated surveillance devices that can be attached to drone. One of these is a laser scanner

[38] Ziemann, M., Volocopter lentää Helsingissä ensi kesänä – Kaupunkien pitää alkaa suunnitella parkkipaikkoja taksi- ja tavara-droneille 17.12.2018, Yle News, https://yle.fi/uutiset/3-10555274 (13.3.2019)
[39] Malmberg, L. Tunnelma kuin tieteiselokuvassa: Helsingin taivaalla risteili 22 poliisin miehittämätöntä lennokkia valvomassa itsenäisyyspäivän viettoa, 7.12.2017, Helsingin sanomat news. Accessible: https://www.hs.fi/kaupunki/art-2000005481201.html (23.2.2019)
[40] Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer. pp. 96-97
[41] Weaver, M., UK public must wake up to risks of CCTV, says surveillance commissioner 6.1.2015, The Guardian. Accessible: https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent (26.2.2019)
[42] Milmo, C., Most British police forces now have drones – and they're getting better at watching us. Is this the future we want? 29.6.2018, iNews. Accessible: https://inews.co.uk/news/uk/eye-in-the-sky-drone-capable-of-spotting-violence-in-crowds-raises-questions-about-hi-tech-policing/ (26.2.2019)

that can scan through walls. If and when this technology reach drones, if the authorities would use such surveillance, it would be a real threat on privacy because persons could be watched from outside and there would basically be no place to be sure that one is not under surveillance. Another thing that is still under development is Micro Aerial Vehicles (MAV). These have been developed since the 70´s. The MAV is a tiny drone that has a camera and other sensors as well. The developers have been studying butterflies, dragonflies and other insects and they try to make a drone in an insect form such as a dragonfly.[43] These drones could be used in densely built and populated area because a bigger drone could not fly on small alleys or shopping centers safely and without people noticing it.

The surveillance that is happening today by the governments is on the other hand a welcome practice to reduce crimes and make the cities safer, but on the other hand it is scary with the mass surveillance and with the loosing of privacy. Because of the facial recognition, location data and other information that can be gathered from the surveillance, the governments can easily make different categories and divide people into groups. During peacetime it is not as big problem but if there become war for some reason, it may be a big threat to some groups. During the Nazi regime, if the government would not had registers of personal information of its citizens, it had been much more difficult to conduct the holocaust. This is of course an extreme example what mass surveillance may lead to but it should be taken into account especially now when the technology enables fast, accurate and large scale surveillance.

2.4 Consumer drones

The consumer or civilian drones have been flying around for a while now, and during the last 10 years they have become more and more common thanks to the new technology and when they have become cheaper. When the skies are filled with drones on an increasing speed also the concerns about privacy have raised. The laws and regulations in Finland regarding drones are relatively free, and if a person has a small drone such as a DJI Mavic 2[44] that is of the top quality, there are basically just the altitude limit that is 150 meters, visual contact with the drone and not to fly it over people or restricted areas.[45] The DJI Mavic 2 weights under 1kg even with a

[43] Boghosian, H. (2013) Spying on Democracy Government Surveillance: Corporate Power, and Public Resistance. Open Media Series, City Lights Books, San Francisco. pp.229-230
[44] DJI Mavic 2 specs. Accessible: https://www.dji.com/fi/mavic-2/info#specs (13.3.2019)
[45] TRAFI legal drone info page. Accessible: https://www.droneinfo.fi/en/how_to_fly_safely (13.3.2019)

zoom lens, so a top quality drone as the Mavic is, its weight is lower than the maximum weight for leisure drones that is 25kg and if the drone is under 4kg it can be flown in densely populated area with precaution. The drone industry is booming and in a SESAR (The Single European Sky ATM Research) research it is estimated that there are 1-1.5 million civilian drones in Europe for the moment and by 2020 the number of drones would be around 5 million. During the last few years the amount have grown over 100% each year.[46] This is a huge amount of drones flying around without a common EU regulation. This will change in the near future when a common EU regulation will enter into force progressively. For the moment each EU member state has their own legislation for drones weighting under 150kg but it will change when the Opinion 01/2008[47] has been reviewed and implemented to the Regulation 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency. So far the 216/2008 Regulation has applied to drones with a Maximum Takeoff Mass (MTOM) of 150kg, so it has not been applied to consumer drones. An average consumer drone weight around 500g and the top end drones around 1-1,5kg. The aim with the revised Regulation 216/2008 is to harmonize the drone rules across EU and that the 216/2008 Regulation applies to all drones despite the MTOM.[48] This will make a change to the consumer drone flying and industry. The consumer drones will be regulated more than before and compulsory registrations, restrictions and other measures are harmonized across the EU.[49]

The drone industry is growing and when the drones are very sophisticated today, they can be used for different purposes such as for agriculture, governmental use, traffic monitoring, security, rescue services, medical services and delivery to mention few. There are still a lot of undiscovered potential in drones and the drones can help a lot with different tasks, but when they are used for surveillance it rises concerns. Civilians, governments, police and other authorities can use the drones for different kind of surveillance. Because of the high quality of the cameras and other sensors in the drones, it raises questions about selling drones with surveillance capabilities for consumers. A company named Face-six is advertising its drones with live facial

[46] SESAR, European Drones Outlook Study, Unlocking the value for Europe, November 2016, pp. 17 Accessible: https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf (12.3.2019)
[47] European Aviation Safety Agency Opinion No 01/2018, Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories
[48] Ibid., pp.5
[49] European Aviation Safety Agency Opinion No 01/2018

recognition, tracking, face log, alerts and more both for governmental and private use.[50] The author of this thesis finds it alerting that basically anyone could use drones for spying.

When we talk about consumer drones, one question came to mind to the author of this thesis; Is it necessary that private persons can buy consumer drones equipped with facial recognition program, tracking or other surveillance equipment? Private persons and consumer drones are usually needed and used for photography and video recording or just for flying them. This topic will be discussed in more detail later in the thesis.

As mentioned earlier the drone industry is growing rapidly and for the consumers there are a huge variety of different drones for different use, size, price and quality. The normal consumer drone prices can be everything between 10€ and 1500€ and most of them includes a camera even in the cheaper versions. If the price is higher than 1500€, it is usually more for professional use than leisure. The fast growth of consumer drones is because there is a big variety to choose from and the consumer can find a drone that fit to the consumers' budget and purpose. A downside with the huge variety is that in a survey in 2015 by the joint cross border R&TTE Market Surveillance campaign, it was found that for the technical part 23% of the drones and 38% of the remote controllers did not fulfil all of the requirements[51] and overall 92% of the devices did not fulfil all of the requirements such as labelling or markings that is set in the R&TTE Directive[52]. This is over four years ago, but it is an alarming amount of devices that are not according to the requirements. The lack of product safety in consumer drones is also a safety and privacy risk.

The biggest problem at the moment with consumer drones is that they are flying in places where they should not fly e.g. near to airports, military bases or nuclear plants. In December 2018 the Gatwick airport was shut down due to many drone sights. This case was widely in the news and showed how vulnerable an airport is against drones.[53] Then again in January 2019 London Heathrow Airport had to suspend all flights when a drone was spotted close to the airport. This incident affected thousands of passengers that were stuck at the airport. The police, the military

[50] Face-Six, Accessible: https://www.face-six.com/drone/ (visited 13.2.2019)
[51] 7th joint cross-border R&TTE market surveillance campaign (2015) on RPAS Final report adopted by ADCO R&TTE 51 on 21st October 2015, pp.10
[52] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
[53] McKenzie, S., Mezzofiore, G., Police hunt drone pilots in unprecedented Gatwick Airport disruption. 21.12.2018, CNN. Accessible: https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html (12.2.2019)

and Scotland Yard was investigating the drone incident.[54] This was not the first time drones have been flying close to airports. There have been also close calls when passenger airplanes have almost hit drones during take-off, landing or flight. In August 2018 pilots spotted a drone extremely close to their plane when they were flying at 1200 meters altitude over Edmonton. Canada has relatively low maximum altitude fore drones, that is only 90 meters above the ground. The drone pilot exceeded this limit with over 1km.[55] In South Carolina it is possible that a drone was reason for a helicopter crash landing. Neither of the helicopter pilots were injured but if the drone had hit them at higher altitude it could have lead to another more sever outcome.[56] These issues are of high importance and it is important that there are laws and regulations that limit where, how and with what one is flying a drone. Even if there are not harmonized consumer drone laws and regulations in EU, every member state has their own and flying close to airports are prohibited in every country.

The United Kingdom passed new drone laws in May 2018, but the effects of the law will become in force in September 2019. The idea with the new law was to make the passenger flights safer. In 2016 there were 71 drone incidents and in 2017 it was already 93. All of the incidents have not been serious and to the total amount is counted all disturbances that drones have caused, including drone sights near airports so that the airport personnel have had to take actions. After the incidents at Gatwick when the airport was closed for a while because of drone sights, the UK government and the Civil Aviation Authority (CAA) passed a new law that come into force in March 2019, that will extend the no fly zone to 5km from the runway.[57] This is a significant extension compared to the law that had been planned in 2018. The previous law that had planned to come into force in 2019 had prohibited to fly within 1km from an airport and it is also restricting the flight altitude to 120 meters. It is not in knowledge if the law will come into force for the other parts such as that the pilots, who fly drones heavier than 250 grams, have to register

[54] BBC News, Heathrow airport drone investigated by police and military, 9.1.2019. Accessible: https://www.bbc.com/news/uk-46804425 (15.2.2019)
[55] CBC News, Airliner has close call with drone, 4,000 feet over Edmonton, 1.8.2018. Accessible: https://www.cbc.ca/news/canada/edmonton/airliner-drone-near-miss-edmonton-1.4770662 (12.2.2019)
[56] Levin, A., Drone collisions, close calls underscore growing risks for aircraft, 17.2.2018, Washington Post. Accessible: https://www.washingtonpost.com/politics/spate-of-drone-collisions-close-calls-underscore-growing-risks-for-aircraft/2018/02/17/4b630714-1433-11e8-8ea1-c1d91fcec3fe_story.html?noredirect=on&utm_term=.4e72f8a1494a (12.2.2019)
[57] Gov.UK, From: Department for Transport, Home Office, Civil Aviation Authority, New drone safety partnership with business launched as government sets out plans to limit drone misuse, 20.2.2019. Accessible: https://www.gov.uk/government/news/new-drone-safety-partnership-with-business-launched-as-government-sets-out-plans-to-limit-drone-misuse (6.3.2019)

their drone to the CAA and to pass an online safety test to get permission to fly a drone.[58] It is good and important that the airport areas are safe and people are not flying drones there. When comparing UK drone legislation with the Finnish drone legislation, the airport safety area has been in Finland for many years already, at least from 2014[59] onwards and in 2018 TRAFI extended the restriction and safety zones close to Finnish airports. Earlier drone flights closer than 1km from the airport was prohibited and within 1-3km distance one could fly a drone on 50 meters altitude or 15 meters above a permanent obstacle such as a hill, tree or house. Now the safety zones have been extended up to 5km in some places and in some parts the safety zone can go up to 13km where the maximum altitude is 50 meters above ground but the basic zones are 1km and 3km. TRAFI have made an drone app for every drone pilot and it shows the exact allowed altitude and restrictions when it is opened at the place where the flight is planned.[60] Both the UK and the Finnish laws are directed more to civilian consumer drones than professional and other commercial or authority drones.

3. DRONES AND LAW

When new technology or devices come to the market and the use of such devices grow in an increasing speed, the authorities can sometimes have trouble to keep up with the fast growth. This happened with the drones because earlier there were not that many civilian drones and there were not serious incidents and the drone flying was in control even without proper legislation. When the popularity of drones and the big variety became the new normal, there started to be more and more incidents and problems when drones are flying everywhere. The authorities had probably not expected such a fast growth and this might be one reason that the drones were basically without legislation for a long time. Another reason for the late regulatory work regarding drones, at least in Finland, was that the authorities wanted to encourage to try new technology and also because the Finnish authorities wanted to explore the possibilities the drone could bring.[61]

[58] Department for Transport, Civil Aviation Authority, and Baroness Sugg CBE. New drone laws bring added protection for passengers, 30.5.2018 Accessible: https://www.gov.uk/government/news/new-drone-laws-bring-added-protection-for-passengers (6.3.2019)
[59] Kilpeläinen, M. (2.10.2016) Journalismia lintuperspektiivistä. https://blogit.metropolia.fi/median-maailma/avainsana/drone/ (6.3.2019)
[60] https://www.droneinfo.fi/fi (the English site does not show the app but there app is also in English)
[61] STT, Yle News 18.7.2017. Suomessa on arviolta kymmeniä tuhansia droneja - EU kiristää Suomen löyhää lennokkilainsäädäntöä. Available at: https://yle.fi/uutiset/3-9727680 (8.3.2019)

3.1 Current situation

During the first 80 - 100 years of the existence of drones, there has basically not been any need for laws about flying consumer drones, because it has been almost only governments, military and other authorities who have had access to drones, but since 2010 when civilian drones started to become more popular, also the authorities woke up to the need of laws and regulations regarding drones. Earlier the drones were more expensive and the technology was not very developed. To fly a drone was not easy and one could not buy them as easy as it is today. In 1999 when the first commercial drone could be bought[62], flying a drone was challenging and it required more practice to be able to fly it without crashing it, but when the technology developed, also the flying experience has become better. Since 2010 the consumer drone prices have dropped and technology become better and now one can buy a drone with a decent camera for less than 100 €. As of 17.12.2018, an Eachine E58 camera drone was 86,98 € on Amazon.de[63] and it is said to be a affordable copy of DJI Mavic drone that is one of the top quality consumer drones[64] and the DJI Mavic cost between 800 € to 1400 € depending on the model. These new drones are easy to fly even if the pilot would not have any experience from before thanks to the technology in it. If the pilot does nothing and do not touch the remote control, the drones hover in one place and do not move without further commands. Most of the drones do also have automatic take-off and landing ability. All of these things, price, easiness and good quality have boosted the drone industry. Now when there are millions of drones there is a need of new legislation and regulations. Even though all of the European countries have a national legislation concerning drones, there is not yet EU wide harmonized legislation for consumer drones.

Finland is still relatively un-regulated what it comes to flying civilian drones. There are no mandatory registration requirements and on not-restricted areas one can fly up to 150 meter high with a drone. This is 30 to 50 meter higher than in many other European countries where the maximum altitude is usually either 100 meters as in Germany and Denmark[65] or 120 meters as in Portugal, Sweden, and Norway and from March 2019 onwards UK. Also the civilian drones

[62] Rothstein, A (2015) Drone, Object lessons series, Bloomsbury Academic., pp. 37
[63] Amazon.de, Eachine E58 drone. Accessible: https://www.amazon.de/EACHINE-Übertragung-120°Weitwinkel-Quadrocopter-App-Steuerung/dp/B077MFPZTN/ref=sr_1_5?s=toys&ie=UTF8&qid=1545062130&sr=1-5&keywords=drone (22.2.2019)
[64] Techradar, best drones of 2018. https://www.techradar.com/news/best-drones (20.1.2019)
[65] http://dronerules.eu/en/professional/regulations (12.3.2019)

maximum take-off mass must not exceed 25 kilograms, and a drone that does not exceed 3 kilograms can be flown over densely populated area when taken the security in account.[66]

There are different areas of law that has to be taken into account when flying and recording with a drone. The first is the different aviation laws and regulations that regulates where, how, whom and whit what one can fly a drone. This masters´ thesis does not concentrate that much on this area, but more on the privacy issues such as the recorded footage and how it is used, stored and processed. Even though the different aviation laws are not in the focus, they have to be taken into consideration also when discussing about privacy.

What it comes to drones and privacy there are several laws and regulations such as the European General Data Protection Regulation (GDPR), Finnish legislation: Personal Data Act (Finnish Henkilötietolaki 22.4.1999/523), Information Society Code 917/2014 (Finnish: Laki sähköisen viestinnän palveluista 7.11.2014/917), The Constitution of Finland 11 June 1999, 731/1999 (Finnish: Suomen perustuslaki 11.6.1999/731), The Criminal Code Of Finland 39/1889 (Finnish: Suomen Rikoslaki 39/1889) and the Finnish Police Personal Data Act (Poliisin henkilötietolaki SM064:00/2015) that is under review at the time of writing this masters´ thesis.

At the time of writing this thesis, the European Union is working on new regulations that will affect the civilian drones and pilots. For the moment (2/2019) the EU does not have any common regulations for civilian drones that are lighter than 150kg, but there are plans that during 2019 and 2020 also the lightweight civilian drones would be regulated by EU regulations. Now, the laws and regulations for civilian drones under 150kg, are ruled by the national laws of the member states, and there can be significant differences between the laws of the member states.[67] Germany has the maximum flight altitude as 100 meters, visual contact, compulsory insurance and special authorization to fly a drone whereas Finland has the maximum flight altitude set as 150 meters and visual contact without mandatory insurance, authorization or registration.[68] Most of the laws and regulations concern more where and how to fly the drone rather than the privacy. There are already laws and regulations that apply to all personal data, and the data the drones

[66] Kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun OPS M1-32 (TRAFI/334638/03.04.00.00/2017)
Accessible: https://www.finlex.fi/fi/viranomaiset/normi/498001/44667 (15.3.2019)
[67] http://dronerules.eu/en/professional/eu_regulations_updates (10.3.2019)
[68] http://dronerules.eu/en/professional/regulations (10.3.2019)

may collect falls under these laws and regulations, but even this, the concerns about privacy regarding drones are in the news relatively often.

The GDPR that came into force in May 2018 is covering basically all the privacy issues when it comes to companies and authorities, but the facial recognition technology and other surveillance technologies in drones are still raising concerns. The GDPR regulates what kind of personal data companies and authorities can process and store. The purpose with the GDPR is to make the privacy better for EU citizens and to regulate the personal data. Companies for example need a genuine consent from the customer to be able to collect personal data, e.g. when the person visits an online shop and orders an item from there. Then again, when the authorities collect personal data they do not necessarily need any consent depending on the purpose of the collection of personal data, but they need to have a legal purpose for the collecting. Furthermore, the authorities may process the data and store it more freely than private companies. This is because the authorities may have a legal responsibility to store the personal data for even a long periods to be able to provide its citizens the services it is obligated to do, whereas the private companies does not have any reason to keep the personal data for 20 years if the person is not using the companies products or services. The GDPR regulates all personal information of EU citizens. The GDPR applies in the EU and EEA but also everywhere where personal data is processed of a EU or EEA citizen in regards to sales or services.[69] This means that if a company from Australia sell products or services also to EU citizens, the GDPR will apply to the sale. The idea with the GDPR is that the given or collected personal data will not be processed in unnecessary way or transferred to a third party or stored for too long time and that there is a better control of how and who process and collects the data. The GDPR is not exactly stating how the data is collected but as mentioned, the companies need always a given consent from the data subject for the personal data. More over, the GDPR take strong stand to biometric data. The GDPR Article 9 (1) say among other things, that processing of biometric data that can reveal the persons racial or ethnic background shall be prohibited. In Article 4 (14) of the GDPR the facial images are considered to be biometric data because with facial recognition the person can be identified and biometric data are used in this case. This again does not apply if the company or authorities has a legit reason to process, store and collect biometric data, or it is necessary for the public safety or general order.

[69] The GDPR Art. 3

Most of the laws about aviation and privacy are made before the drones filled up the sky and basically the laws and regulations apply the same way to drones as they apply to fixed video surveillance or cameras, but the main difference to the fixed cameras is that the drones can easily be moved to different places. Also the fact that private persons can get drones equipped with different sensors that can e.g. track, recognize, and record images of persons without their consent can be seen as a threat to privacy. This raise concerns about privacy especially with facial recognition.[70] Another privacy issue is the security of the recorded or stored data. Cyber security company Check Point, found vulnerabilities in the DJI drones software. They said that the risk was high but that the probability to happen was low. The attacker could have been able to see all the flight data including footage from the drone as well as all the personal information that was attached to the account, such as name, address and credit card information. The probability that the attack had happened was considered low because the pilot should have had to download a program and grant permission to it, and this had been very unlikely to happen. DJI is the leading company of commercial and consumer drones with an approximately 70% share of the market. DJI fixed the vulnerabilities after they were found.[71] This kind of vulnerability can also be used to hijack a drone and use it to criminal purposes. As mentioned in chapter 2.3 about the lack to fulfil the requirements laid down in Directive 1999/5/EC, the vulnerability in the drones or remote controllers software can lead to exposed personal data. This issue is also discussed in the Opinion 1/2018 that will be taken to account when the 216/2008 Directive is revised.

The EU 216/2008 Regulation that is currently under review will take stand to the civilian and consumer drones. The 216/2008 Regulation is now basically regulating and setting common EU rules for drones but only to drones that weight over 150kg. This means that all consumer drones are outside the 216/2008 Regulation because drones that are meant for civilian and leisure use, are rarely heavier than 150kg, usually they are under 5kg. Most of the changes that will come to the 216/2008 Directive concerns how, where and with what to fly, but there is also requirements that the privacy shall be taken into consideration. The concern about the privacy regarding drones equipped with cameras, GPS and other sensors is still present even if the Opinion 1/2018

[70] Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer. pp.50
[71] Linnake, T., Hittilennokin omistajia pystyi vakoilemaan – ei mitään keinoa huomata, 9.11.2018 Iltasanomat. Accessible: https://www.is.fi/digitoday/tietoturva/art-2000005894206.html and Checkpoint Software Technologies Ltd. The Spy Drone In Your Cloud. Accessible: https://blog.checkpoint.com/2018/11/08/the-spy-drone-in-your-cloud/ (14.3.2019)

is stating several times that the privacy shall be taken into account, but there are no concrete measures how the privacy would be ensured. At the moment the Finnish legislation prohibits illicit recording or preparing to do so.[72] The Opinion 1/2018 does not bring any new safety measures or practices to the existing Finnish legislation in regards to illicit recording.

The maximum penalty for illicit recording is one-year imprisonment but usually the court gives only fines. The maximum penalty length is also problematic in Finland. The crimes have a certain time after which the crime is expired. If the maximum penalty is one-year imprisonment, the crime expires in two years if no charges have bee brought, and in some cases this may be a too short time, because sometimes the illicit recording is exposed after even three years, and then the crime will not be counted as a crime anymore. If the maximum penalty would be two-years imprisonment for illicit recording, the expiring time would be already 5 years, and it would give time to get the responsible for the illicit recording to be charged.[73]

Between 2009 and 2015 there were six sentences for eavesdropping and 53 for illicit recording. From these crimes only three offences lead to imprisonment sentence. These cases are civil cases and do not include governmental, police or other authority cases where above-mentioned measures have been used. The government asked opinion if the legislation about illicit recording, eavesdropping or preparing to do so should be reviewed, but in 2017 the minister of justice said in his opinion that there is not for the moment need to review it.[74] These statistics shows that there were in Finland almost every month a case about illicit recording during those six years. There have been discussions about possible need to intensify the sentences in cases about illicit recording. The Finnish police got informed about 81 cases of illicit recording in 2010 whereas in 2017 the amount was already 256 cases. This is a clear sign that the amounts of illicit recording is on the raise and one of the reasons is the new devices that are capable of recording more easily than before. In most of the cases the device used were a mobile phone camera or other video

[72] Suomen Rikoslaki 39/1889 Luku 24, 6§ ja 7§
[73] Information from the Finnish Prosecutors. Accessible: https://oikeus.fi/syyttaja/en/index/syyttajalaitos/syyteoikeudenvanhentuminen.html (19.3.2019)
[74] Vastaus kirjalliseen kysymykseen KKV 61/2017 vp, Accessible: https://www.eduskunta.fi/FI/vaski/Kysymys/Documents/KKV_61+2017.pdf (17.2.2019) (Answer to the parliament about reviewing the Chapter 24, section 5,6 and 7 regarding eavesdropping and illicit recording.)

camera,[75] but even though the drones are not yet represented in the statistics as many as other recording devices, the privacy threat is still real.

The laws and regulations with drones are still in the beginning whereas traditional aviation industry have been working for 70 years with international regulations and the self-regulation works well in the industry because the international regulations have made basically all national legislations very similar.[76] In 2014 Roger Clarke criticized in his paper "The regulation of civilian drones' impacts on behavioural privacy", that because the drone industry is involved with technology, there are often more promises than deeds from the technology companies. This means in other words, that he does not believe that the drone industry could self-regulate itself what it comes to privacy, security, technical requirements or geographical limitations and there should be international and national regulations on the drone industry.[77] As in many news during the past years, we have seen that his prediction in 2014 was relatively accurate. There are still many drone companies that have taken the different privacy and security aspects seriously and tried to make the flying of drone as safe as possible.[78]

3.2 Drones and privacy overview

The question about privacy concerning digital material is all the time more important when the society is turning more and more into a digital world. Many of our normal and daily activities are often related to Internet and digital services and so are also photos and videos, and as any digital material they can be compromised even if one would take all the possible precautions to keep them safe. It is not always what one does, but more of what others do. Many of our daily activities include transferring of information from one device to another and also drones use often Wi-Fi, Bluetooth, a Smartphone or other gadgets to control and transfer the recorded or live footage. This material can be stolen from the device or the drone and the material end up to someone who is not authorized to have them. The material can also include GPS information that

[75] Koskinen, A. L., Mies kuuli ääniä eteisessä ja alkoi nauhoittaa naista salaa – salakuuntelu ja -katselu yleistynyt Suomessa: "Mistään harmittomasta ei ole kyse", 10.11.2018,
Yle news. Accessible: https://yle.fi/uutiset/3-10500284 (15.2.2019)
[76] María de Miguel Molina Virginia Santamarina Campos (Ed.) (2018) Ethics and Civil Drones, European Policies and Proposals for the Industry. SpringerBriefs in Law. Springer Nature. pp. 79.
[77] Clarke, R. (2014). The Regulation of Civilian Drones' Impacts on Behavioural Privacy. Computer Law & Security Review. 30. 286–305. pp.291-293
[78] E.g. DJI company have been working wit GEO fencing system to restrict flying in prohibited areas (see point 5 MEASURES TO PROTECT PRIVACY AND SAFETY, page 51-54)

can reveal the targets movements.[79] All the devices that are using Wi-Fi or Bluetooth to transfer data can be target for hacking. The hacking is just one issue with the privacy concerning drones. The other privacy issues are filming without permission or authority conducted surveillance and facial recognition.

Camera drones have taken their space in our society and there is no going back anymore. The drones will be here and they will develop to be even smaller, faster and more silent and with better cameras, recognition technology and other sensors. As Bart Custers wrote in his book "The future of drone use", times has changed with the drones. We cannot assume that even if we have had the possibility to be basically out of reach of cameras earlier, the small camera drones has changed the situation. An example about this is when a woman who was living on the 26th floor in Seattle had never had to think that someone could peer or film her while she is at her home. One day she saw a drone with a camera flying outside her window filming her and her apartment. The two men who had probably been flying the drone left when they had seen that the management that she had informed about the drone watched them.[80] There are still many cities and countries where flying a camera drone is allowed, but at the same time there are basically no places left where it would be allowed to film or take photographs inside someone's home. It does not matter if it is a camera drone or a normal camera; the law is the same for both cases because it is the camera that is used to take footage and the privacy law prohibits it if the photographs or video is taken from someone's private home.[81] The only difference is that with a drone it is easier to reach those places where it has not been possible to film or photograph before.

Drones equipped with devices that enable identification of persons makes it easy for authorities and other parties to easily find people from even crowed places. This together with the material that can be found on Internet or gathered by the authorities about persons can be dangerous in countries where the privacy and human rights are not respected, as they should. These things combined with military technology could be even a more dangerous combination. People would loose their privacy and people with unwanted ideas or opinions could be easily eliminated as in

[79] Ahmad, I. et al., 2017 "5G security: Analysis of threats and solutions", Conference Paper, September 2017, 193-199, Conference: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), At Helsinki, Finland. Accessible: https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions (14.3.2019)
[80] Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer. pp. 4
[81] Suomen Rikoslaki 1889/39, Luku 24, 1§

the fictional but still relevant video about Slaughterbots from Stuart Russel[82] that he presented at the United Nations Convention on Conventional Weapons.[83] It is a video about small killer drones with facial recognition and a small bomb that kills the target. The drone is of a size of a box of matches and it is not only one drone, but a swarm of drones which have been programmed to find the persons who the party behind the drones wants to be eliminated. The small drones are pre-programmed and they fly autonomously and find their target. When the target is found, the drone targets the person's head. When the drone hit the head, the small explosive penetrate the head, killing the person. Because of the explosive, also the drone will be destroyed and for this reason it will be difficult or even impossible to trace the party behind it. If the terrorists would get the technology they could take photos of desired targets from the Internet, program the Slaughterbots and send them to kill the targets. It is not just the terrorists, but also there could be governmental or other authorities behind eliminating people who they find as a threat. Because the drone has a small explosive, it is destroyed and can be difficult or even impossible to trace who had sent it. They are autonomous and cannot be stopped and they would create a new world order when it would be almost impossible to defend against them. The video was made to raise awareness what will possible happen if the drone technology combined with military and robot technology continues. Letters to ban the autonomous weapons has been signed already by over 20,000 researchers in the field including Elon Musk and Stephen Hawking.[84] This was just an example of what facial recognition can lead to in worst-case scenario if it is used to hostile purposes.

Besides these privacy and safety issues, also a privacy concern has raised about police and governmental surveillance. The new technologies enable clear and sharp footage from long distance, facial recognition and silent drones. China has launched project "Dove" and uses drones that can copy 90 per cent of a real doves movements. It is not in knowledge if the drones have facial recognition but at least they are equipped with cameras. The drones have been tested in several cities in China, mostly to monitor in areas where the Chinese government claim to be problems with the public order. The dove drones are really difficult to detect even on lower

[82] https://futureoflife.org/2017/11/14/ai-researchers-create-video-call-autonomous-weapons-ban-un/
[83]https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument
[84] https://futureoflife.org/2017/11/14/ai-researchers-create-video-call-autonomous-weapons-ban-un/

altitudes because they flap their wings like a real dove and they are almost silent.[85] This kind of surveillance is a major threat to privacy because it is easy to monitor from where and to where people are going, what they are doing and how they are behaving. When people cannot recognize dove drones from real doves they do not know that they are under surveillance.

In Finland the police has used drones for few years now in their work almost daily. They are used in searching operations, crime and accident scenes and during bigger events but facial recognition is not yet used in Finland by police drones.

3.3 Privacy

The concept of privacy can sometimes be difficult to determine, especially in today's information society. The first time privacy as a right was defined and taken into discussion in legal aspect, was in the end of 1890 in an article by Warren and Brandeis the U.S.A. They pointed out that everyone should have the right "to be let alone". The article took stand to privacy and how the new technology and portable cameras invaded and violated privacy and thereby discriminated the personal space. They also stressed that violating privacy can hurt and harm even more than physical violence. They also said that the court should soon take the right to privacy for consideration and determine if the law will recognize and protect the right to privacy.[86] Today in 2019, over one hundred years later, there are similar questions and discussions about privacy and cameras. Yes, taking photos without the objects consent is a violation against his or her privacy, but for example when there are surveillance cameras around the cities, is that a violation to persons privacy? Often it is said that depends how the recorded content is processed and it depends also how it is seen when a person walks in a public place.

The term privacy as a right, as we now it, is relatively new. Even if laws have been around for thousands of years, privacy as a human right has been around for a little bit over one hundred years, but as we know it today, it has been only for few decades. In 1948 when United Nations Declaration on Human Rights was adopted, there was also privacy included in Article 12. Few years later, based on the United Nations Declaration on Human Rights The European

[85] Fernández Esteban, C. China is testing creepy drones that look and fly like real birds to monitor citizens, 28.6.2018, Business Insider España. Accessible: https://www.businessinsider.com/china-is-testing-creepy-dove-drones-to-monitor-citizens-2018-6?r=US&IR=T&IR=T (12.3.2019)

[86] Warren, S. D. ; Brandeis L. D. The Right to Privacy, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890) Accessible: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents (12.3.2019)

Convention on Human Rights and Fundamental Freedoms (ECHR) was made in 1950. The ECHR Article 8 about "Right to respect for private and family life" did not expressly define privacy, but the right to private life has been seen as privacy. Later the ECHR articles have got guidelines that are amended when needed. The ECHR Article 8 has its latest guideline dated 31.8.2018[87] and there the privacy is explained in more detail including the person's photos, surveillance and collection of private data. Still today there are difficulties to determine privacy exactly and this can be because it can bee seen and interpreted differently depending how one feels about it. To determine privacy has been a difficult task and legal scholars J. Whitman and D. Solove described privacy as "an unusually slippery concept".[88]

Privacy has been during the last years been a lot in the news and other medias. With the fast developing ICT sector and especially the facial recognition an Artificial Intelligence (AI) technology, it is understandable that the question about privacy is one of the hottest topics. When we talk about privacy we should ask why privacy is so important? Is it because we do not want to share our personal life with people we do not know or is it that we do not want to be in the authorities register in case we act against rules or conduct some other illegal act? Or if we live in a country where ones opinions may be a reason to fear of ones health and life. Whatever the reason is, the privacy question is not easy to answer. If we voluntary give our personal information to be used by someone, it is our own decision and then we cannot say it would a loss of privacy. Then again if the same information is gathered to similar purpose without our consent, it is seen as a violation against our privacy. Then there are countries that collect information that even the person does not know about him- or herself. China has been in the news because of its Social Credit Score (SCS) system where basically everyone's every move is under government surveillance. The SCS system is meant to control people and how they behave. Everyone get points or points are taken away depending on their behavioural and if the persons SCS points go below a certain amount, he or she can loos his or her right to e.g. travel, go to some specific school or shop in certain shops. Points can be calculated of the money spending, video game playing, Internet behavioural and behaving on public places such as

[87] Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence. Accessible: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (5.3.2019)
[88] Rachel L Finn, David Wright, and Michael Friedewald, Seven Types of Privacy, European Data Protection: Coming of Age, Springer Science+Business Media Dordrecht 2013, pp. 4-5

smoking on a smoke free zone.[89] This is done by facial recognition by drones and other cameras, Internet surveillance and as a new method also by "gait recognition". The gait recognition measures the body shape and how people move. It does recognise the person even if the persons face would be covered and according to the developers, changing how the person walk does not affect the recognition.[90] This kind of surveillance and personal data collection is a violation against privacy because the person who lives in these cities where the surveillance is carried out has not a real choice if his or her personal data is collected and this way they basically loose their privacy. The only way to avoid the privacy loss is to move away, probably to another country, but if his or her SCS points are too low, it might be that he or she cannot travel anymore.

This kind of surveillance is like in the George Orwell's book 1984 where the Big Brother (government) is watching everyone and everything. The above described surveillance in China may sound like it is from a scientific future movie, but it is happening and there are fears that similar surveillance will spread to other countries as well and even to Europe. This is an extreme example of surveillance and how privacy is violated and in a way lost. There are different forms of privacy and people may experience privacy in different ways.

In today's information society where many, if not most of our communication and daily activities is done through computers, mobile phones and other devices that are linked to the internet, it is impossible to have full privacy. One good example of today's privacy and how one cannot have full privacy, is as Olga Mironenko Enerstvedt wrote in her book: Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles. When she wants to travel, she has to buy a ticket to an airplane. She has to type in her name, birthday and other personal information to the ordering form. The travel agency or the flight company get her information even if she would not want. After that she has to go through the security check where she is scanned with a body scanner and her luggage is scanned with x-ray and the workers can see what she have with her, and she may be even checked by hand if the body scanner beeped. There are a lot of CCTV´s and other surveillance devices at the airport that record her

[89] Nittle, N. Spend "frivolously" and be penalized under China's new social credit system, 2.11.2018, Vox. Accessible: https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games (22.2.2019)
[90] Kang, D., Chinese 'gait recognition' tech IDs people by how they walk, 6.11.2018. Accessible: https://apnews.com/bf75dd1c26c947b7826d270a16e2658a (22.2.2019)

and watch her movements. Even before she goes to the airport she have to have a passport and to that she have to give her fingerprints, full name and other personal information.[91]

If she would like to keep her privacy fully to herself, the only way would be that she would not have a passport or would not travel with vehicles that require any personal information. This is basically not an option in developed countries. The idea about privacy today is totally different what it was 20 years ago. Now we can think that we can regulate our privacy but if we want to live a normal life, we have to give up some of our privacy to be able to do things we desire and the same goes with security. We have to give up some of our privacy to the authorities to be able to have a more safe and healthy life.

The Finnish police forces want to use the photographs of the Finnish passport register for facial recognition. The new police act that is under review but it will not be allow the use of photographs from the passport register even if the police forces had hoped for it.[92] During the end of 2018 and beginning of 2019, many child abuse cases were revealed in Finland. This triggered a new opportunity to get the passport, drivers license and personal ID register to be used in more serious crimes. The Government proposed new actions how to solve and prevent sexual offences and offences by immigrants and at the same time the police would get passport photos of basically everyone in Finland.[93]

There has been a lot of discussion in the social media and news about the possibility that the police could use the passport, drivers' license and ID register in criminal investigation. In a way this can be seen as a good thing but at the same time there is a question about privacy and how the police would ensure privacy to those who are not involved in the investigation. Kai Mykkänen, the Finnish minister of the interior, said that the investigation work in sexual offences can be mentally really hard and slow for the investigators and that automated facial recognition would make it less stressing and faster for the investigators. He also pointed out that

[91] Olga Mironenko Enerstvedt. (2017) Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, Law, Governance and Technology Series, Issues in Privacy and Data Protection Volume 37, Springer International Publishing AG, pp. 25
[92] Poliisin henkilötietolaki SM064:00/2015 (English: Police Personal Data Act (under review))
[93] Ibid. Accessible: https://intermin.fi/artikkeli/-/asset_publisher/10616/hallitus-linjasi-toimia-seksuaalirikollisuuden-ja-maahanmuuttajataustaisten-rikollisuuden-torjumiseksi?_101_INSTANCE_jyFHKc3on2XC_languageId=en_US PDF available at: https://vnk.fi/documents/10616/11449843/Preventing+and+combatting+sexual+crime/821a9e5d-f9dc-e5d2-f57f-efa2cec7caa0/Preventing+and+combatting+sexual+crime.pdf (point 13.2) (9.3.2019)

if the police have the whole register in use, they would probably find the suspect much faster and this way the police would have a possibility to prevent further crimes.[94]

The concerns with privacy and the photos in the passport register are not just concerns. There is also a possibility that if the police can use the picture registers to facial recognition in more serious crimes, it can lead to the situation that the police start to use the register to less serious crimes and after some time it is a normal practice in every investigation where the police have footage. There is also the scenario that the police would use the register for automated facial recognition in all footage that they have to track people with even small crimes such as walking against red lights. This kind of use of the register would with no doubt make the police work much more efficient but at the same time there would be the question about privacy. If the police could use the registers as they wish, it could lead to the point where they could basically collect any data about anyone without any reason, and then we would be in the same situation as many cities in Chine with their SCS system.

The technology and the information society we live in have put a lot of pressure to our privacy. Thanks to the computers, mobile phones and the information technology we have we can do almost everything online, but at the same time when it makes our life more easy, we loose a major part of our privacy and there are all the time coming more devices and technology that requires to give personal information in order to use the device or technology in question. The same is with drones. When using a drone, it does not require to inform any personal details in Finland, yet, but with a drone the pilot can get other persons personal details such as pictures and location. If the drones are used by authorities, the information may contain also name, address, age and sex if the drone use facial recognition.

3.4 Facial recognition

The facial recognition technology has developed fast and in a report done by Frost & Sullivan in 2016, the biometrics technology industry to which the facial recognition belong to was about

[94] Teittinen, P. Hallitus selvittää passikuvien ja sormenjälkien avaamista poliisille – Tietosuojavaltuutettu on huolestunut, 25.2.2019, Helsingin Sanomat. Accessible: https://www.hs.fi/politiikka/art-2000006012856.html (24.2.2019)

US$ 1,5 billion in 2012 and it is estimated to be over US$ 6 billion in 2019.[95] Both drone and facial recognition technology is relatively new and develops on an accelerating speed so it is a challenge for the authorities to follow up and keep the laws up to date. The facial recognition is determined as biometric data[96] that is regulated by the GDPR. Even though the GDPR requires a genuine consent from the natural person to collect personal information, authorities may collect it without consent if it is necessary for public safety or interest.[97] This exception enables the use of drones and facial recognition without consent in e.g. demonstrations or protests. If the police is allowed to use drones equipped with cameras and facial recognition technology it can create a situation where the police might start to use it to monitor as a normal surveillance method. Some may say that it should be allowed and that it would make the countries and cities safer but at the same time most of the people who would be scanned with facial recognition program does not be suspected of anything and do never be a suspect. This aspect has to be taken into account.

When drones became more common, the authorities woke up to the problem whit small flying unmanned vehicles in the skies. Now, when there are already some laws and regulations for drones, but they are still developing, the people have woke up to the fact that drones can be used for surveillance with facial recognition. This fear includes surveillance drones by private, governmental and corporate drones. Because the drones are easy to fly from one place to another, they become smaller and silent, it can be difficult to see or recognize them and this may lead to that people feel like "Big brother is watching".[98] If drones start to fly in the sky in surveillance means, this will probably also lead to so-called "chilling effect".[99] The chilling effect means that people do not behave in normal way when they know that they may be watched and this cause behavioural change in people.

The facial recognition technology and the privacy threat that it brings are not just with drones, but also with all devices that can capture images. The problem or threat with drones is that they can be flown high up in the sky and still get good and sharp footage from persons. If a drone is

[95] Fujitsu Limited. Cloud-based Identity and Authentication: BIOMETRICS-AS-A-SERVICE. A White Paper by Frost & Sullivan in collaboration with Fujitsu, 2016, pp.8 Accessible: https://www.fujitsu.com/us/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf (23.1.2019)
[96] The GDPR Aricle 4 (14)
[97] The GDPR para. 55
[98] Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer. pp. 44
[99] Stalla-Bourdillon, S. et al. (2014) Privacy vs. Security, SpringerBriefs in Cybersecurity, Springer, pp.93

flying at e.g. 150 meters altitude, as it is allowed in Finland for civilians, it can be difficult to see or hear it and because the cameras that are attached to the drone are technically very advanced, it is possible to get sharp footage of people without their knowledge. If the drone is a police or other authority drone, it may have permission to fly even higher and it does probably have an even better camera than the consumer drones has, and this would give the authorities a possibility to practice surveillance without people's knowledge. Another issue with drones compared to CCTV´s and other fixed surveillance cameras is that people can avoid going to places that are equipped with surveillance cameras but with drones it is not as easy because they can change place easily. This kind of surveillance is done usually by the national authorities, but when facial recognition is carried out by civilians with a drone, it is much more difficult to know where the personal data ends and how or for what purpose it is used.

With today's technology, facial recognition can be done by almost by anyone. The process itself is not too complicated and the legislation is still developing. This is why authorities struggle with the legislation about facial recognition. We have already facial recognition in our mobile phones to unlock the phone and the OP Financial Group is the first to launch a pilot project in September 2018 where the OP´s employees can pay with their face in the company's staff restaurant. The customer shows his or her face to a camera that uses facial recognition and when the person is recognized, the program charges the items bought from the person's credit card.[100] At the same time there are already over 300 places where one can use facial recognition to pay the purchases in China. The first facial payment restaurant was taken in use in 2017, but Alipay introduced the facial payment already in 2015 in Germany in the CEBIT show in Germany.[101]

This sounds that it would make the payment faster and safer if the facial recognition is accurate. The drones have also good cameras and facial recognition and this may be also not just a privacy threat but also a question of safety of the facial payment. If the facial payment will become more common as it is predicted, there might be a possibility that drones tries to use the facial payment. There were some concerns about the contactless payment in Finland as well as in other countries where it is used that criminal's tries to scan the credit cards in crowded public places. These

[100] European Association of Co-operative Banks EACB, OP Financial Group first in Finland to pilot facial recognition payments, 18.9.2018. Accessible: http://www.eacb.coop/en/news/members-news/op-financial-group-first-in-finland-to-pilot-facial-recognition-payments.html (24.2.2019)
[101] Lee, J. Alipay launches facial recognition-based payment system at fast food restaurant in Hangzhou, 7.9.2017, Biometricupdate.com. Accessible: https://www.biometricupdate.com/201709/alipay-launches-facial-recognition-based-payment-system-at-fast-food-restaurant-in-hangzhou (25.2019)

crimes were more theoretical than real but there is still a possibility to scan the cards.[102] Then there comes the question if it would be possible to do the same with a drone and facial recognition? The facial payment is in its beginning and there are not yet so many people who have registered them self to the payment system, but when it become more common, there might be criminal who tries to use the drones to collect money, but it can also be really difficult because it needs a software that recognises the person and can link it to the right credit card. With the contactless payment it is different, because there the machine recognizes the card but not the person.

There are many facial recognition programs on the market and with today's technology it is relatively easy to make an own facial recognition program with tutorials found on the Internet.[103] Also ready facial recognition software's are widely available. When typing in "facial recognition software for personal use" in Google, one can find a huge range of facial recognition software's sold by many different companies. For the facial recognition program one need a database to compare the recognized faces, but if it is a private person who want to find one person he or she knows from e.g. an event, he or she probably have a picture of him or her and then the facial recognition program can be used. Basically if a private person uses these kinds of programs with the drones against another person he or she violates The Criminal Code Of Finland 39/1889[104] chapter 24, section 5,6 and 7 that prohibits eavesdropping, illicit observation or preparation for the above mentioned crimes.

With the new smart phones many of us are familiar with facial recognition. The phone can be unlocked with showing the face to the phone. Most of the phones facial recognitions are working well and fast. This would suggest that all the facial recognition programs are at least relatively good, and especially the authorities would have a facial recognition program that would work. Even though the smart phones facial recognition works, the reliability with facial recognition is still in 2019 a bit uncertain. According to Big Brother Watch (BBW) organisations research, the facial recognition the UK police are using is far from reliable. The report shows that the police's facial recognition work only with an average of 5% accuracy and some departments have an

[102] Biryukov, V. Are contactless payments safe? 29.7.2015, Kaspersky Lab. Accessible: https://www.kaspersky.com/blog/contactless-payments-security/9422/ (25.2.2019)
[103] Manwani, N. Face-Recognition Using OpenCV: A step-by-step guide to build a facial recognition system. 23.10.2018, Hackernoon. Accessible: https://hackernoon.com/face-recognition-using-opencv-a-step-by-step-guide-to-build-a-facial-recognition-system-8da97cd89847 (5.3.2019)
[104] Suomen Rikoslaki 39/1889 Luku 24

accuracy of only 2%. The BBW claims that the police has taken photos of almost 2500 falsely identified persons and stored them to a database without their knowledge and that it violates their privacy. The facial recognition system has given false matches and the police have checked identity of over 30 persons who have been informed by the system to be someone else. Of the almost 2500 alerts the facial system gave, only 15 arrests were made and that is only 0,005% of all the matches.[105] The author could not find any information about the Finnish police, because the facial recognition law in Finland is still under review. The police have basically all it needs for automated facial recognition, the programs, drones, cameras and their own photo register of criminals. The Finnish police are now waiting for the new Police Personal Data Act to be decided if it will be passed. If it is passed, the police are ready to start using facial recognition.[106]

For the moment, the author of this thesis thinks that the law about facial recognition in Finland is a bit confusing. Private persons and companies, schools and other institutions can use facial recognition if they have the consent from the persons who are recognized, while the police do not have yet permission to use it. Omnia vocational school tried a facial recognition system for participation in lectures in December 2018.[107] Many schools have been interested in the same system and also in Sweden there was a similar experiment.[108] The schools say that it reduces the teachers' work when the system checks who has participated to the lectures. In Omnias´info sheet it did not say how many students were participating the testing and how many refused. In Sweden the English news did not specify this either, but in Finnish news it was told that it was a 30 persons class from which 21 gave their consent to facial recognition and 26 gave their consent for tagging them. From the 30 students one student's parents did not give permission for facial recognition and the rest 8 did not answer.[109] The police have started to test facial recognition

[105] Big Brother Watch repot, Face Off - The lawless growth of facial recognition in UK policing May 2018. pp. 3-4. Accessible: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[106] Havula, P. MTV: Poliisiylijohtaja haluaa kasvojen-tunnistuksen valvonta-kameroihin – "En havittele mitään poliisivaltiota", 17.6.2018, Iltasanomat. Accessible: https://www.is.fi/kotimaa/art-2000005723344.html (15.3.2019)

[107] Omnia vocational school's info about facial recognition. Accessible: https://www.omnia.fi/uutiset/omniassa-testataan-opiskelijoiden-lasnaolon-seurantaa-kasvojentunnistuksen-avulla (18.3.2019)

[108] Lynn, A. Facial recognition tested in Swedish high school, 15.1.2019, Electronic Specifier. Accessible: https://www.electronicspecifier.com/artificial-intelligence/facial-recognition-tested-in-swedish-high-school (19.3.2019)

[109] Helminen, L. Kasvojentunnistuksella varmistettiin, onko oppilas koulussa – Suomalainen Tieto asensi kameran ruotsalaiseen luokkahuoneeseen, 15.1.2019, Helsingin Sanomat. Accessible: https://www.hs.fi/teknologia/art-2000005966231.html (19.3.2019)

already in the beginning of 2018 on its own personnel,[110] but as mentioned, the police have to wait until the new law is passed, if it is.

4 DRONE USAGE

When you see a drone in the sky, the first thing you probably think is, that is it filming and is it filming you? This is unfortunate as the drones can be used to many other things as well than just spying. It is nice to get breathtaking footage of an amazing sunset over the city or filming your best moments when paddling on the sea, but here again people around you might be suspicious about your drone. There are also plans for commercial drones that they would deliver packages or pizza to you, but here again the same suspicions would probably raise. The surveillance with drones are in its early stage, and we do not exactly know how well it works or does it cause a real threat to privacy, but that might be the reason that people are afraid of the consequences of surveillance drones when there is not knowledge. People had similar fears about mobile phone cameras when they became more common, but as we have seen, now days it is a rare mobile phone if it does not include a camera and people does not mind them. We are also already used to CCTV´s and other fixed surveillance cameras and most of us do not even notice them anymore. When and if surveillance drones become more common, the time will tell if the same happens with drones as with the CCTV´s and other fixed security cameras, or will it be different because of the drones' ability to move and that people does not know where they might be. The author thinks that with the civilian and commercial drones, the same thing happens as with the mobile phone cameras. After they become common enough, and pilots respect the rules, they will be flying without people getting disturbed about them.

4.1 Authority use of drones

The authorities are using drones for many different purposes and in many ways. The use of drones by the authorities is not just the surveillance of citizens, but also forest management, counting wild animals, observing different natural phenomenon, fighting forest fires, border

[110] Nyman, R. Kaleva: Suomen poliisi testaa kasvojentunnistus-teknologiaa, 12.1.2018, Iltalehti. Accessible: https://www.iltalehti.fi/kotimaa/a/201801122200663171 (19.3.2019)

surveillance and checking road conditions to mention few.[111] To the above-mentioned activities that the authorities are doing with drones, privacy issues are usually not involved because the drones are not equipped with technology that can identify persons. These drones are used for maintenance, observation and other similar purposes. There is a small risk of privacy issues also in these activities if the recorded material would be available for the police forces, then they could basically run facial or other recognition program to identify possible persons in the material but this is basically just an hypothetical risk. Other purposes of drone use by the authorities can be different kind of rescue missions, fire fighting, border control and of course surveillance.

The surveillance of big protests or events with thousands of participators with drones starts to be relatively common. Another surveillance area is the border control that has started to increase the use of drones for surveillance. The use of drones for border surveillance is not yet widespread and the use of drones also depends on the country in question and which border to control if it is useful and are there some advantages compared to normal border control. The main advantages with drones are that there can be border surveillance on a much larger area. The drones used for border surveillance are usually bigger drones, more of a military grade than civilian or commercial drones. The drones can be equipped with infrared, heat or motion detectors that help to detect if there are movement in the border area. Furthermore compared to manned flights, drones can detect more easily the movement than a human and there are no human error possibilities. It is also safer because the drones can operate for a long time, up to 20 hours whereas a manned flight would require change of pilots and refuelling. Also the use of drones reduces costs when fewer personnel need to patrol the area.[112] The question about privacy is somehow relevant what it comes to border control with drones. Here again it depends which border is under surveillance. In south Europe where irregular migrants are trying to get to Europe, there is much more people crossing the border unlawfully[113] whereas the border between Finland and Russia is relatively quiet compared to the south Europe. The Russian border control

---

111 Rengel, A. (2013) Privacy in the 21st Century, Koninkl ijke Brill Koninkli jke Brill nv, Leiden, The Netherlands. Martinus Nijhoff Publishers. pp.60

112 Marin, Luisa. (2016). The deployment of drone technology in border surveillance, between techno-securitization and challenges to privacy and data protection. https://www.researchgate.net/publication/302591065_The_deployment_of_drone_technology_in_border_surveillance_between_techno-securitization_and_challenges_to_privacy_and_data_protection (A part of book: Forthcoming in "Discourses of Privacy and Security", Routledge)

113 Završnik, A. (2016) Drones and Unmanned Aerial Systems, Legal and Social Implications for Security and Surveillance. Springer International Publishing Switzerland. pp. 101-102

of irregular immigration is rather effective, and this reduces the attempts to cross the Finnish border unlawfully. Most of the irregular immigration attempts from Russia to Finland get caught at the Russian border.[114] The privacy aspect with border surveillance with drones can be compared to a normal boarder control because the persons, who are recorded by a drone, are violating two countries laws if they are crossing the border without permission. If the person would be able to get to the country, the recorded data could be used to track the person later on if the police are using facial recognition. The boarder guards could send the recoded material to the police, and the police could put the persons picture to the program and compare it to the surveillance material to be able to locate the person. Here the facial recognition system and all the surveillance footage would be a good tool to prevent crimes and to locate irregular migrants. The use of drones to find irregular immigrants can be a useful tool in big cities. The drones can monitor the streets, parks and other public places with facial recognition and inform when the suspect is found. There are laws and regulations but there are also always people who do not follow them. The authorities come at some point to a limit when just laws and regulations do not be enough, and at this point the surveillance usually increase.[115] This has happened in many countries, but in Finland the use of drones, facial recognition and other surveillance is more of a precaution, and it gives a signal that even if it relatively safe, the authorities want to increase their power of surveillance.

4.1.1 Authority drones, a possible threat to privacy?

When we talk about privacy and drones, there are usually few different things that come up that people think is a threat to privacy. The first one is drone surveillance done by authorities and the second one is civilian or commercial filming or surveillance with drones. The civil and commercial filming or surveillance is not exactly surveillance but if footage of persons are recorded, stored and processed somehow, it can be a threat to privacy. The recording itself is not a big threat but when it is stored and analyzed, it become a database, and when the database is big enough, it is easy to find specific persons from the street or monitor on a specific group. Also if the database is hacked or leaked, the privacy is threatened. The police use drones for

[114] Winberg, V. Yle News, 12.7.2014 Venäjä nappaa laittomia rajanylittäjiä kiinni jo ennen Suomen rajaa – silti painetta EU:n itärajalla riittää edelleen. Available: https://yle.fi/uutiset/3-7349266 (15.3.2019)
[115] Broeders, D. (2009) Breaking Down Anonymity, Digital Surveillance of Irregular Migrants in Germany and the Netherlands, Amsterdam University Press. pp. 84

surveillance, but how does it effect the privacy and how does citizens react to that? There is still often a thought that "Nothing to hide, nothing to fear", but this is maybe because of lack of knowledge of what companies, people or authorities can do with the personal information. Even if many think that they can protect their privacy, they put their information everywhere and many do not worry about increased surveillance because they think it is only for the wrong doers, they probably will end up in some database and even be a victim of identity theft.[116] As we saw in the last U.S president elections, our private information was leaked to third parties that used it to direct campaigns and tried to change opinion of the voters. There was some 50 million persons Facebook information that Cambridge Analytica used without permission.[117] This was information taken from Facebook and it is different kind of information than the authorities gather, but if the authorities would start to use the information they have gathered from the citizens, it would be much worse and the people would be more afraid than now when it was a company behind it. This happened in China, Xinjiang when a private company who works for the government had a database of 2,5 million citizens and it was available for anyone. This information was not given by the citizens, but collected by surveillance drones, CCTV cameras, facial recognition and other surveillance devices and methods. This is covered in more detail in section 4.4. This is why it is important that if the authorities collect biometric data or any other information about its citizens, the data shall be stored safely so that third parties will not get that information. This is also one of the reasons why the GDPR was made, to give better protection for the personal data.

The technological surveillance the police and other authorities do is to reduce crimes and to make the environment safer. The police in New York tried this at Times Square in 1973 when the crime rates were on top level. They wanted to reduce the crimes because the tourists and businesses had started to suffer. The video surveillance did not go as planned and there were only ten arrests during two years. Later in 1981, the New York police made its first large-scale video surveillance at Columbus Circle station with 76 cameras to reduce crimes, but the outcome was not as hoped. The crime rate actually raised by 30% after the surveillance started, even when

[116] Perry, S., Roda, C. (2017) Human Rights and Digital Technology, Digital Tightrope. Macmillan Publisher Ltd. Springer Nature. pp.76-77

[117] Cadwalladr, C., Graham-Harrison, E. The Guardian News 17.3.2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Accessible: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (23.3.2019)

the police had believed that the video surveillance would reduce them.[118] The raise of the crimes could not be explained. In many cases, just a sign of possible camera or drone surveillance is enough to reduce crimes in this particular area. According to Järvinen in his book Ysityisyys, there is certain amounts of surveillance that usually reduces the crimes and make people feel safer, but when that amount of surveillance is exceeded, the surveillance feels as unsafe as the crimes but there are no guarantees that the crime rates are reduced.[119] The problem with the drone surveillance in the light of privacy is that the drone cameras are the newest technology and enables clear footage from a long distance and can be flown almost everywhere. When people are walking on the street, they probably do not have any idea that a drone is filming them from a distance. This is problematic in Finland, because the GDPR prohibits biometric data collection, if it is not explicitly necessary for general safety or other national safety reason. Now, a new Civilian Intelligence Act has been approved on the 11.3.2019 by the Finnish parliament that gives the Suojelupoliisi (SUPO(Safety Police)) the right to do almost all kind of surveillance even without suspicions. This means that the police can use drones, Internet and other surveillance basically on everyone. SUPO and the police would like to have also the facial recognition, but law that would possibly allow using it, is still under review. If there is no use or evidences of any crimes, the police have to delete all the material about that person immediately, but they do not need to tell those under surveillance about it. The act was passed to be able to fight terrorism, organized crime and other serious crimes.[120] The law was reviewed and checked that it is in line with the EU and international laws, but even tough, it gives an impression that it could be challenged, because the SUPO does not need a real suspicion to do surveillance, even if the laws states that unnecessary interference with persons privacy shall be restricted. The ECHR Art. 8 prohibit authorities to interfere privacy if it is not to protect the national and public security and safety or to prevent a crime. The GDPR Art. 9 is similar but there it is stated that it is prohibited to process personal or biometric data without a legal reason. The laws give the authorities the right to interfere with people's privacy for reasons such as national safety and public order. In one way it is a good, but on the other hand it can pose a privacy threat if the authorities are not controlled how they use their power. With the new Civilian Intelligence Act the SUPO get the right to do surveillance on people even if they would not be suspected of any crime or suspected for preparation of such. SUPO claims that it will use the surveillance only to

[118] Yesil, B., (2009) Video Surveillance: Power and Privacy in Everyday Life, LFB Scholarly Publishing LLC. pp.40-41
[119] Järvinen, P. (2010) Yksityisyys, Turvaa digitalinen kotirauhasi, WSOYpro Oy. pp. 109
[120] Ministry of the Interior, Press release, 11.3.2019. Accessible: https://intermin.fi/en/article/-/asset_publisher/siviilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta

persons who might be, or is suspected to be involved in criminal activity. This means that if a person is seen together with a suspect, the person might be put under surveillance just in case.[121] The law about the use of passport and driving licence photo register in criminal investigations and in facial recognition is still under review, but if it will pass, the police will get a powerful tool from it together with the drones.

Besides the facial recognition made by drones, there are also programs that can detect suspicious behaviour. The program can recognize if there is a fight, if someone leaves a bag and leaves, shootings and so on. This kind of program in a drone is useful for the police to keep order and act faster when there is a need. Moreover, this kind of program is also safe when taking the privacy in account. The drone does not recognize the person, but only how he or she is behaving and with this the police get the information where the police is needed without knowing who it is.[122]

Furthermore, a drone can be equipped with a Wi-Fi__33 hotspot that can read the data that is transmitted from another Wi-Fi. When a drone equipped with a Wi-Fi__33 hotspot is used, the drones hotspot takes over the Wi-Fi that is wanted to monitor. If the police use the drone hotspot, the suspected persons devices connects to the hotspot without the suspects knowledge and all the traffic that goes through the Wi-Fi__33 hotspot can be monitored by the police. This option can be used by the police in criminal investigation, but this can also be misused especially if it is available for everyone to buy. If a Wi-Fi can be monitored from a distance, it poses risks for privacy. Another thing that can be done is to block or jam the Wi-Fi. Neither of these options is for the moment fully working but in the future these can be used.[123]

The use of drones by the police does not require facial recognition, and the police can use drones to carry out surveillance without it. There have been discussions in the U.S about drones and police surveillance. Many have said that the 4th amendment[124] does not necessary protect people

[121] Hallituksen esitys HE 202/2017 vp. Acessible: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_202+2017.aspx
[122] Järvinen, P. (2010) Yksityisyys, Turvaa digitalinen kotirauhasi, WSOYpro Oy. pp. 109
[123] Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer. pp. 108
[124] U.S Constitution, amendment iv (1791) The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants

in their homes from drones as long as the cameras can see only what a human eye can see, even if it was from the air. This means that as long as the drone does not have infrared or other sensors that can see through walls and roof, the police can carry out surveillance without a search warrant.[125] In Finland the situation is different. The police cannot conduct surveillance without a permission from the court, and to be able to do video surveillance, the crime, the suspect has done have to be serious and the minimum sentence has to be one-year imprisonment.[126] Because of this, the police cannot use drones that often to conduct drone surveillance above someone's home but in public places there are no such restrictions. The Finnish police have the right to record footage at public places such as streets, parks and markets from cars, drivers, pedestrians or persons participating in events on a public place if there is information about technical surveillance in that area.[127] This kind of technical surveillance is possible in cities because the police can put signs more easily to city centres than to sub-urban areas. If the police is using drones for surveillance purposes without informing about it, it is not technical surveillance but more of normal surveillance if it is not directed to some specific person or group. This is still a bit unclear regarding the Finnish law. The police are allowed to use cameras, even body cameras that film all the time, but because the drones are still quite new, it is not exactly clear how the law is regarding drone surveillance. The police have already used drones for surveillance in larger events, but for normal drone surveillance there is only laws about recoding in general such as with body cameras. There is also a difference regarding law about drones and body cameras, namely, that body cameras can compromise the privacy if the police go in to someone's home with the body camera recording where the privacy is strict. Drones then again are flying outside and are filming usually only in public places.[128] It is important that the use of drone surveillance is regulated strictly by the law, otherwise even a democratic state can turn into a police state even without noticing it before it is too late.[129] If the police is able to follow citizens every move and knows where they are, what they do and whit whom, it is a extremely serious violation on the privacy

---

shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

125 Ambrosio, D. (Ed) 2014, Domestic drones - Elements and considerations for the U.S., Nova Science Publishers, Inc. pp. 55

126 Pakkokeinolaki 806/2011, Luku 10, 19§

127 Poliisilaki 872/2011 Luku 4, 1§ (Police act)

128 Lehtonen, T. (2016) Mikrokamera poliisin työvälineenä – Oikeudellisia näkökulmia, Poliisiammattikorkeakoulu, graduation thesis, pp. 15 and 30. Accessible: https://www.theseus.fi/bitstream/handle/10024/117585/Lehtonen_Tommi.pdf?sequence=1 (20.3.2019)

129 Haque, A. (2015) Surveillance, Transparency, and Democracy : Public Administration in the Information Age. Tuscaloosa : University Alabama Press. pp.41-42

There is a difference how authorities and civilian or companies can use drones and sensors attached to it. The Finnish law is strict what it comes to authorities. The law states clearly what the police or other authorities can and cannot do. One of the laws is regarding all sorts of surveillance and how and where it can be gathered. The police have to follow strictly the Police Act[130] about surveillance, the Criminal act[131] and the Constitution[132] about privacy and the Personal data act[133] about personal data and how, what, where and for how long the data is stored and/or processed. These are few of the important laws that regulate the footage recording done by the police. As Caputo in his book Digital video surveillance and security said, the authority surveillance is safer than the filming a paparazzi or a civilian do. This is because a civilian or a paparazzi usually have their personal agenda for filming and the recorded material can end up in public places and can harm the recorded much more than the surveillance the authorities do. The material of authority surveillance is kept safe with strict confidence and used according to laws, but when other has similar footage, there is no one who controls it.[134] The book was written about the U.S., but the same situation is also in Finland. The surveillance footage is well controlled what it comes to the police or other authorities in Finland, but there is basically only few laws and rules regarding recording footage by civilians or companies. Recoding footage by civilians or companies is very un-regulated but then again publishing it, is a very different thing. There are many of the same laws that regulate the police such as the Criminal, code, the Constitution and Personal data act that restrict the publishing of such material to protect the privacy. The police are usually not publishing any material so it is more about recording, but the laws are also regulating the publishing, because if one publish pictures or video about an identifiable person, it might violate this persons privacy.

4.2 Civilian and private company drone use

As discussed in the previous chapter, the recording of footage is very un-regulated in Finland for civilians and companies. This does not mean that one can record where or whatever, but more that video recording or picture taking e.g. in public places are generally allowed. According to TRAFI, there are over 3000 drones and 2416 commercial drone operators from which around

[130] Poliisilaki 872/2011 (Police act)
[131] Rikoslaki 531/2000 and 879/2013 (Criminal code)
[132] Suomen perustuslaki 11.6.1999/731 (Finnish constitution)
[133] Henkilötietolaki 523/1999 (Personal data act)
[134] Caputo, A. C.. 2014, Digital video surveillance and security, 2nd Edition, Elsevier Inc. pp. 8

10% is operating on the security sector and the rest in many different areas.[135] For the security companies as well as for other companies, mainly the same laws and rules apply for them as for civilians. As long as the pilot has visual contact to the drone, and the drone is lighter than 3kg, there is no need to inform TRAFI about it.[136] Many of the operators use bigger drones because they have to carry different devices and companies need also often longer flight time. The civilian drones have usually from 15 to 30 minutes flight time, whereas the professional drones can have up to hours long flight time. When bigger and more heavy drones are used, the operators have to follow the TRAFI regulation OPS M1-32 where it is established the rules when operating a bigger drone. As mentioned before, Finland has very liberal rules regarding drones. One reason for this is that TRAFI want to encourage drone use and to give companies advantage of the liberal legislation. The EU is harmonizing the drone regulations, but there will probably be two to three years transition time. Of course the new legislation have to taken into consideration when planning the use of drones, but for now, it is quite easy. Because the same rules and laws apply basically to civilians and companies there is no need to separate them in this chapter. The law about privacy is not always clear and it depends on the case if a violation against someone's privacy is made. If it is allowed to fly with a drone in a public place, and the pilot is filming person x, even if x would be identifiable but the video is neutral and published in a neutral manner, there is probably no violation against privacy. Even if a private person would film a person with a drone several times in a public place, it is not necessary violating the person's privacy. It depends on many different things, such as what is the relation with the filmed person and the one who is filming, is it published and in what kind of context and can it cause harm to the filmed person.[137] Because the liberal laws regarding recording footage, it is difficult to know exactly when the privacy is violated. Another problem is the interpretation with the Finnish privacy law. It is seen that when a person go to a public place, he or she is willingly taking a risk to be recorded on video or picture and basically the freedom of taking pictures or video is stronger than the person's privacy when the person is on a public place.

The privacy questions concerning drones and public places are difficult, and for the moment there are only restrictions about where, whit what and how high a drone can fly. The filming

[135] TRAFI Drone operator list, updated 15.1.2019. Accessible: https://www.droneinfo.fi/fi/lentotyo/rpas_tilastot (21.3.2019)
[136] TRAFI legal drone info. Accessible: https://www.droneinfo.fi/en/how_to_fly_safely (21.3.2019)
[137] Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi, HE 184/1999 vp. pp.15
(English: Government proposal to Parliament to reform the penal provisions for violation of privacy, peace and honour)

with a drone is for the civilians and companies basically the same whereas the police use is much more regulated by the law.

4.3 The danger with drone surveillance

The surveillance is growing all over the world with an increasing speed as well as the development of technology, drones and different types of surveillance devices and programs such as facial recognition. In today's world, when there are a threat of terror attacks, drug and human trafficking and other serious crimes without underrating less serious crimes like robberies, assaults and vandalism, the surveillance seems to be a relatively good tool to fight these crimes and make the cities safer for the citizens. When CCTV´s are recording on the streets, drones are monitoring wide areas from the sky and other sorts of cameras are filming people walking by, it sounds like the city is a big surveillance city where everything is monitored and you cannot hide from the all-seeing authorities. This kind of surveillance sound more like it would be Dystopia from George Orwell's 1984 science-fiction book, where Big Brother sees and hears everything. Well, luckily we are not there yet, but in China, there is a city that the surveillance have reached new records. Xinjiang, a city with around 20 million citizens from which about 10 million are Muslims with different origins. Most of the Muslims are Sunni Muslims. It is not in knowledge how many CCTV´s, drones or other surveillance devices there are, but an Internet expert found that the register, a Chinese surveillance company had was open for everyone and could be accessed. Later this was fixed and put behind a firewall. The expert found that there were personal data of 2,5 million Xinjiang residents, names, addresses, location data etc. It was noticed that there were almost 7 million GPS locations in 24-hour periods. These locations were often labelled as mosque or hotel.[138] China has also used dove drones[139] for surveillance and many activist, experts and human right experts have said that Xinjiang is Chinas surveillance laboratory. Besides the GPS tracking China is using facial recognition and it has came to knowledge that the AI and rest of the software's that are used for facial recognition are built for only one purpose in Xinjiang, namely to track Muslims. We do not know if the footage

[138] Editorial Board, China has turned Xinjiang into a zone of repression — and a frightening window into the future, 23.2.2019, The Washington Post. Accessible: https://www.washingtonpost.com/opinions/global-opinions/china-has-turned-xinjiang-into-a-zone-of-repression--and-a-frightening-window-into-the-future/2019/02/23/780092fe-353f-11e9-854a-7a14d7fec96a_story.html?utm_term=.7a1f84bf524c (28.2.2019)
[139] See point 3.2 Drones and privacy overview

that are used for facial or gait recognition are from CCTV´s or drones but it does not matter.[140] What matters is that it is alarming that the technology enables this kind of ethnic minority surveillance.

This could probably never happen in countries where the rule of law is strong and where new laws are checked before they are passed that they are in proportion to the desired result and e.g. in the EU there are common laws on privacy that prohibits surveillance if it is weakening the protection of privacy unnecessary. If any politics would even suggest this kind of surveillance as in Xinjiang, even if it would not be targeted to only one group but for every citizen, it would be a political suicide. In EU there are common regulations and laws that prohibits this kind of ethnic profiling, and even this kind of mass surveillance violates many laws in EU and Finland. To name few of the laws that prevent this kind of surveillance in the EU is the ECHR Art. 8 to respect private life that reduce such kind of mass surveillance and then the Finnish Police Act that prohibits surveillance of persons without a reason as well as the Finnish Criminal Code that prohibits illicit recording and eavesdropping if there is not a reasonable and legal reason and the police have also to get permission to conduct this kind of surveillance.

This kind of surveillance a state practices is not just alarming but also dangerous. It is estimated that over 1 million people have been sent to concentration camps and most of these people are Muslims.[141] It had not been possible to select mostly Muslims to the camps without a widespread and mass surveillance. This raise fears that there are ethnic cleanings under progress in China. The different surveillance devices enables this kind of surveillance and the technology is developing all the time more and the recognition of individuals gets all the time easier. All of these features such as facial and gait recognition, GPS tracking and Internet surveillance can be done through a drone. The technology does not yet allow a large-scale use of drones with these features but in the near future it will, because now in 2019, these features can be already be used in drones but they are on an early stage so they are not yet reliable enough .

[140] Kuo, L. Chinese surveillance company tracking 2.5m Xinjiang residents, 18.2.2019, The Guardian. Accessible: https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents (28.2.2019)

[141] Editorial Board, China has turned Xinjiang into a zone of repression — and a frightening window into the future, 23.2.2019, The Washington Post. Accessible: https://www.washingtonpost.com/opinions/global-opinions/china-has-turned-xinjiang-into-a-zone-of-repression--and-a-frightening-window-into-the-future/2019/02/23/780092fe-353f-11e9-854a-7a14d7fec96a_story.html?utm_term=.7a1f84bf524c (28.2.2019)

When the drone technology develops further, they can be used instead of CCTV´s and other cameras on streets and in places where the drones can see the ground and operate as they have been planned to because one drone can easily be used instead of tens of fixed cameras. Because the drones are easy to fly from one place to another, also more remote areas can be under surveillance when earlier they have been out of reach of surveillance cameras. This is why it would be important to see, research and understand the possible risk and threats to privacy.

5. MEASURES TO PROTECT PRIVACY AND SAFETY

The development of drones has brought new possibilities to use them to many different purposes. The drones have also brought problems with them, such as privacy and safety issues. The Finnish authorities are aware of the problems, but they have not wanted to restrict the drones too much to give them the possibility to develop and so that Finland could become more advanced in the use of drones.[142] Because there are limited ways to protect the privacy and safety through legal measures concerning drones, the authorities and civilians should have also alternative measures to protect them self. The difficulty with the law, related to drones and privacy, is that if a good stage of privacy is achieved it might restrict the use of drones too much and the advantages of drones are gone. This is why it is important to have laws and regulations combined with technical measures. When planning on other measures, the law and privacy has to be taken into account so that there are no conflicts between the parties. Sometimes protecting privacy and safety only through law can be hard, because there are always those who do not follow the laws and if we want also these persons to be covered, very strict laws or even ban has to be made. This option is not good and that is why there have come many new technical measures to protect the privacy together with the law.

The police forces in Finland will get more power to take actions against drones flying or filming in prohibited places or if the drone causes or may cause danger or disturbance to the general safety in 18th of March 2019.[143] The rescue department as well as the police have noticed that drones are often flying and filming around accident scenes and this can be a risk to the rescue

[142] See capter 4.2

[143] Finnish Police Personal Data Act (Poliisin henkilötietolaki SM064:00/2015) (under review) Accessible: https://vnk.fi/documents/10616/11449843/Preventing+and+combatting+sexual+crime/821a9e5d-f9dc-e5d2-f57f-efa2cec7caa0/Preventing+and+combatting+sexual+crime.pdf (point 13.2) (9.3.2019)

mission and also to the privacy of the victim. Furthermore flying a drone around an accident scene can also generate new accidents if the drone fall down or hit something or someone. Flying a drone close to nuclear plants or oil factories, prisons, military areas or if the drone flies over crowds or otherwise is a threat, the police can take actions against the drone. The Finnish police forces does not yet have any specific tools to drop, jam or hijack a drone except normal guns, but use of guns with bullets in residential area is not safe. The are plans to get new technology and tools to the police forces and an estimations of the price is from tens of thousands up to hundreds of thousands euro's.[144] There are already jamming and hijacking guns on the market such as Dronegun Tactical. It is a gun that shoots a signal up to 1km and the drone can be either brought down controlled by the Dronegun operator, or sent back to the starting point to be able to track the pilot. The Dronegun is manufactured by Droneshield company that focuses to develop and sell their products to governments and authorities.[145] This kind of gun would be good to tackle the illegal drone flying because it does not harm bystanders, it is silent and because it does not drop the drone from the sky, it is safe to use also in crowded places. This kind of gun against the drones can be extremely useful to prevent terror attacks done by drones. In a hypothetical case where there is a stadium concert with 70,000 people, the police see a drone trying to fly over the stadium. There might be explosives or chemicals loaded on the drone. With a Dronegun or similar, the police could take total control of the drone and land it to a safe place and disarm it without casualties. In 2014, the FBI arrested a person who had planned to fly a consumer drone with a homemade bomb to a school.[146] The threat of this kind of terror attacks is real and if the drone is already in the air, it is important that the police have resources to battle them.

There are always people who do not follow the rules, and there are not many ways to get these people to obey the law. This is one reason why the leading consumer drone and aerial photographing manufacturer DJI is launching a new version of its Geospatial Environment Online (GEO) 2.0 system in 2019. In 2013 it made No-Fly Zones for the drones and in 2016 it launched a more sophisticated GEO system where it had included also nuclear plants and

[144] Yle News, Police allowed to stop drones if new law steps into effect, 21.2.2019. Accessible: https://yle.fi/uutiset/osasto/news/police_allowed_to_stop_drones_if_new_law_steps_into_effect/10657737 (27.2.2019) Finnish version: Parviala, A. Poliisi saa valtuudet kaapata droonin lennosta – tiukemmat säännöt voimaan kuukauden kuluttua, 21.2.2019, Yle Uutiset. Accessible: https://yle.fi/uutiset/3-10657112 (27.2.2019)
[145] Droneshield. Accessible: https://www.droneshield.com/dronegun-tactical (27.2.2019)
[146] Wassom, B., D. 2015 Augmented Reality Law, Privacy, and Ethics:
Law, Society, and Emerging AR Technologies. Elsevier Inc. pp.220

prisons. The DJI geofencing prevents the DJI drones of flying close to airports or other sensitive places. Their new 2.0 geofencing system will come to 32 European countries. To the new GEO 2.0 system are included 19 more countries that did not have advanced geofencing. DJI is working together with Altitude Angel[147] which is an aviation technology company which also work with authorities. The new GEO 2.0 system is said to be flexible so that it can place temporary restrictions for drone flying during special events or similar. This kind of technology makes the drone flying much safer when the drone does not fly if it is inside a no-fly zone.[148] This is a great improvement but there is a small problem. The GEO 2.0 has to be downloaded to the flight control application. If a pilot does not download the new version, the pilot can still fly in a no-fly zone. This was at least the situation with the old version. The author himself has a DJI drone and hi tested to take-off with the drone inside a house without downloading the update for the geofencing system. The drone was lifted to 1,5 meter without the update, even if the house is within 500 meters of an airport. In a legal aspect, the authorities could require all drone manufacturers to have a geofencing system and make it mandatory to download the software before the drone could fly.

Other measures that could improve safety and privacy could be that all drones would have a small sensor that sends a signal with a code. The code should have the information of the owner of the drone and in a case when a drone is suspected to fly in restricted area, private land or filming without permission, the code could be taken e.g. with the TRAFI´s drone app and the code could be sent to the authorities who could investigate if there was some kind of violation. This code could be read only by the authorities to ensure also the pilot's privacy. The author does not know if it is technically possible to get the register code to a smart phone, but this or a similar solution would ensure better privacy and safety, when there is a big possibility to get caught if filming or flying against the laws.

When the facial recognition become more common, the question about privacy will become even more important. There are laws about it regarding police and authorities, but not for civilians and companies. It will probably be easy to implement programs and devices to drones that enable facial recognition, so the author think that the best way would be to prepare a new law about facial recognition before it becomes a problem. The law should determine if facial recognition is

[147] Altitude Angel Ltd. Accessible:https://www.altitudeangel.com (12.2.2019)
[148] DJI News. Accessible: https://www.dji.com/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities (12.3.2019)

allowed to be used in drones, and if yes, who can use and what kind of precautions should be taken to ensure the privacy. This would need further research to be able to decide how the facial recognition issue can be solved. If the facial recognition for some reason would become a norm, one could protect one's privacy whit covering his or her face. It is not convenient, and in some countries it is prohibited to use scarves or similar that cove the face, but there is another way. One could use a mask that looks almost like the person wearing it, but the face is made a bit different from the real one, and then the facial recognition system would not recognize this person. This is an extreme example, but it may be one solution for those who do not want to be recognized in public places but does not want to stand out either with a totally covered face.[149]

6. CONCLUSION

Different types of UAV´s, RPAS´s or drones as we know them better, have been flying around our skies for about five decades. Unmanned, and even remotely piloted air vehicles have been around for a century even though the first ones were remotely piloted airplanes. First the military showed its interest to drones, because it could reduce own causalities, give valuable information with its surveillance ability, and later the drones were able to precisely bomb the enemy. When hobbyist started to get interested to fly their own small drones, the first drones were difficult to operate and probably because of that, the bigger crowd was not so interested in them. When the technology and development of consumer drones began to increase in the beginning of 2000, also some companies understood that the drones could have potentially a big market. Around 2010, the boom started to bee seen. The drones came suddenly without any notice to a widespread phenomenon among civilians, companies as well as authorities. Because the extremely fast growth and development, the legislators did not keep up with the speed the drones came and now they are working on many new laws and regulations. The increased use of drones has brought many new issues and concerns, both to the authority and the private side. The first problems the increased civilians use of drones brought was the flying in places where the drones could cause a threat to safety. The biggest safety concern has probably been the flying with drones close to airports or too high so that they have been close to collisions with airplanes. This issue have been around for longer and the authorities have given new restrictions where a drone can be flown. This has not been as efficient as hoped, and new measures are planned to be taken

[149] Timan, T. et al. (Ed) (2017) Privacy in Public Space - Conceptual and Regulatory Challenges. Elgar Law, Technology and Society series. Edward Elgar Publishing. pp. 49-50

to be able to reduce the dangerous drone flying close to airports or other places where a drone could cause major damage if it crashes with or to something. These measures are so called droneguns that are able to take full control of the drone and bring it down safely. Other measures are geofencing that stop the drone from flying in restricted area. These are still relatively new measures and there are not yet concrete examples if they work or how well they work.

The other problem the drones brought is also the main topic of this thesis and it is the question about privacy. This is a problem that especially citizens have been worried about. The police use of drones for surveillance has become during the last few years more and more common. The fears of drones that are capable for facial recognition have risen because the drones are easily moved, they can do surveillance over a big area and if equipped with facial recognition system, even only one drone can be used to carry out surveillance over an event with thousands of people. With a drone with facial recognition, the police can find a specific person from an event with tens of thousands of people and this is one reason people fear of loosing their privacy. Since the start of military drones, the surveillance has been one of the main purposes for drones. Now, this surveillance method is coming to the citizens' life when drones start to fly over the cities and do surveillance. The findings during the research showed that depending on the country, if it is the U.S., China, Finland or some other EU country, there are huge differences regarding the rights of the police to conduct drone surveillance on regular basis. In Finland the drone use by the police for surveillance is not yet a danger for the privacy, whereas in China it is a significant threat for the persons privacy. The laws regarding drones and facial recognition are on an early stage in most of the countries. EU is at the moment reviewing few regulations to harmonize the drone laws in the EU, Finland got new laws that allow the police to interfere illegal drone flying and there are laws under review in Finland that would allow drones and facial recognition also for the police. Now, in March 2019, the flying with civilian drones in Finland is very liberal and there are not many laws regulating the drones if it is below 3 kg like most of the civilian drones are. If it is allowed to fly a drone in a certain place, it is basically always allowed to film as well. In public places the right to film or take pictures is sometimes even stronger than the privacy, because the person is willingly in a public place and therefore he or she give up some of his or her privacy. The Finnish law about privacy is relatively up to date what it comes to drones. Filming itself is as mentioned, almost always allowed in public places, but publishing it is another thing. The laws about privacy take a strong stand to what is allowed to be published. If footage is published of a person that is recognizable and it cause or might cause harm to the person, the laws are usually interpreted that the publication is violating the persons privacy. The

outcome of the thesis showed that what it comes to civilians, drones and privacy, the law does not restrict the drones but more of what kind of content is allowed to publish.

The privacy regarding police drones are also well covered in Finland, but it might change if the new Police personal data act is passed where the police get more rights. The SUPO got already more rights to fight terrorism, organized crime and other serious crimes. The new Police personal data act would basically give SUPO the right to carry out surveillance with facial recognition on anyone. The police would get also the right to use facial recognition, but the police would still need a strong suspicion that the person is involved is criminal activity. The new EU regulation that is to harmonize the drone laws in member states was planned to come into force in the spring of 2019, but for the moment there are no new news about it.

The drone surveillance brings both positive and negative things with them. There are maybe even more positive things because the drones can be used for many different purposes and we still do not know the whole potential of the drones. To the positive things includes search and rescue, fire fighting, checking bridges, towers and other difficulty and dangerous places and so on. The negative things are then again the threat to privacy and security. These two are extremely important topics in a democratic state. The authority use of drones in Finland and EU is on a relatively good stage and privacy is quite well respected, but there is a fear that the drone surveillance will become more common and this can cause a threat to privacy even if the privacy laws in EU and Finland is protecting the citizens. For the moment there are not ways for civilians to protect oneself from drones, except covering the face. In the future there is hopefully some kind of identification system of drones that would reduce illicit recording. The topic about drones and privacy would need further research when the new laws and regulations have been passed to see if the issues have been solved. Also because the development is very fast, the drones can get new features, they become more silent and smaller, there is a need for more research regarding the drones.

7. LIST OF REFERENSES

Scientific books:

Ambrosio, D. (Ed) 2014, Domestic drones - Elements and considerations for the U.S., Nova Science Publishers, Inc.

Banner, S. (2009) Who Owns the Sky? : The Struggle to Control Airspace from the Wright Brothers On, Harvard University Press.

Bartsch, R. et al. (2016) Drones in Society: Exploring the strange new world of unmanned aircraft. Routledge.

Bernard, C. W. (2013) Tesla : Inventor of the Electrical Age, Princeton, New Jersey : Princeton University Press.

Boghosian, H. (2013) Spying on Democracy Government Surveillance: Corporate Power, and Public Resistance. Open Media Series, City Lights Books, San Francisco.

Broeders, D. (2009) Breaking Down Anonymity, Digital Surveillance of Irregular Migrants in Germany and the Netherlands, Amsterdam University Press

Caputo, A. C.. 2014, Digital video surveillance and security, 2nd Edition, Elsevier Inc.

Chamayou, G. (2015) A Theory of the Drone, , Translated by Janet Lloyd, New Press

Custers, B. (Ed). (2016) The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives, Information Technology and Law Series Volume 27, T.M.C. Asser Press, Springer

Dvorkin, D. (2013) Dust Net: The Future of Surveillance, Privacy, and Communication: Why Drones Are Just the Beginning, David Dvorkin.

Fahlstrom, P. Gleason, T. (2012) Introduction to UAV Systems, , John Wiley & Sons, Ltd.

Gross, C. J. (2002) American military aviation : the indispensable arm, College Station : Texas A & M University Press.

Rachel L Finn, David Wright, and Michael Friedewald, Seven Types of Privacy, European Data Protection: Coming of Age, Springer Science+Business Media Dordrecht 2013

Haque, A. (2015) Surveillance, Transparency, and Democracy : Public Administration in the Information Age. Tuscaloosa : University Alabama Press.

Järvinen, P. (2010) Yksityisyys, Turvaa digitalinen kotirauhasi, WSOYpro Oy

Kaag, J. Kreps, S. (2014) Drone Warfare, Polity Press, Oxford.

María de Miguel Molina Virginia Santamarina Campos (Ed.) (2018) Ethics and Civil Drones, European Policies and Proposals for the Industry. SpringerBriefs in Law. Springer Nature

Neocleous M. (2014) War Power, Police Power. Edinburgh: Edinburgh University Press.

Newcome, L. R. (2004) Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles, American Institute of Aeronautics and Astronautics, Inc., Reston, Virginia,

Olga Mironenko Enerstvedt. (2017) Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, Law, Governance and Technology Series, Issues in Privacy and Data Protection Volume 37, Springer International Publishing AG

Perry, S., Roda, C. (2017) Human Rights and Digital Technology, Digital Tightrope. Macmillan Publisher Ltd. Springer Nature

Rengel, A. (2013) Privacy in the 21st Century, Koninkl ijke Brill Koninkli jke Brill nv, Leiden, The Netherlands. Martinus Nijhoff Publishers.

Rothstein, A (2015) Drone, Object lessons series, , Bloomsbury Academic.

Senior, A (ed). (2009) Protecting Privacy in Video Surveillance, Springer-Verlag London Limited, Springer

Stalla-Bourdillon, S. et al. (2014) Privacy vs. Security, SpringerBriefs in Cybersecurity, Springer

Timan, T. et al. (Ed) (2017) Privacy in Public Space - Conceptual and Regulatory Challenges. Elgar Law, Technology and Society series. Edward Elgar Publishing.

Wassom, B. D. 2015 Augmented Reality Law, Privacy, and Ethics:
Law, Society, and Emerging AR Technologies. Elsevier Inc.

Yesil, B., (2009) Video Surveillance: Power and Privacy in Everyday Life, LFB Scholarly Publishing LLC.

Završnik, A. (2016) Drones and Unmanned Aerial Systems, Legal and Social Implications for Security and Surveillance. Springer International Publishing Switzerland.

Scientific articles:

Ahmad, I. et al., 2017 "5G security: Analysis of threats and solutions", Conference Paper, September 2017, 193-199, Conference: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), At Helsinki, Finland. Accessible: https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions (14.3.2019)

Clarke, R. (2014). The Regulation of Civilian Drones' Impacts on Behavioural Privacy. Computer Law & Security Review. 30. 286–305. Accessible: https://www.sciencedirect.com/science/article/pii/S0267364914000570

Clarke, R. Understanding the drone epidemic. Computer law & security review 30 (2014) 230-246. Xamax Consultancy Pty Ltd. Published by Elsevier Ltd Accessible: https://www.sciencedirect.com/science/article/pii/S0267364914000545 (20.2.2019)

Hiltner, P. J. (2013). The drones are coming: Use of unmanned aerial vehicles for police surveillance and its fourth amendment implications. Wake Forest Journal of Law Policy 3(2), 397-416. Accessible: https://wfulawpolicyjournal.com/issues/past-issues/volume-32/ AND PDF: https://wfulawpolicyjournaldotcom.files.wordpress.com/2016/05/6_hiltner.pdf (12.3.2019)

Kremer, J. The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space. Doctoral dissertation, Faculty of Law University of Helsinki, 2017. Accessible: https://helka.finna.fi/Record/helka.3052131

Luppicinia, R., Sob, A.. A technoethical review of commercial drone use in the context of governance, ethics, and privacy, Technology in Society Volume 46, August 2016, Pages 109-119. Accessible: https://www.sciencedirect.com/science/article/pii/S0160791X16300033 (3.3.2019)

Marin, Luisa. (2016). The deployment of drone technology in border surveillance, between techno-securitization and challenges to privacy and data protection. Accessible: https://www.researchgate.net/publication/302591065_The_deployment_of_drone_technology_in_border_surveillance_between_techno-securitization_and_challenges_to_privacy_and_data_protection (A part of book: Forthcoming in "Discourses of Privacy and Security", Routledge)

Sullivan, J. M. "Evolution or Revolution? The rise of UAVs", IEEE Technology and Society Magazine, vol. 25, no. 3, 43-49, 2006. Accessible: https://ieeexplore.ieee.org/abstract/document/1700021

Warren, S. D. ; Brandeis L. D. The Right to Privacy, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890) Accessible: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents (12.3.2019)

EU legislation:

Regulation EU 2016/6790 (the European General Data Protection Regulation)

European Aviation Safety Agency Opinion No 01/2018, Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories

The European Convention on Human Rights and Fundamental Freedoms (ECHR)

Regulation 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Riga Declaration on Remotely Operated Air Systems
Accessible: https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf (8.3.2019)

Resolution of the European Parliament on the safe use of remotely piloted aircraft systems (RPAS), commonly known as UAVs, in the field of civil aviation (2014/2243(INI))

USE OF REMOTELY PILOTED AIRCRAFT AND MODEL AIRCRAFT IN AVIATION REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence. Available at:
https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (5.3.2019)

http://dronerules.eu/en/professional/regulations

http://dronerules.eu/en/professional/eu_regulations_updates

Other legislation:

The original Finnish legislation is accessible at: https://www.finlex.fi and English versions at: https://www.finlex.fi/en/

Henkilötietolaki 523/1999 (Finnish Personal data act)

Kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun 04.12.2018 OPS M1-32 (TRAFI/334638/03.04.00.00/2017) (Use of Remotely Piloted Aircraft and Model Aircraft in Aviation)

Suomen Rikoslaki 39/1889 and 531/2000 (The Criminal Code Of Finland)

Ilmailulaki 1242/2005 (Finnish Aviation Act)

Pakkokeinolaki 806/2011 (Finnish Coercive Measures Act)

Poliisilaki 872/2011

Ministry of the Interior, Press release, 11.3.2019. Accessible: https://intermin.fi/en/article/-/asset_publisher/siviilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta

Answer to the parliament about reviewing the Criminal code of Finland 39/1889, Chapter 24, section 5,6 and 7 regarding eavesdropping and illicit recording. (Only in Finnish. Vastaus

kirjalliseen kysymykseen KKV 61/2017 vp,
https://www.eduskunta.fi/FI/vaski/Kysymys/Documents/KKV_61+2017.pdf (17.2.2019)

Poliisin henkilötietolaki SM064:00/2015 (Finnish Police Personal Data Act (under review))
Accessible: https://intermin.fi/artikkeli/-/asset_publisher/10616/hallitus-linjasi-toimia-seksuaalirikollisuuden-ja-maahanmuuttajataustaisten-rikollisuuden-torjumiseksi?_101_INSTANCE_jyFHKc3on2XC_languageId=en_US
PDF Accessible:
https://vnk.fi/documents/10616/11449843/Preventing+and+combatting+sexual+crime/821a9e5d-f9dc-e5d2-f57f-efa2cec7caa0/Preventing+and+combatting+sexual+crime.pdf (point 13.2)
(9.3.2019)

Information from the Finnish Prosecutors. Accessible:
https://oikeus.fi/syyttaja/en/index/syyttajalaitos/syyteoikeudenvanhentuminen.html (19.3.2019)

TRAFI legal information about drones. Accessible: https://www.droneinfo.fi/fi (18.3.2019)

Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi, HE 184/1999

Other sources (in the order they are used)**:**

History of Chinese Kites. Accessible:http://chinakites.org/htm/fzls-gb.htm (21.12.2018)

https://multicoptercenter.fi/pages/miksi-ostaa-meilta (7.6.2019)

Salmisalo, V. (2015) Taivaalla surisee, Multikopterit ja niiden yleistyminen. Metropolia Ammattikorkeakoulu Medianomi (AMK) Bachelor Thesis. Accessible in Finnish at:
https://www.theseus.fi/bitstream/handle/10024/95819/Opinnaytetyo_Salmisalo.pdf?sequence=1&isAllowed=y (9.3.2019)

DJI, Mavic 2 specs. Accessible: https://www.dji.com/fi/mavic-2/info#specs (5.2.2019)

Face-Six, Identify your targets from distance! Accessible: https://www.face-six.com/drone/ (13.2.2019)

7th joint cross-border R&TTE market surveillance campaign (2015) on RPAS Final report adopted by ADCO R&TTE 51 on 21st October 2015
PDF Accessible:
https://ec.europa.eu/docsroom/documents/13343/attachments/1/translations/en/renditions/pdf (13.32019)

Amazon.de, Eachine E58 drone. Accessible: https://www.amazon.de/EACHINE-Übertragung-120°Weitwinkel-Quadrocopter-App-Steuerung/dp/B077MFPZTN/ref=sr_1_5?s=toys&ie=UTF8&qid=1545062130&sr=1-5&keywords=drone (22.2.2019)

Techradar, best drones of 2018. https://www.techradar.com/news/best-drones (20.1.2019)

Future of Life Institute, Accessible: https://futureoflife.org/2017/11/14/ai-researchers-create-video-call-autonomous-weapons-ban-un/ (27.2.2019)

The United Nations Convention on Conventional Weapons. Accessible: https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument (12.1.2019)

Fujitsu Limited. Cloud-based Identity and Authentication: BIOMETRICS-AS-A-SERVICE. A White Paper by Frost & Sullivan in collaboration with Fujitsu, 2016 (14.3.2019) Accessible: https://www.fujitsu.com/be/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf (7.3.2019)

European Association of Co-operative Banks EACB, OP Financial Group first in Finland to pilot facial recognition payments, 18.9.2018. Accessible: http://www.eacb.coop/en/news/members-news/op-financial-group-first-in-finland-to-pilot-facial-recognition-payments.html (24.2.2019)

Biryukov, V. Are contactless payments safe? 29.7.2015, Kaspersky Lab. Accessible: https://www.kaspersky.com/blog/contactless-payments-security/9422/ (25.2.2019)

Big Brother Watch report, Face Off - The lawless growth of facial recognition in UK policing May 2018. Accessible: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Omnia vocational school's info about facial recognition. Accessible: https://www.omnia.fi/uutiset/omniassa-testataan-opiskelijoiden-lasnaolon-seurantaa-kasvojentunnistuksen-avulla (18.3.2019)

TRAFI Drone operator list, updated 15.1.2019. Accessible: https://www.droneinfo.fi/fi/lentotyo/rpas_tilastot (21.3.2019)

Droneshield. Accessible: https://www.droneshield.com/dronegun-tactical (27.2.2019)

Altitude Angel Ltd. Accessible: https://www.altitudeangel.com (12.2.2019)

DJI News, DJI Improves Geofencing To Enhance Protection of European Airports and Facilities, 12.2.2019. Accessible: https://www.dji.com/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities (3.2.2019)

TRAFI legal drone info. Accessible: https://www.droneinfo.fi/en/how_to_fly_safely (3.1.2019)

SESAR, European Drones Outlook Study, Unlocking the value for Europe, November 2016, Accessible: https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf (12.3.2019)

Ministry of interior, Government proposes new powers for police to intervene in use of drones in certain cases. Accessible: https://intermin.fi/artikkeli/-/asset_publisher/poliisi-voi-jatkossa-puuttuja-dronejen-lennattamiseen-tietyissa-tilanteissa?_101_INSTANCE_jyFHKc3on2XC_languageId=en_US (27.2.2019)

Department for Transport, Civil Aviation Authority, and Baroness Sugg CBE. New drone laws bring added protection for passengers, 30.5.2018 Accessible:

https://www.gov.uk/government/news/new-drone-laws-bring-added-protection-for-passengers (6.3.2019)

EU drone rules. Accessible: http://dronerules.eu/en/recreational/eu_regulations_stakeholders (1.3.2019)

Lehtonen, T. (2016) Mikrokamera poliisin työvälineenä – Oikeudellisia näkökulmia, Poliisiammattikorkeakoulu, graduation thesis. Accessible: https://www.theseus.fi/bitstream/handle/10024/117585/Lehtonen_Tommi.pdf?sequence=1 (20.3.2019)

TRAFI Drone operator list, updated 15.1.2019. Accessible: https://www.droneinfo.fi/fi/lentotyo/rpas_tilastot (21.3.2019)

News (in the order they are used)**:**

STT, Yle News 18.7.2017. Suomessa on arviolta kymmeniä tuhansia droneja - EU kiristää Suomen löyhää lennokkilainsäädäntöä. Accessible: https://yle.fi/uutiset/3-9727680 (8.3.2019)
CNN (Cable News Network), U.S. drone registrations skyrocket to 770,000, 28.3.2017, https://money.cnn.com/2017/03/28/technology/us-drone-registrations/index.html

Helminen, L. Suomen poliisin käyttämistä suosituista kuvauskoptereista löytyi haavoittuvuus – samoja koptereita käytössä tavallisilla kuluttajilla ja yrityksillä, Helsingin Sanomat 8.11.2018, https://www.hs.fi/teknologia/art-2000005892603.html

NYTIMES, Rise in US police use of drones triggers backlash over spying and other abuses 6.12.2018, Business Times, https://www.businesstimes.com.sg/technology/rise-in-us-police-use-of-drones-triggers-backlash-over-spying-and-other-abuses (12.3.2019)
Ziemann, M., Volocopter lentää Helsingissä ensi kesänä – Kaupunkien pitää alkaa suunnitella parkkipaikkoja taksi- ja tavara-droneille 17.12.2018, Yle News, https://yle.fi/uutiset/3-10555274 (13.3.2019)

Ziemann, M., Volocopter lentää Helsingissä ensi kesänä – Kaupunkien pitää alkaa suunnitella parkkipaikkoja taksi- ja tavara-droneille 17.12.2018, Yle News, https://yle.fi/uutiset/3-10555274 (13.3.2019)

Malmber, L., Tunnelma kuin tieteiselokuvassa: Helsingin taivaalla risteili 22 poliisin miehittämätöntä lennokkia valvomassa itsenäisyyspäivän viettoa 7.12.2017, Helsingin sanomat news. https://www.hs.fi/kaupunki/art-2000005481201.html (23.2.2019)

Weaver, M., UK public must wake up to risks of CCTV, says surveillance commissioner 6.1.2015, The Guardian. Accessible: https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent (26.2.2019)

Milmo, C., Most British police forces now have drones – and they're getting better at watching us. Is this the future we want? 29.6.2018, iNews. Accessible: https://inews.co.uk/news/uk/eye-in-the-sky-drone-capable-of-spotting-violence-in-crowds-raises-questions-about-hi-tech-policing/ (26.2.2019)

McKenzie, S., Mezzofiore, G., Police hunt drone pilots in unprecedented Gatwick Airport disruption. 21.12.2018, CNN. Accessible: https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html (12.2.2019)

BBC News, Heathrow airport drone investigated by police and military, 9.1.2019. Accessible: https://www.bbc.com/news/uk-46804425 (15.2.2019)

CBC News, Airliner has close call with drone, 4,000 feet over Edmonton, 1.8.2018. Accessible: https://www.cbc.ca/news/canada/edmonton/airliner-drone-near-miss-edmonton-1.4770662 (12.2.2019)

Levin, A., Drone collisions, close calls underscore growing risks for aircraft, 17.2.2018, Washington Post. Accessible: https://www.washingtonpost.com/politics/spate-of-drone-collisions-close-calls-underscore-growing-risks-for-aircraft/2018/02/17/4b630714-1433-11e8-8ea1-c1d91fcec3fe_story.html?noredirect=on&utm_term=.4e72f8a1494a (12.2.2019)

Kilpeläinen, M. (2.10.2016) Journalismia lintuperspektiivistä. https://blogit.metropolia.fi/median-maailma/avainsana/drone/ (6.3.2019)

STT, Yle News 18.7.2017. Suomessa on arviolta kymmeniä tuhansia droneja - EU kiristää Suomen löyhää lennokkilainsäädäntöä. Available at: https://yle.fi/uutiset/3-9727680 (8.3.2019)

Linnake, T., Hittilennokin omistajia pystyi vakoilemaan – ei mitään keinoa huomata, 9.11.2018 Iltasanomat. Accessible: https://www.is.fi/digitoday/tietoturva/art-2000005894206.html

Checkpoint Software Technologies Ltd. The Spy Drone In Your Cloud. Accessible: https://blog.checkpoint.com/2018/11/08/the-spy-drone-in-your-cloud/ (14.3.2019)

Koskinen, A. L., Mies kuuli ääniä eteisessä ja alkoi nauhoittaa naista salaa – salakuuntelu ja -katselu yleistynyt Suomessa: "Mistään harmittomasta ei ole kyse", 10.11.2018, Yle news. Accessible: https://yle.fi/uutiset/3-10500284 (15.2.2019)

Fernández Esteban, C. China is testing creepy drones that look and fly like real birds to monitor citizens, 28.6.2018, Business Insider España. Accessible: https://www.businessinsider.com/china-is-testing-creepy-dove-drones-to-monitor-citizens-2018-6?r=US&IR=T&IR=T (12.3.2019)

Nittle, N. Spend “frivolously” and be penalized under China’s new social credit system, 2.11.2018, Vox. Accessible: https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games (22.2.2019)

Kang, D., Chinese ‘gait recognition’ tech IDs people by how they walk, 6.11.2018. Accessible: https://apnews.com/bf75dd1c26c947b7826d270a16e2658a (22.2.2019)

Teittinen, P. Hallitus selvittää passikuvien ja sormenjälkien avaamista poliisille – Tietosuojavaltuutettu on huolestunut, 25.2.2019, Helsingin Sanomat. Accessible: https://www.hs.fi/politiikka/art-2000006012856.html (24.2.2019)

Lee, J. Alipay launches facial recognition-based payment system at fast food restaurant in Hangzhou, 7.9.2017, Biometricupdate.com. Accessible: https://www.biometricupdate.com/201709/alipay-launches-facial-recognition-based-payment-system-at-fast-food-restaurant-in-hangzhou (25.2019)

Helminen, L. Kasvojentunnistuksella varmistettiin, onko oppilas koulussa – Suomalainen Tieto asensi kameran ruotsalaiseen luokkahuoneeseen, 15.1.2019, Helsingin Sanomat. Accessible: https://www.hs.fi/teknologia/art-2000005966231.html (19.3.2019)

Havula, P. MTV: Poliisiylijohtaja haluaa kasvojen-tunnistuksen valvonta-kameroihin – ”En havittele mitään poliisivaltiota”, 17.6.2018, Iltasanomat. Accessible: https://www.is.fi/kotimaa/art-2000005723344.html (15.3.2019)

Lynn, A. Facial recognition tested in Swedish high school, 15.1.2019, Electronic Specifier. Accessible: https://www.electronicspecifier.com/artificial-intelligence/facial-recognition-tested-in-swedish-high-school (19.3.2019)

Nyman, R. Kaleva: Suomen poliisi testaa kasvojentunnistus-teknologiaa, 12.1.2018, Iltalehti. Accessible: https://www.iltalehti.fi/kotimaa/a/201801122200663171 (19.3.2019)

Winberg, V. Yle News, 12.7.2014 Venäjä nappaa laittomia rajanylittäjiä kiinni jo ennen Suomen rajaa – silti painetta EU:n itärajalla riittää edelleen. Available: https://yle.fi/uutiset/3-7349266

Cadwalladr, C., Graham-Harrison, E. The Guardian News 17.3.2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach Accessible: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Editorial Board, China has turned Xinjiang into a zone of repression — and a frightening window into the future, 23.2.2019, The Washington Post. Accessible: https://www.washingtonpost.com/opinions/global-opinions/china-has-turned-xinjiang-into-a-zone-of-repression--and-a-frightening-window-into-the-future/2019/02/23/780092fe-353f-11e9-854a-7a14d7fec96a_story.html?utm_term=.7a1f84bf524c (28.2.2019)

Kuo, L. Chinese surveillance company tracking 2.5m Xinjiang residents, 18.2.2019, The Guardian. Accessible: https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents (28.2.2019)

Manwani, N. Face-Recognition Using OpenCV: A step-by-step guide to build a facial recognition system. 23.10.2018, Hackernoon. Accessible: https://hackernoon.com/face-recognition-using-opencv-a-step-by-step-guide-to-build-a-facial-recognition-system-8da97cd89847 (5.3.2019)

Yle News, Police allowed to stop drones if new law steps into effect, 21.2.2019. Accessible: https://yle.fi/uutiset/osasto/news/police_allowed_to_stop_drones_if_new_law_steps_into_effect/10657737 (27.2.2019) Finnish version: Parviala, A. Poliisi saa valtuudet kaapata droonin lennosta – tiukemmat säännöt voimaan kuukauden kuluttua, 21.2.2019, Yle Uutiset. Accessible: https://yle.fi/uutiset/3-10657112 (27.2.2019)

Gov.UK, From: Department for Transport, Home Office, Civil Aviation Authority, The Rt Hon Chris Grayling MP, and The Rt Hon Sajid Javid MP, New drone safety partnership with business launched as government sets out plans to limit drone misuse, 20.2.2019. Accessible: https://www.gov.uk/government/news/new-drone-safety-partnership-with-business-launched-as-government-sets-out-plans-to-limit-drone-misuse (6.3.2019)