Interaction with AI

Iteration 3

Group 3: andrgrae eivias erikhma emilylo

Contents

About us	3
Area of interest	3
Background China and SCS	4 4
Methods	5
Findings Document study Theme 1: The use of AI for producing scores Theme 2: SCS in China and its potential growth internationally Survey	7 7 7 9 10
Moving forwards	11
References	13
Appendix 1 - Chatbot design task Introduction Process Reflection and learning	16 16 16 17
Appendix 2 - Machine learning task Process Learning outcomes	18 18 19
Appendix 3 - Questionnaire Responses	21 23

About us

This project is being run by:

Andreas Græsmo - andrgrae@uio.no

Eivind Askeland - eivias@uio.no

Erik Mahlum - erikhma@uio.no

Emily Lo Kam Chuen - emilylo@uio.no

We are a group of 4 master students doing our first year of Design, use and interaction. We have different backgrounds with only one of us having a bachelor's degree from IFI while the other three have their degrees from Kristiania University College, OsloMet, and Høgskolen i Østfold.

Area of interest

We are interested in the field of Social Credit Systems (SCS), particularly the implementation of SCS by the Chinese government. It caught our attention due to interesting topics related to the ethics of Al-powered surveillance, government control, and automated decision-making. We see this system as one that is intrusive into the lives of Chinese citizens and there is a fear among us that this system could spread to other countries - including Norway - in the future.

The goal of the Chinese SCS is to "foster pro-social behaviour" by guiding people to "behave in accordance with society's interests" (Langer, 2020, p. 164). The means by which this is accomplished revolve around "automated evaluation of individual behaviour and social interactions". As a result, it is clear that this is a process where the privacy of citizens is not the top priority. Facial recognition and automated data processing are two aspects of SCS where we think AI is involved and we would like to dig deeper into the field to find out more about these in particular.

We pose the following research questions:

RQ1: How is AI used in the Chinese Social Credit System?

RQ2: How is Al-based surveillance such as facial recognition perceived by

Norwegians?

Background

The majority of the facial recognition technology (FRT) we humans experience first-hand today are benign, we mostly see it on our phones in the form of security. Instead of using a password, or our fingerprint, we can use our face as a way to identify ourselves (Gray, 2003, p. 2).

However, FRT is also used as a way for the government to survey and control the citizens. The technology is being used to enhance security in public spaces, locating missing people, fighting crime and corruption, imposing age restrictions on online viewing of pornography. These seemingly positive examples come with ethical drawbacks. Examples being biases, inaccuracies, mass surveillance and privacy intrusion (Kostka et al., 2021, p. 2).

Some countries, and cities have begun imposing regulations and bans on the use of FRT. The state of California has banned the use of FRT by law enforcement agencies. In 2020, Portland, Oregon banned the use of FRT for all city departments, including private retailers, for example hotels and restaurants (Kostka et al., 2021, p. 2).

China and SCS

The Chinese government has started implementing a social credit system in China. The reason for doing so is to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step" (Engelmann et al., 2019, p. 70). However, this statement does not consider the ethical parts of the social credit system.

The system works by giving each citizen an 18-digit ID card, called the Unified Social Credit Code (Engelmann et al., 2019, p. 69). Each individual code will have a score connected to it. How this will be used in real life is not described in the paper by Engelmann et al. (2019).

According to Engelmann et al. (2019, p. 70) there are three main reasons why the Chinese government wants and can implement this system. The first reason is that dishonest activities stand for a loss of around 92 billion USD for the Chinese government every year. The second reason is that with a credit score system a person without money can get a loan to buy a house. However the government is more interested in loaning people money that they can use on investing in the domestic market. Without a social credit score system the bank only has a credit check to control if it's safe to give someone a loan. The third reason is that privacy is seen differently in China than in the Western society. For the Chinese population this will hardly be seen as a privacy-violation. Therefore, it is easier to implement this system in China than in other countries.

Methods

In our project we would like to use different ways of collecting data in search of answers to our research questions.

A document study should give us further insight into the use of AI in connection to the Social Credit System (SCS), as well as giving us more information on how the system works and how it impacts Chinese society. While this method was primarily chosen for answering research question 1, we identified several topics and questions which were used in our data collection for research question 2.

Initially, we had a wide scope for finding articles relevant for research question 1. To cater to our area of interest we found articles which addressed SCS and China. We used Google scholar, ACM digital library, and IEEE Xplore: digital library. We then decided to narrow down our search to articles which dealt with the ethical aspects of

SCS and how AI is used in this context. The AI technology we focused on was facial recognition and AI-assisted/AI-powered decision-making.

We had planned on using interviews as our main data gathering source for trying to answer the second research question. In some part due to the scope of the assignment and our limited time however, we have decided that a survey is more suited for this task. In order to gather enough data through interviews, we would have had to interview many people to end up with a representative data set to analyze. We want to gather a broader set of views in order to be able to explore varying opinions and potentially see some emerging themes.

We have decided to dampen our explicit focus on the social credit system in this questionnaire. Instead, we will focus on general opinions of AI, as well as facial recognition as a tool for individuals, organizations and the Norwegian government. This is still relevant to our case, as it tries to highlight opinions related to the ethics of surveillance systems such as the SCS, while also trying to gauge where the line should be drawn when it comes to the use of AI technology such as facial recognition by different actors.

The questionnaire was made in Google Forms. With this tool we could then spread it through social media. We used both single choice and open-ended questions. The results from single choice questions would give us an overall view of people's relationship with Al-surveillance. Following with open-ended questions to get more depth and opinions from the participants.

The questions investigate how familiar the respondents are with the technology, and explore how negatively or positively they view certain subjects related to our second research question:

Hva er ditt syn på hvorvidt norske myndigheter burde benytte kunstig intelligens og ansiktsgjenkjenning til å forhindre kriminalitet?
○ Veldig negativt
○ Negativt
○ Nøytralt
Opositivt
○ Veldig positivt
O Det er komplisert
○ Vet ikke

Findings

Document study

Theme 1: The use of AI for producing scores

A core component of the SCS is the calculation of a score for each citizen (Engelmann et al., 2021; Langer, 2020). This score can increase or decrease depending on various events related to different aspects of the life of a citizen. Similar systems are already in use by banks, especially in North America. The data which the score is based upon are meant to give an estimate of how reliable an individual is when it comes to paying back a loan.

The paper by Yu et al. (2020) looks at how to use social media data to create such a score. The purpose of the score is for banks to get another way to give out loans. As the bank operates today, they don't lend out money to people who don't pass the credit risk check. With the current system, people that are trustworthy but don't have credit can't get a loan.

To make this system work they use machine learning to get a score. First, they make categories to find abnormal users (Yu et al., 2020, p. 9-10). For example, advertisers and other companies also use social media, but should not be given a credit score.

To find these users the AI looks at how many followers and followees an account has. An account with many followers but few followees can be categorized as an abnormal user.

The next step is to clean the data so the machine learning doesn't make wrong calculations based on wrong data. For example, the score can't be affected if your activity has been high one day but low every other day (Yu et al., 2020, p. 11). After this the AI system makes a calculation based on your activities, followers, who you are friends with, how many books you bought and so on. In the end you are ending up with a score based on an AI systems judgement.

This is interesting to our research due to the fact that the Chinese SCS has undoubtedly taken much inspiration from the banking sector with regards to the use of AI technology, such as machine learning, with the aim of gathering and processing online data on Chinese citizens.

Al-produced scores can also assist humans in making decisions. Al is widely recognized for its ability to analyze and learn from patterns in data (ACM, 2018). The accuracy of machine learning (ML) algorithms can rapidly be improved to match, or even surpass that of humans for specific data sets. The importance of having "humans-in-the-loop" in automated processes has been much discussed (DeArteaga et al., 2020; Norman, 1990). While the outcome of Al using ML may appear very accurate statistically, humans can be capable of identifying when it makes mistakes.

In the case of child welfare risk assessment in Allegheny County, an Al-tool was used to assist call workers in their assessments of whether or not an incoming call about concerns of child maltreatment should be screened in or screened out for investigation. De-Arteaga et al. (2020) conducted a study focusing on the question of whether humans are "capable of identifying cases in which the machine is wrong, and of overriding those recommendations". Their findings indicate that human intervention with regards to "erroneous algorithmic recommendations" can reduce its harmful effects. In other words, the score produced by the ML algorithm should not be trusted blindly, and having humans-in-the-loop is encouraged. These findings also concur with the findings of Norman (1990).

Theme 2: SCS in China and its potential growth internationally

Prior to the implementation of SCS in China, the government was involved in what was called the Golden Shield Project. This was China's plan to link all of its state's individual surveillance networks with a large centralized online database to automate information sharing. This has only become feasible as of recently (Wong & Dobson, 2019, p.224), and as technology proceeds to evolve, the SCS system has integrated AI tools such as facial recognition. China is believed to own the world's largest surveillance camera network with 176 million surveillance cameras, and this number is expected to increase up to 626 million by 2020 (Wong & Dobson, 2019, p.224).

A question we had been asking ourselves was "how likely is it for a country to implement AI-surveillance and how widespread is it already?" According to Feldstein (2019), a breakdown of military expenditures in 2018 shows forty of the top fifty military spending countries also have AI surveillance technology. Perhaps even more worryingly, there are quite a lot of technologies linked to Chinese companies that are found in at least sixty-three countries worldwide. The Chinese tech giant Huawei alone is responsible for providing AI surveillance technology to at least fifty countries (Feldstein, 2019, p. 11).

Feldstein (2019) presents three AI surveillance techniques, smart cities/safe cities, facial recognition system, and smart policing. Smart cities focus on making the city safer, with sensors, facial recognition and police body cameras. This is in order to prevent crimes, ensure public safety and respond to emergencies. Facial recognition systems involve biometric technology to match and compare live footage of individuals with images from a database. The last technique, Smart policing, is a data-driven technology used to facilitate investigations and police response. An example being the use of an algorithm to make a prediction of future crimes (Feldstein, 2019, p. 16). These predictions can run the risk of being inaccurate however, as Amershi et al. (2019) argues that AI systems could respond differently over time and their behaviour can be unpredictable.

Survey

The age of the people who answered the questionnaire is very homogeneous (see Appendix 3). Only one of the respondents was not in the age group 19-28. This may have affected the variance in the answers that were given, for example due to the fact that we would generally expect younger people to be more familiar with different technologies.

As we see in the second question, 53,3% of the respondents say they have a positive relation to AI. 47,7% of the respondent say they are neutral, which indicates that no one answered that they have a negative relation to it. This came as a surprise, because an impression of ours is that people generally have some negative feelings towards AI. Following this, the respondents answered how well they know facial recognition. 40% answered that they are either familiar, well familiar or very well familiar, which indicates that a large number of the respondents have a good basic understanding of AI. We think this may explain some of the answers to the first question, because many of the respondents know what AI can do and what kind of limitations it has. It might have been a more negative relation to AI if the group of people with limited familiarity with AI had been higher.

On the question of facial recognition use in public, over 50% of the respondents answered that they are either negative or it's complicated. However, about 60% answered that they are positive or very positive about using AI and facial recognition to prevent crime, and in a way these answers give us some mixed signals as they appear quite contradictory.

On the open question about negative aspects, one of the respondents answered that AI can have negative consequences if it is used by the wrong people. The respondent explained further that AI is not a problem as long as the government or company that uses it are trustworthy and if they are open on what data is saved and how it is used. However, the majority of the respondents answered that they are worried about their data being misused, with 26.7% being worried and 40% being worried to a lesser degree.

While analysing the open questions we noticed that in the question concerning positive aspects of using AI in surveillance, 10 out of 14 responses referred to crime

related aspects or increased safety. While this might be because that is the general viewpoint of the respondents, there might also be a possibility that this is influenced by the very last question concerning the use of AI to prevent crime.

In the question concerning the negative aspects, the majority of answers given showed that the respondents were worried about the privacy aspect. One of the respondents wrote that a negative effect of constant surveillance is that people will behave as if someone is watching. The concern is that people will behave as "good" as they can all the time and their freedom to be themselves will be gone, and this will affect all people, not only criminals.

Moving forwards

At this point in our study of SCS, Al-powered surveillance and the ethics surrounding these, we have explored some of the surface-level topics and themes. We recognize that what we have found so far may not be sufficient to answer our research questions. Our preliminary findings have given us a good basis for further research into some of the more complex and perhaps interesting aspects of our area of interest.

The questionnaire has given us useful insight of how Al-based surveillance is perceived by some Norwegians. If we were to move forward with this study, we would have further investigated how negative attitudes to surveillance in public spaces are intertwined with the positive attitude towards using Al-based surveillance against crime, even though they appear contradictory. We would like to know if the positives seem to outweigh the negatives and where people draw the line for what is acceptable.

We would have liked to use methods which are more qualitative in the future. We have discussed interviews as a possible method, this would give us more opportunities to branch out from the ready-made questions and dig deeper into emerging themes.

We would have liked to also look at how SCS affects the life of the Chinese. For example, in which situations do the Chinese have to "use" their score? Is SCS something that affects Chinese everyday life? These topics could be important background information for creating interviews because we could then have concrete examples of what the conditions are like for Chinese citizens. A core question we would like to ask builds upon our second research question and is as follows: where do Norwegians agree and disagree with China's extensive use of surveillance?

Further inquiry into the effects of Al-assisted and Al-powered decision-making could contribute to society by giving us a better understanding of how new technologies impact national and local governance, as well as the general population. From our document study, we discovered that Al surveillance technology could contribute to predicting future crimes through the means of algorithms with technologies such as facial recognition where images could be compared to a database, and sensors. We have also found examples of how Al technology such as machine learning algorithms can sometimes be wrong or biased, and how this should be dealt with. In the context of Al-surveillance and decision-making with regards to SCS, we would have explored these topics in more detail, as we feel we have only seen the tip of the iceberg so far.

References

2018 ACM A.M. Turing Award Laureates. (2018). Retrieved 12 November 2021, from https://awards.acm.org/about/2018-turing

Amershi, S., Weld, D., Vorvoreanu, M., Fourney, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P. N., Inkpen, K., Teevan, J., Kikin-Gil, R., & Horvitz, E. (2019). Guidelines for Human-AI Interaction. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13.

https://doi.org/10.1145/3290605.3300233

Engelmann, S., Chen, M., Dang, L., & Grossklags, J. (2021). Blacklists and Redlists in the Chinese Social Credit System: Diversity, Flexibility, and Comprehensiveness. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 78–88. https://doi.org/10.1145/3461702.3462535

Engelmann, S., Chen, M., Fischer, F., Kao, C., & Grossklags, J. (2019). Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines «Good» and «Bad» Behavior. *Proceedings of the Conference on Fairness,*Accountability, and Transparency, 69–78. https://doi.org/10.1145/3287560.3287585

F. Langer, P. (2020). Lessons from China - The Formation of a Social Credit System: Profiling, Reputation Scoring, Social Engineering. *The 21st Annual International Conference on Digital Government Research*, 164–174.

https://doi.org/10.1145/3396956.3396962

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment* for International Peace, 42.

Gray, M. (2003) 'Urban Surveillance and Panopticism: will we recognize the facial recognition society?', Surveillance & Society, 1(3), 314–330. https://doi.org/10.24908/ss.v1i3.3343

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671–690. https://doi.org/10.1177/09636625211001555

Wong, K. L. X., & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. *Global Media and China*, *4*(2), 220–232.

https://doi.org/10.1177/2059436419856090

Yu, X., Yang, Q., Wang, R., Fang, R., & Deng, M. (2020). Data Cleaning for Personal Credit Scoring by Utilizing Social Media Data: An Empirical Study. *IEEE Intelligent Systems*, 35(2), 7–15. https://doi.org/10.1109/MIS.2020.2972214

De-Arteaga, M., Fogliato, R., & Chouldechova, A. (2020). A Case for Humans-in-the-Loop: Decisions in the Presence of Erroneous Algorithmic Scores. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3313831.3376638 Norman, D. A. (1990). The "Problem" with Automation: Inappropriate Feedback and Interaction, not "Over-Automation.". *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences , Apr. 12, 1990, Vol. 327, No. 1241, Human Factors in Hazardous Situations (Apr. 12, 1990),* 585-593.

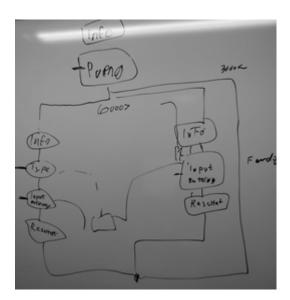
Appendix 1 - Chatbot design task

Introduction

In this assignment we created a chatbot. We tried to connect this assignment to our topic in the group assignment, social credit system. The idea we had was a chatbot that treats people differently based on their social credit score. We ended up creating a chatbot that helps people get loans, but gives different offers based on their score.

Process

In the beginning of the process we started to sketch how the flow in the chatbot should look like. The first box was a greeting box, where the user gets information of what the chatbot can help with. Further, the chatbot would ask what the social credit score of the user is. We decided that the maximum score was 12 000 and then we split the flow in two, those under and those over 6000. The flow for those over 6000 would get more options and better conditions on their loan. We then decided to add a third flow to the system, and this would be for those who have a score under 3000. These people won't get any loan from the bank, because of their low score.



Then we started to create the chatbot. In the beginning we needed to learn how Chatteron works and therefore we watched some tutorial videos on the webpage. This helped us learn some of the basic tools needed to create our idea. During the creation of the bot, we figured

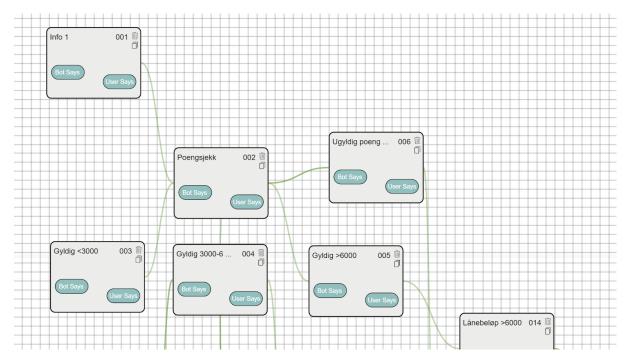
out that we would have to add some elements that we didn't have in our sketch. As an example, if a user provides an invalid input, in our case not a number, the flow needs to take the user back so they can try again.

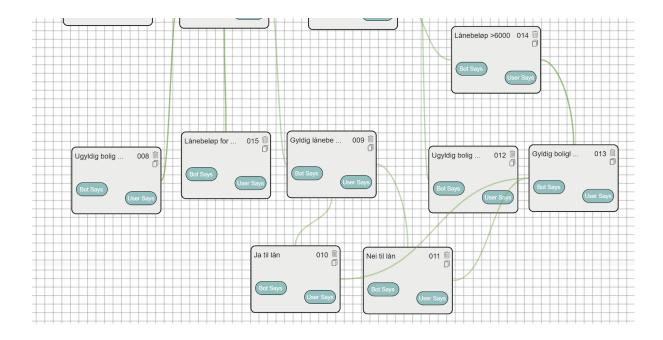
Reflection and learning

We created a chatbot that is simple and missing many of the processes that are necessary to get a loan, for example credit check. But it still shows how the idea works. Our simple chatbot still needed a lot of paths to get through the system. One question ended up having a minimum of two paths to proceed, and our question had only numeric answers. This shows how complex a chatbot is. To create a chatbot with many different answers and questions is difficult, especially if the user can write long answers. What may seem like an easy answer demands a lot of information underneath the surface to make the chatbot able to respond, even with a simple flow-based chatbot such as this.

To get a good flow was something we learned through this process. If the user writes something that is not expected, the chatbot needs to give the user the opportunity to try again. In our chatbot the user was sent back to the question if it was not answered like expected.

Chatbot flow structure in Chatteron:





Appendix 2 - Machine learning task

Process

We spent a lot of time initially trying to understand the code to figure out which numbers we could manipulate in order to see any changes in the training of the chatbot. While the code was not very descriptive, we found out that changes in the batch number and epoch values seemed to have the biggest impact, while changing the "Dense" value in the model also had some minor effects. When we added a dropout to the model of 0.3 the accuracy number seemed to fluctuate up and down a bit more. The number changed from 0.15 to 0.18 after every epoch. Without dropout the accuracy was consistently 0.15 until it changed to 0.17.

Throughout this working with this task, we have been very confused by the output values of the neural network's training. We still don't really have a good understanding of what the loss and accuracy values actually mean and how they correlate to how the bot responds to our input. The difference between val_loss and loss was also not apparent. We ran into some issues where the script would randomly crash after no more than 20 inputs from the user:

Chatbot crashing

Learning outcomes

It seems to take a very high amount of iterations for the chatbot to exhibit any form of intelligence. We have not yet seen any signs of this. We change the batch size to 512 and later to 1000, and change the epochs to 10000. Still the accuracy was 0.17 and the interaction with the chatbot was confusing.

```
Val_accuracy: 0.0000e+00
Epoch 9995/10000
2/2 [samessamessamess] - 0s 15ms/step - loss: 2.6205 - accuracy: 0.1722 - val_loss: 12.4610 - val_accuracy: 0.0000e+00
Val_accuracy: 0.0000e+00
Val_accuracy: 0.0000e+00
2/2 [samessamessamess] - 0s 15ms/step - loss: 2.6227 - accuracy: 0.1722 - val_loss: 12.4459 - val_accuracy: 0.0000e+00
2/2 [samessamessamessamess] - 0s 15ms/step - loss: 2.6192 - accuracy: 0.1722 - val_loss: 12.4459 - val_accuracy: 0.0000e+00
Epoch 9997/10000
2/2 [samessamessamessames] - 0s 15ms/step - loss: 2.6192 - accuracy: 0.1722 - val_loss: 12.4444 - val_accuracy: 0.0000e+00
Epoch 9999/10000
2/2 [samessamessamessames] - 0s 16ms/step - loss: 2.6198 - accuracy: 0.1722 - val_loss: 12.4244 - val_accuracy: 0.0000e+00
Epoch 9999/10000
2/2 [samessamessamessames] - 0s 15ms/step - loss: 2.6198 - accuracy: 0.1722 - val_loss: 12.42110 - val_accuracy: 0.0000e+00
Epoch 9999/10000
2/2 [samessamessamessames] - 0s 15ms/step - loss: 2.6248 - accuracy: 0.1722 - val_loss: 12.4279 - val_accuracy: 0.0000e+00
Epoch 9999/10000
Epoch 9999/
```

High validation loss (12.4) after 10 000 epochs

It was very hard to tell what actually makes a difference and what doesn't. This might be connected to using too few iterations or layers. However, we didn't find what we were supposed to increase or do differently to get a better chatbot. As the chatbot replied with the movie lines, we were confused by whether it had any correlation to what we wrote to the bot. At some point the replies indicated that the chatbot had understood what was written by us, however we were quickly disappointed when the next line seemed to be completely random. We are therefore left with the feeling that it doesn't matter what we write to the chatbot. Its internal workings are a black box to us as users.

Appendix 3 - Questionnaire

Spørreundersøkelse om AI – ansiktsgjenkjenning og overvåkning I vårt prosjekt ved Universitetet i Oslo ønsker vi å finne ut hva personer i Norge mener om teknologier som tar i bruk kunstig intelligens for å yte forskjellige tjenester. Vi ønsker også å se på enkelte etiske sider ved dette. Hva er din alder?
0-18 år 19-28 år 29-35 år 36-50 år 50-70 år
86+ år Hvordan vil du beskrive ditt forhold til kunstig intelligens (Al) generelt? *
Veldig negativt Negativt Nøytralt Positivt Veldig positivt
Hvor kjent er du med digital ansiktsgjenkjenning? * Ikke i det hele tatt Veldig lite kjent Litt kjent Kjent Godt kjent Veldig godt kjent
Hvordan er ditt forhold til bruk av Al til enkle personlige tjenester? (Eks. låse opp mobiltelefon) * Veldig negativt Negativt Positivt Veldig positivt Veldig positivt Vet ikke

Er du bekymret for at data om deg (f.eks bilder) kan brukes til andre formål enn de du ønsker at * de skal brukes til? Nkke bekymret Litt bekymret ○ Nøytral Bekymret Veldig bekymret O Vet ikke Annet... Hva er ditt syn på bruk av ansiktsgjenkjenning i offentlige rom i Norge (Eks. identifikasjon på flyplasser)? Veldig negativt Negativt ○ Nøytralt O Positivt Veldig positivt Oet er komplisert O Vet ikke Annet... Hvilke positive sider ser du ved bruk av ansiktsgjenkjenning for overvåkning? Lang svartekst Hvilke negative sider ser du ved bruk av ansiktsgjenkjenning for overvåkning? Lang svartekst Hva er ditt syn på hvorvidt norske myndigheter burde benytte kunstig intelligens og ansiktsgjenkjenning til å forhindre kriminalitet? Veldig negativt Negativt ○ Nøytralt Ositivt Veldig positivt Oet er komplisert O Vet ikke Annet...

Responses

