Security at any price? Predictive policing and surveillance in times of artificial intelligence

In my opinion, predictive policing falls into the thematic areas of data privacy, social consequences, as well as the ethics of autonomous AI. In the following, I would like to discuss the opportunities, risks and tough questions on the topic, since we are all affected by them. I'll start with a brief definition of predictive policing and the change AI brings with all of its autonomous abilities. After a short explanation of pros and cons I will briefly deal with an arising question.

What is Predictive Policing? In the classic sense, it is the Analysis of case data to calculate the likelihood of future crime for controlling the deployment of police forces. So far, the technique was mainly used to predict burglary offenses by drawing on geographically referenced police statistics, such as the kind of offense, time or place and non-police data, such as weather data or distance to the nearest highway. [3] For me, what's interesting now is when AI comes into play in the form of autonomous surveillance systems, with the pretext to make even more accurate predictions or to provide even more security.

Advocates often argue with theses of a reactive nature. So, preventing and responding to crime, such as being on the spot faster, inhibiting by presence, finding criminals, or detecting conspicuous behavior. For the sake of scarcity, I will not go into further detail, but I admit that these procedures can be quite positive in terms of policing efficiency.

On the other side, I see enormous dangers for the cohesion of our societies, the security of each one of us and the specific limitations and threats to each individual.
First, what happens if you are in the wrong place at the wrong time and automatically fall into a grid that can have far-reaching consequences. For example, you could be wrongfully denied loans or rejected during the application process just because you have been classified as a source of danger. What is particularly frightening is that facial recognition or even gait recognition systems [4] used in this case bring with them high false positive rates. In concrete terms, if applied broadly this means hundreds of thousands of wrongfully suspected people, who may then fall into a certain category, such as posing danger or drug offender, which is then propagated into all kinds of other aspects. [1]
Furthermore, there is a risk of exploiting once established infrastructure. By that I mean that with a change in the political system, these originally well-intentioned means can simply be misused to oppress political opponents, to find people or to participate in the information war. Specifically, people can be tracked down by camera systems and even protests can be defeated or attenuated by targeted counteractions. [2]
These examples are intended to show how great the danger is when police work together with surveillance is not only carried out but increasingly automated by AI. From this, many concrete hard questions can be deduced in my eyes. I focus on the following: Who decides on the one hand about the extent and on the other hand on the degree of independence of these systems with regard to the decisions to be made? Maybe the solution lies in the Synergies between man and machine. Machine processes detect hazards and provide judgments, whereas humans make decisions in order to prevent possible false judgments.

It certainly can not be in our interest to suspend all people to these circumstances without being able to ensure safe procedures. Even if, absolutely hypothetically thought, absolute correctness is attested, the people who live with it should be informed about the technology and decide together with their representatives about their use.

Concluding, it should be the goal to find the right balance to take advantage of the benefits of this technology to fight and solve crime while at the same time preserving privacy and security.

References

[1] Facial recognition false positives: What they really mean. `https://allevate.com/index.php/2018/05/10/how-to-measure-facial-recognition-error-rate/`, 2017. [Online; accessed 20-May-2019].

[2] Pentagon wants to predict anti-trump protests using social media surveillance. `https://www.vice.com/en_us/article/7x3g4x/pentagon-wants-to-predict-anti-trump-protests-using-social-media-surveillance`, 2018. [Online; accessed 20-May-2019].

[3] T. Karppi. "the computer said so": On the ethics, effectiveness, and cultural techniques of predictive policing. *Social Media + Society*, 4(2):2056305118768296, 2018.

[4] The Royal Society. Forensic gait analysis: A primer for courts. `https://royalsociety.org/~/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf`, 2017. [Online; accessed 20-May-2019].