FIVE QUESTIONS

ON SURVEILLANCE TECHNOLOGY IN THE US AND GERMANY

WITH CARMELA TRONCOSO

Ms. Troncoso, according to media reports, US Immigrations and Customs Enforcement (ICE) uses Palantir software called Elite to track down migrants who might be living in the United States without valid residence permits. How does the app work and what is so problematic about it?

First of all, I am not a lawyer and can only answer on the basis of my knowledge and expertise. Elite allegedly has access to extensive information from public and private sources. This information is then utilized by AI to infer a probability score on whether a person could be a target for ICE. *A priori*, they do not know who the targets could be, which is a key difference to how law enforcement normally works – identifying a suspect and then getting information on them after a court order. The app also infers a confidence score on a particular address for a person of interest after processing data like bills, social media posts, family links, economic status, future plans, or hobbies. This is extremely problematic, as it allows the creation of arbitrary criteria which can then be applied without transparency or control.

AI reasoning and decision-making processes are often criticized for being opaque and inexplicable. Are human outcomes now at the mercy of this black box?

The inferences the app makes are not certain by definition. "A confidence score" means that there is always a chance that people may be targeted without reason. A system that uses automated targeting cannot be built in a proportional, reasonable manner, in contrast to the kind of targeted surveillance that we have nowadays. What's more, such an AI system is not interpretable, meaning that it is not possible to understand why errors happen.

The far-right AfD party in Germany is sympathetic to the idea of establishing a task-force like ICE in Germany. Would the use of an app like Elite be possible in Germany, despite the fact that this would contravene Germany's Basic Law?

The use of an identical app would be difficult as the same sources of information do not exist in Europe. Sensitive medical data, banking data, or telephone records cannot be freely accessed or processed for the purpose of profiling and targeting people. But the data exists and thus can be accessed with subpoenas, or by penetrating the system. However, there is a lot of available information around that can be crawled or acquired. Even with less extensive information, very damaging applications could be created. For example, individuals have data footprints on social media and the web that could be used to infer a movement profile. Similarly, we have shown that even AI tools which are designed to automatically moderate online conversations and filter false information, bullying, or hate speech, will be biased or work based on confidence. So, in some cases, they cannot distinguish right from wrong. We must always be very careful when making decisions based on AI.

The company Palantir that supposedly built the app used by ICE, also built Vera, which is used by the German police. What is the difference between Elite and Vera?

Looking at news reports, Vera only uses information from police records. This is in contrast with Elite, which gathers external sources to make inferences. So, in my view, Vera is not a light version of Elite. In my understanding, repurposing data from records to train AI models is prohibited by the General Data Protection Regulation. However, Vera uses AI and it suffers from issues similar to those experienced by Elite: data collected for purposes other than surveillance and targeting is reused for this purpose without consent, transparency, or control. In addition, inferences made by Vera will have errors and will be systematically biased towards certain subgroups. As is the case with Elite, Vera is not a proportional tool, as it will generate surveillance on and cause harm to innocent people.

Do we need to guard against autocratic/dictatorial tendencies in data protection?

From my perspective, autocratic tendencies are not the reason we should be better protecting our data. We need to protect it better because having data that is accessible and usable by anyone creates a world in which manipulation is easier – potentially by governments but also by private parties that use this data for their own profit. Protecting personal data should be a high priority in any case.

Interview: Tobias Beuchert

Carmela Troncoso is Scientific Director at the Max Planck Institute for Security and Privacy in Bochum

ILLUSTRATION: SOPHIE KETTERER FOR MPG