**CONCLUSIONS**

The reliability and assimilation of AI technology in security systems require fairness and respecting privacy and ethical regulations. However, intelligent systems rely on knowledge, which usually forms biased AI systems both by design during development and also via training procedures using biased data sets. Significant work has been done regarding the techniques of detecting biases in data sets on specific features and ways of refinements.5, 9, 14 As a complement to this, we suggest a way of incorporating legal regulations in bias detection procedures to target biases of legal importance. Our solution corresponds to a binding of legal unstructured text information and the quantitative algorithmic procedures of automatic AI systems. The outcome of our system is the compliance of the intelligent components of a surveillance system with the legal framework as designed by legal official authorities.

Even if any bias in intelligence systems is successfully detected, the final goal is to alleviate it and restore fairness. Our research aims at the refinement of input data sets to be in compliance with legal frameworks without losing accuracy. However, most of the time, bias in data sets results from the lack of general knowledge about human behavior for all cases of sensitive data. In surveillance systems, the result is that intelligence components can infer potential threats only for specific sensitive data groups that are available, which, of course, is unfair. Our further research focuses on simulation models that enrich intelligence-component-training data sets

with data that are as coherent as possible with the real visitors’ behavior and simultaneously maintaining the compliance of the data set with the legal framework.