

December 14, 2023

Israeli Court Criticizes Predictive AI Output for Being Unexplainable and Unjustifiable

Client Updates

Over the past year, we have all been caught up in the AI storm. Wherever we turn, artificial intelligence is on everyone's mind. New AI systems are being launched daily, companies that brand themselves as AI companies receive great attention and significant investments, and it seems like every day there is another conference or seminar dealing with various aspects of artificial intelligence and its use. The legal arena of AI has not been left untouched – in legislation (which is still in its infancy, with the most significant efforts being made in the EU – [see our recent client update on this matter](#)), in pioneering litigation in this uncharted legal territory, and of course in numerous law firm updates (like this one...).

The reason for all the commotion is the breakthrough entry of generative artificial intelligence (GenAI) into our lives, with the launch and immense overnight popularity of GenAI tools such as ChatGPT, CoPilot, Midjourney and others – all of which have amazed us with their ability to generate texts, images, and other wonderful works. But with all the hubbub surrounding GenAI, we tend to overlook that other category of AI tools, Predictive AI, which has been present in various aspects of our lives for several years now.

Predictive AI tools are AI systems that assist us in making decisions by predicting future events and trends. These serve as operational and decision support tools. Predictive systems analyze vast data and variables and "predict" probabilities for future behaviors, patterns and events. In the business sector, they may help predict consumer preferences, market trends, loan repayment capabilities, when to expect a "sales peak", etc. In healthcare, they may provide medical predictions based on tests, personal information and medical history. In autonomous vehicles, they can predict the likelihood of an accident in a given situation. When we navigate using a navigation app, it predicts the fastest route while considering traffic and road data. Such systems exist nowadays in almost every aspect of life.

Although Predictive AI systems have been present for years and are now an integral part of our daily lives, their use is not devoid of risks. These systems raise significant issues of transparency, fairness and ethics, which have only recently begun to be duly discussed.

These systems are supposed to operate in a transparent, understandable and explainable way, and their output should be justifiable. The main risk is due to the fact that, in many cases, these systems operate as a "black box" that no one can explain. Even the creators of some Predictive AI systems or those who operate them do not always understand how and based on what data these systems reach one result or

another. This may be a major issue especially (but not only) when considering systems used in sensitive situations, such as by government and law enforcement agencies.

The Israeli Police learned this fact "the hard way" after, in a recent allowed-to-publish court ruling, the Israeli District Court criticized the use of a particular predictive AI tool by the Police, which no one seemed to be able to explain how it operates and why it reached certain results.

The system in question is a "profiling" system operated by the Israeli Police at Ben-Gurion International Airport. This system uses information from various sources and databases and generates a list of people who supposedly have a high likelihood of being drug couriers. Based on the system's output, the Police detained incoming passengers whose names were included in the list, and body searches were conducted to reveal whether these passengers were smuggling drugs. During trial, it was revealed that no one in the Police could explain precisely how the system reaches its conclusions, how it determines who will be included in the list, and what weight its algorithm gives to each data point. This ambiguity raised concerns about arbitrariness that may render such searches unlawful and contrary to the detainees' rights to privacy and equality.

The judge criticized the system and the Police's use of the system in several points, including the following:

- It is unclear what relative weight the algorithm gives to each datum – the Police was able to indicate which data was used but not how the algorithm reached the results and the relative weight given to each datum – as the system operates as a "black box."
- The algorithm "teaches itself" independently and without transparency – it may independently determine and change the weight each datum receives with no human intervention or influence possible.
- No one at the Police could explain with certainty and in-depth how the system operates.
- The system takes into account data whose connection to the prediction of drug crimes is unclear ("irrelevance"), and no one could explain why such data were fed into the system.
- There are no clear guidelines regarding the inclusion or exclusion of data used by the system.
- No updates were made to the system since it was first used, and it is unclear whether it was validated at any point – the use of the system began several years ago as a pilot that was never declared terminated and with no conclusions reached nor improvements made.

The main criticism by the judge can be grouped into two categories: **explainability** (no one knows how the system works or reaches its outputs) and **justifiability** (due to the lack of ability to explain how the system works, its conclusions cannot be validated nor justified).

While in this case the criticism was on a government agency, which by nature is subject to more stringent

rules of reasonableness, transparency and ethics, the principles it raises may also have an impact on the private sector and therefore deserves attention. This is especially true regarding systems in the business sector the operation of which may affect people's rights – for example, who is entitled to a loan or credit and who is not, or who should be offered certain products. These systems pose clear risks to companies that operate them and rely on them.

So, what are the main takeaways from this case? **Here are the points every company whose Predictive AI systems are used in Israel or that use Predictive AI systems in Israel need to know:**

1. Only introduce or use Predictive AI systems with respect to which we can explain how results are reached and justify such results.☒
2. ☒Ensure that you have put clear procedures in place regarding the addition or removal of data ☒from the system and ensure that it does not take into account irrelevant data. ☒
3. Knowing which data went into the system is not enough – it is crucial to be able to explain the specific weight ☒given to each datum and how it affected the final output.☒
4. Keep a human in the loop to regularly audit and validate the system's operation and output.☒
5. Ensure that the system is regularly updated and keep all validation data, update logs and technical documentation.☒
6. If a Predictive AI system is operated as a pilot, clearly define precisely when the pilot ends and what happens afterwards (to ☒prevent continued use without clear conclusions and correction of any non-compliance).☒

We regularly assist our clients in dealing with legal risks associated with the implementation and use of new artificial ☒intelligence systems in Israel. Please contact us with any legal need with respect to AI systems in Israel – we will gladly assist. ☒

Special thanks to Ms. Hila Davidi for assisting in the writing of this paper.

CA (Central District) 24474-01-22 **Berger v. State of Israel** (11.09.22, Judge Drori-Gamliel).

Key Contacts



Dr. Ziv Rotenberg
Partner



Netta Shaked-Stadler
Partner