Митя Йермол
Магистр, Жозеф Стефан институти билимларни узатиш маркази раҳбари (Словения)

ДАВЛАТ БОШҚАРУВИДА СУНЪИЙ ИНТЕЛЛЕКТДАН ФОЙДАЛАНИШ: СЛОВЕНИЯ ТАЖРИБАСИ

Митя Йермол
Магистр наук, руководитель Центра передачи знаний Института Йожефа Штефана (Словения)

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: ОПЫТ СЛОВЕНИИ

Mitja Jermol
M. Sc. head of the Centre for Knowledge Transfer at Jožef Stefan Research Institute (Slovenia)

USE OF ARTIFICIAL INTELLIGENCE IN PUBLIC ADMINISTRATION: THE EXPERIENCE OF SLOVENI

Slovenia is doing a lot of work on making public data publicly available. The Ministry of Public Administration has a project that covers all public databases – Open data governmental portals. There is another portal, called ERAR, that has been originally started by Goran Klemencic, while presiding the Commission for Prevention of Corruption of Slovenia. In this database you have all information about all state expenditures: sources of funds, expenditures, and purpose of used funds.

Institute Jožef Stefan (IJS) have worked with Ministry of Public Administration, Ministry of Education, Science and Sport, Ministry of Justice, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Interior, Anticorruption Agency, Prosecutor's Office, Bank of Slovenia, Municipalities, European Commission and NATO.

The first thing that IJS has done with the Slovenian Commission for Prevention of Corruption was a system that represents all public procurement, calls and results in maps and graphs which show where money has been concentrated –source, context, money flow. In the map you can see potential new scenarios that might be leading to different source of public procurement.

In another map of this website you can see the graph of NATO researches that is publicly available. Since we have historical data, we can also see trends and thus, do predictions.

Another project we did at IJS is the Bad Investment Bank project called DUTB, where you can see the main entities leasing bad investments. You can see there which companies were responsible for bankruptcies that happened in early 2010. You can combine this information with lobbyist contacts and get full picture. The fact is: more data you can combine, more accurate the results and clearer picture you will get.

We did the analytics of public procurement and clearly saw that different IT companies got money from the ministries at different times – from the left government and the right government. When we combined this data with publicly available information, it became clear that the owner of IT companies in question was the same person just using the different entities.

IJS also used publicly available data to monitor legislative process of adopting law through parliament: the process from discussion to law adoption. We constructed a timeline with available data and saw how voting in each particular step happened – not just across parties, but also across regions. This is crucial information which allows you to see where the problems are and how they relate to particular law. We transcript all debates in parliament, we can track changes and shifts in rhetoric. We can see how these MPs, even from different parties, are similarly voting. We can check their voting, their interest and combine this data with lobbyist data to see the whole picture.

In the public portal service, we don't do the interpretation. The interpretation has to be done by public – not by us.

Science analytics is a very useful tool. IJS collects data on research, projects, publications and constructs automatically social networks: who is collaborating with whom; competency networks: what are competencies of particular individual. We can also see trends and help policy makers decide or see in what areas of research to invest.

We did a landscape for European Commission – we structured a map of 8000 studies. This was a helpful tool for the European Commission to see where the empty spaces are, where investment is needed.

We also developed email analytics for enforcement agencies. In the beginning this tool was for our own use but at some point, it became interesting for law enforcement agencies, because the prosecutors and investigators have too much email data on a particular company. This tool collects all information, creates social networks, dependencies, story lines to track where a particular case has started, which people were excluded from communication, what has been discussed – everything that is needed for the case. Instead of reading billions of emails you can go through this system and find out roots, where things started to happen.

IJS did another project on automatic anonymization. This software was used to anonymize the documents that must be anonymized.

A risk assessment tool was done for the Bank of Slovenia to assist in assessing risks not only in the country, but also related to external entities. The same tool we use to see and detect potential threats: predicting defaults of

companies, sectors and problems in value chains. Based on the model that learns from these transactions between the companies, we can predict with 80% accuracy that a company in Slovenia will default. This is crucial information for the companies in same value chain.

Another project that we did is energy trading support for municipalities. The regulation of the energy market in Europe is open: anyone can trade with energy. In most cases, all municipalities in Slovenia and Europe as well, the mayors are dependent on entities they are running and mayors are not usually the experts in the field of energy. Thus, mayors/municipalities requested us to help them to understand what is going on inside their municipalities in the sphere of energy supply. We created the system that is able to allow better predictions for demand, prices and failures in infrastructure.

IJS is deeply involved in cybersecurity analytics projects. Right now, we are running a European funded project: we are reading all available sources – news, social media and dark web. Based on collected information we detect and formalize potential new scenarios for cyber threats. Thus, we do preventive measures before the problem occurs. A lot of European entities are involved in the project and Uzbekistan will be very much welcomed to join next calls for cybersecurity.

Transparency in this field is “name of the game”. As an institute, as researchers and developers we don’t interpret. We just provide different insights into data, so that others – journalists, analysts, law enforcement bodies can do the interpretation.

Data is public, but hardly publicly available. Even in Slovenia, where we have all laws set up, we spent 6 months of negotiations with the parliament to get information about the MPs – event if this data must be publicly available.

Every application is useful in a variety of scenarios. One application can’t be used in all circumstances, and you need to be prepared, that it should be adapted for each particular user or public administration.