# Disinformation narratives storytelling (banking)

## Task definition

In this technical test, you must play the role of a disinformation analyst. Starting from a dataset containing information from social network X, you should try to tell a story to a fictitious client interested in the disinformation that has circulated over a month about the banking sector.

An artificial intelligence system has previously analyzed all the data, generating transformations and metrics that include:

* Toxicity classification: a message is classified as “toxic” if it includes some potential attack on people, organizations or other entities. Toxic messages could include dangerous disinformation.
* Claim matching: if some part of a message “matches” a published fact-check, the message has a high probability of being false. The claim matching AI could find more than one match for a particular message.
* Topic modelling: messages discussing similar topics are grouped together in “common narratives”

The objective is to analyze the data, detect insights and construct a data story about disinformation (or targeted attacks) through the identification of suspicious narratives of attacks on banking. You must consider as suspicious (both at the content level and at the narrative / group of contents level)

* The one that presents a high level of toxicity
* The one that presents a specific attack on a bank company, institution and/or product
* The one that supports or is related to some verification content (claim\_review, factcheck article)
* The one that, regardless of the rest of the criteria, can be considered suspicious and/or malicious under the criterion of the storyteller

To achieve this objective, the following specific **(technical) tasks** must be addressed at different levels:

1. Loading the data into a database or other management system that allows them to be exploited analytically (OLAP)
2. Analyze the content
3. Create some visual representation using the BI tool of your choice to support a storytelling about the data (potential ideas: funnel of data processed, main features of the suspicious narratives, most affected brands, users involved, etc.)

### Other requirements

In addition to the stories, specific panels should be set up to comparatively visualize the volumetry in the general context, in the banking context, and in the context of suspected attackers. With filters or temporary aggregations according to the candidate's criteria.

## The Data

There are five zipped files with:

1. about 200K of X messages including: raw text/content; user (name), publication date; (if any) explicit relation with other content; and other author data such followers and friends
2. toxicity and targeted attacks (to a specific object) into the content (linked through the *content\_id column*), according the reasoning of a model powered by generative AI. Each row in the dataset includes: when the content contains toxic language (*toxic / no toxic*); and, when the content contains a targeted attack, the type of the attack (*attack column*) and the target (*object\_attack column*).
3. factcheck - x content relations extracted from a claim matching process based on semantic similarity and natural language inference. It includes a content identifier, a factcheck url and a sentence (extracted from the content) matched with the factcheck. Since different models have been used to find the relationships, there may be repeated content-sentence-factcheck relationships.
4. Content clustering based on semantic similarity (about ~850 topics). This dataset only includes membership relationships of a content to a topic (cluster\_id).
5. Cluster/Topic metadata, including keywords and a title / description according to the reasoning of a model powered by generative AI.

### Other considerations

* Data annotations and/or transformations use the message *“link”* as unique identifier for the content. These tables store it as *“content\_id”*.
* Data are (temporally) contextualized in the last October
* There are no annotations/transformations on all content. For example, there may be content for which there is no record of toxicity; or there may be content not included in any topic.

## Delivery

* Please check the problem description and the dataset. If something doesn't add up, don't hesitate to contact us. In general, if you encounter any unexpected problem or if you have doubts about a specific part, contact us before the deadline to see if we can find the solution or clear any doubts.
* Both generated code and screenshots (dashboards, panels, etc.) or any other kind of resource must be shared from a git repository accessible by our team (GitHub, GitLab, etc.). Please consider including a README (markdown) with the most important details (e.g. decisions, links to resources, etc.) Also, if any, deployment instructions or credentials. If necessary, before uploading the test datasets to a service other than GitHub/GitLab, get in touch to discuss the need and agree, in common, on the best site.
* Apart from the fact that you may consider recording a video presentation of the results (as part of telling the story), due to the type of technical test we consider it necessary to have such a live presentation / demo live in a video conference for this purpose.