ERICSSON

Ericsson – BEREC AI Report consultation response

Contact:
Daniel Gueorguiev
Director Policy Advocacy Europe
daniel.gueorguiev@ericsson.com

1 Introduction

Ericsson welcomes the BEREC report on Artificial Intelligence. The report tries quite well to cover a very complex topic, the challenges, opportunities and use cases. At Ericsson we are dedicated to bring the latest and best technology to the telecommunication market, as such we have developed industry leading AI tools that we offer, in Europe and around the world.

In this reply, we would like to share some initial thoughts on a few specific sections as well as some general observations regarding some of the use cases. Of course, we are ready to share more details and provide evidence of the technology with an educational purpose. We invite BEREC to also visit our Ericsson AI page where a lot of resources are made public.

1.1 Risks – 'Vendor lock-in'

Ericsson provides network management AI, much like our competitors, and customers are able to decide which provider they would like to use, based on the product and service that they find are best. That is the nature of healthy competitive forces that drive market players to develop different products with the objective of attracting customers. In that sense, we have not yet seen proof of vendor lock-in as such.

The Ericsson AI systems used for managing the networks are vendor agnostic and work independent of the vendor used. The AI systems offered work as finetuning pieces on top of the network. Furthermore, in the radio-units where AI is embedded, we would like to emphasize that the AI applications (rApps) are meant to work as an open platform for external parties. They can be used in any network - the network of our competitors or our own.

Additionally, there is network equipment that Ericsson produces where the AI is embedded into the final product and is a feature it has. Here again, the driving force is to be able to more adequately compete on the market by offering network equipment that has more and or better features than our competitors. Our customers have a choice and can chose Ericsson or other network equipment manufacturer based on their needs, performance of the equipment, their strategy and costs to name a few. Much like any other customer service provider, they can swap equipment and chose at any point to go with another – the nature of competitive market forces.

1.1.1 Model ownership and training

In the AI telecommunication market, and whenever those services and products are discussed, ownership of the model and all other relevant

elements (how the data is used for example) relating to the product are negotiated through commercial agreements based on market economics. Currently Ericsson does not see any market failures or risk thus far or potentially in the future. Hence, issues around ownership are more appropriately dealt with in the realm of business agreements and contracting, thus making it less in scope of any regulatory initiatives.

BEREC also raises the concern that an AI can be trained by data in the network of one operator and carry those efficiencies to the next network where it is applied, posing some privacy concerns. At Ericsson we train our AI products on information from the particular network in question and "tune" the model before each new application in a novel network. This is done in collaboration with our customers because every network operator that we work with has different KPIs, requirements and level of AI integration that we meet. As such no two networks are alike and require this AI "tuning" from our part to deliver efficient, effective and relevant results for each specific case. The amount of sensitive data carried over from one network to another when using the same trained model therefore seems limited.

1.1.2 Lack of trust and Validation of data

The report does not elaborate on how to validate the data handled by the model. Ericsson would like to point to the existing ways of actually validating the data.

1.2 Security and malicious attacks

First of all, we should remember that all systems can fail, regardless if AI is used or not. The impact of system failure is handled for all critical parts using failover mechanism, graceful restart, geo-redundancy and other mechanisms. This is not a question of AI, but of design and test of robustness and resilience of all networks.

If we look at AI under the hood, we will see that it is another piece of software. What differentiates it from traditional programming is the fact that it is driven by data. It is important that correct safety mechanisms are introduced when using this software in critical environments (like live networks), as in the case of any other type of software used for the same task.

There are network safety fallback mechanisms that the machine-learning system will use in case of undesired behavior. These mechanisms are usually put in place when dealing with a 'critical' system. This practically means that whenever the AI algorithm is unsure of the action it deploys, it uses some hard-coded rules on how to behave.

These safety fallback mechanisms will - within a foreseeable future - remain hard-coded and deterministic (linked to a pre-defined behavior), thus not likely to consist of an AI system itself.

Another example, which is pointed out in the report, is using simulated and emulated environments to test potentially unsafe actions of the system before any AI is used in the network. This way we are able to test a potentially unsafe action in a digital representation of the network, rather than the actual network and according to the results deploy it, or not, to the live network.

Human oversight is another mechanism that reduces uncertainties with AI systems. In short, the AI system escalates critical decision points to humans to make sure no risk behavior is allowed. Negligible decision points are allowed to be automated.

1.3 Other challenges

In terms of the currently negotiated AI Act, Ericsson echoes what many other respondents have already explained. Digital infrastructure is indeed essential for the functioning of a modern society. That does not, however, mean that all AI systems used in networks are "high-risk" (for safety and fundamental rights). Simplified, the 5G infrastructure could be described as a "bit-pipe". The infrastructure cannot on its own pose a risk to fundamental rights or safety. Any potential risks to safety or fundamental rights would derive from the applications. And these applications are already classified as 'high-risk' in the proposed Regulation. AI is just another technology in this context.