Finnish Competition
and Consumer Authority

KKV/727/03.05/2020

12.6.2020

Consultation on the White Paper on Artificial Intelligence - A European Approach

Opinion from the Finnish Consumer Ombudsman

Human-centric approach and maintaining a high level of consumer protection and trust are important goals. Progress should be made towards a consumer-friendly digital environment. There is a need for clear and general ground rules, since artificial intelligence and algorithm-based processes are advancing quickly for example in e-commerce, digital advertising and customer (self-)service. Consumers are always the weaker party and do not have the market power to negotiate fair risk allocation. For example a consumer cannot negotiate the contract terms but can only accept or reject the standard form contract.

The consumer always needs to have one party, whom he can turn to and who is responsible. Consumer rights cannot be enforced effectively unless someone takes responsibility for the AI system design (including algorithms and interfaces). This is too important a principle to be left to self-regulation or freedom of contract, but needs to be grounded in the law. Also the private enforcement questions need to be solved.

In most cases the product offered to the consumer is not “AI” but goods or services which make use of AI. Absolute minimum requirement is transparency: who is the responsible party and making clear the roles of different actors. Already consumers find it difficult to comprehend that there are several actors and different processes involved when they use digital commodities or are involved in digital processes. Moreover, consumers face real problems when they seek redress. Actors keep avoiding responsibility and instead juggle with different liability limitations.

In the field of AI, IoT, robotics and algorithms it is extremely difficult for the consumers to prove their case. They cannot collect evidence since they cannot break down the digital codes or enter the level of digital infrastructure. For these reasons also strict liability could be considered. A minimum requirement should be reverse burden of proof, which already exists in EU-legislation like the Regulation (EU) No 910/2014 on electronic identification and trust services (article 13) and the Digital Content and Digital Services Directive (EU) 2019/770 (article 12).

The best way to promote consumer rights and trust is to create general principle based and technology neutral legislation. Legislation, which is general in nature, also treats all businesses alike. Setting categories might not be the best legislative technique. Categories always have limits and the definitions outdate fast. Many of the requirements described in the White

Paper could be understood as general quality requirements for any AI affecting humans

Besides general safeguards, in the areas of high risk AI applications there might be need for ex ante -processes such as standardization, audit and/or certification. However, it is not an easy task to define high risk AI applications or usage. It stems from the essence of the AI and the interconnected digital environment that interoperability may be spontaneous or even accidental. Any malfunction or unintended communication may create chain reactions and system shutdowns that endanger essential facilities of the society. The damages to private and public parties may be irrecoverable, vast and severe. There are already examples where it was the everyday “smart objects” like household appliances which created real risks.

Also the tools and working methods of the supervisory and/or enforcement authorities need to be considered in a new way. Digital activities are fast moving and global by nature and this creates problems in sanctions and powers. In consumer protection there is also a need for digital measures and tools for preventing the harm. Enforcement and supervisory authorities are challenged with the problems of collecting digital evidence. In the digital environment it is more and more about algorithms finding algorithms and robots fighting robots.

It is not always easy to identify the origin of the AI or algorithm. One important point to be considered is whether the identity of the party responsible for the AI or algorithm should be stated openly within the software and in a digital format. For example the algorithm could contain a water stamp, ID-code, certificate number, etc. which could be made accessible for both individuals and authorities. This would make it easier to detect “homeless” and suspicious algorithms and could create new possibilities for malware takedowns and crime prevention as well.

Katri Väänänen Consumer Ombudsman	Riikka Rosendahl Team Manager

ALLEKIRJOITETTU KONEELLISESTI
ASIANHALLINTAJÄRJESTELMÄSSÄ