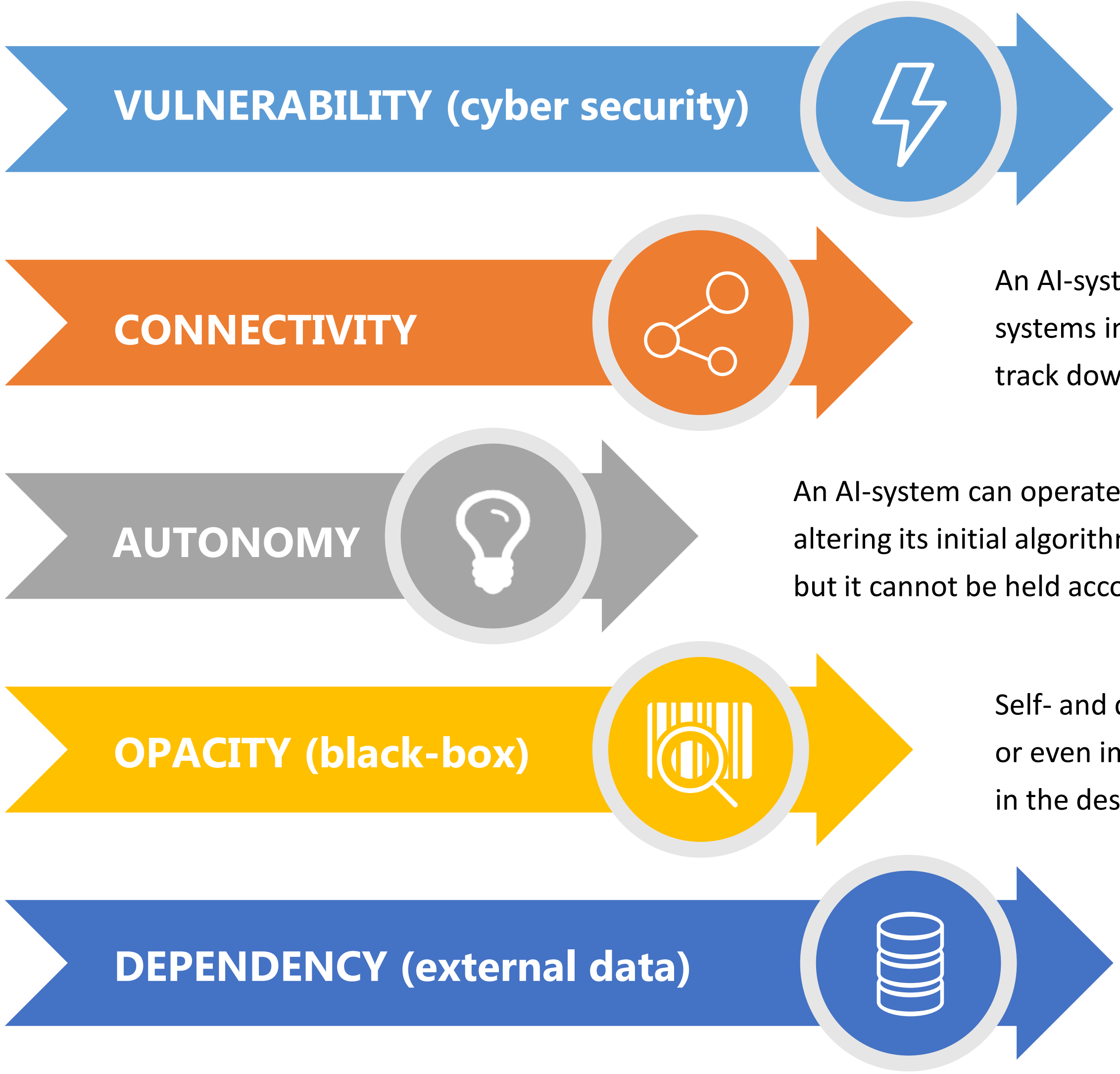
epp group in the european parliament

Axel Voss

LEGAL GAP: Liability & AI-systems

Five reasons why a victim could end up without compensation



VULNERABILITY (cyber security)

Frequent updates and constant external interactions allow hackers (that are often untraceable or impecunious) to modify the AI-system or to cause malfunctions that lead to harm.

CONNECTIVITY

An AI-system is connected with many other AI- and non-AI-systems in complex digital ecosystem, making it very difficult to track down the system that causes the harm.

AUTONOMY

An AI-system can operate without control or supervision by independently altering its initial algorithm or by deviating from the original instructions but it cannot be held accountable for its actions.

OPACITY (black-box)

Self- and deep-learning processes of the AI-system make it difficult or even impossible to trace back specific human input or decisions in the design that triggered the harmful activity.

DEPENDENCY (external data)

External information without which the AI-system cannot operate could be flawed or missing, wrongly perceived by built-in sensors or falsely communicated by regular data sources or ad-hoc suppliers.

Potential Liability Claims

of a victim for harm caused by an AI-system

Contractual Partner

Contract Law

Situation: The victim suffered harm caused by an AI-system, while the AI-system was component of a contract.

Procedure: The contractual partner is liable if he/she is at fault or if the contract has a strict liability clause.

Producer

Product Liability Directive

Situation: The victim suffered harm, which was caused by a defective AI-system.

Procedure: The producer is liable if he/she is not able to exonerate and if the victim can prove the damage, the defect and the causal relationship between both.

Interfering Party

National Tort Law

Situation: The victim suffered harm, which was caused by an interference that affected the operation of the AI-system.

Procedure: The interfering party (e.g. hacker) is subject to fault-based liability, if the interference caused the harm and he/she is at fault for the illicit act.

Deployer

New Regulation

Situation: The victim suffered harm, which was caused by a deployed AI-system.

Procedure: The deployer is subject to strict liability of the AI-system if it is classified as 'high-risk'. In all other cases, the deployer is liable if he/she is at fault and not able to exonerate himself/herself.

Axel Voss

Liability of the Deployer

based on a risk based approach

Strict Liability

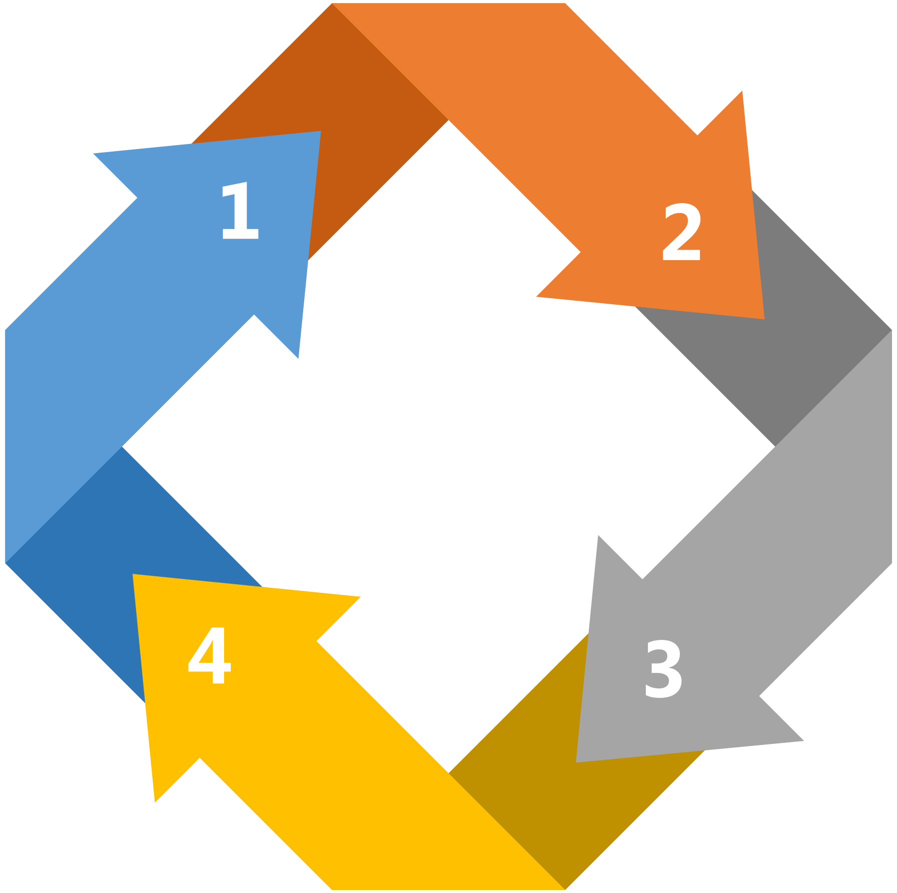
- The deployer is liable for harm/damage caused by the high-risk AI-system regardless of his/her fault.
- Has to compensate harm/damage up to a max. total amount of 10 Mio. (death/health) or 2 Mio. (property).
- Liability claims are subject to special limitation period of 10/30 years depending on the legally protected right.
- No possibility to exonerate. The deployer is not liable only in cases of force majeure.
- A liability insurance cover is mandatory for each high-risk AI-system.

Fault Liability

- The deployer is liable for harm/damage caused by the AI-system if he/she is at fault for the harmful act.
- The victim of harm caused by an AI-system benefits form a presumption of fault of the deployer.
- Exoneration possible by proving that due diligence was observed or activation took place without knowledge.
- Deployer is liable for harm/damage caused by a hacker if this person is untraceable or impecunious.
- National laws on the amounts/extent of compensation and the limitation periods continue to apply.

Classification of a new high-risk AI-system

legislative procedure



Notification

Civil society, consumer organizations, academia, businesses or Member States notify Commission that an AI-system might qualify as 'high risk'

Review

Commission + standing TCRAI-committee assess legally/technically if AI-system matches the high-risk criteria set out by the Regulation

Objection

Parliament and Council (which experts can also attend Review meetings) have two months to object the Commission’s decision

Transitional Period

Delegated Act of the Commission classifies the AI-system as 'high risk‘ and becomes effective six months after the adoption