

The AI Act, Cybersecurity and the State of the Art

Sandra Schmitz

This research was funded by the Luxembourg National Research Fund (FNR)
C18/IS/12639666/EnCaViBS/Cole, <https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/>.

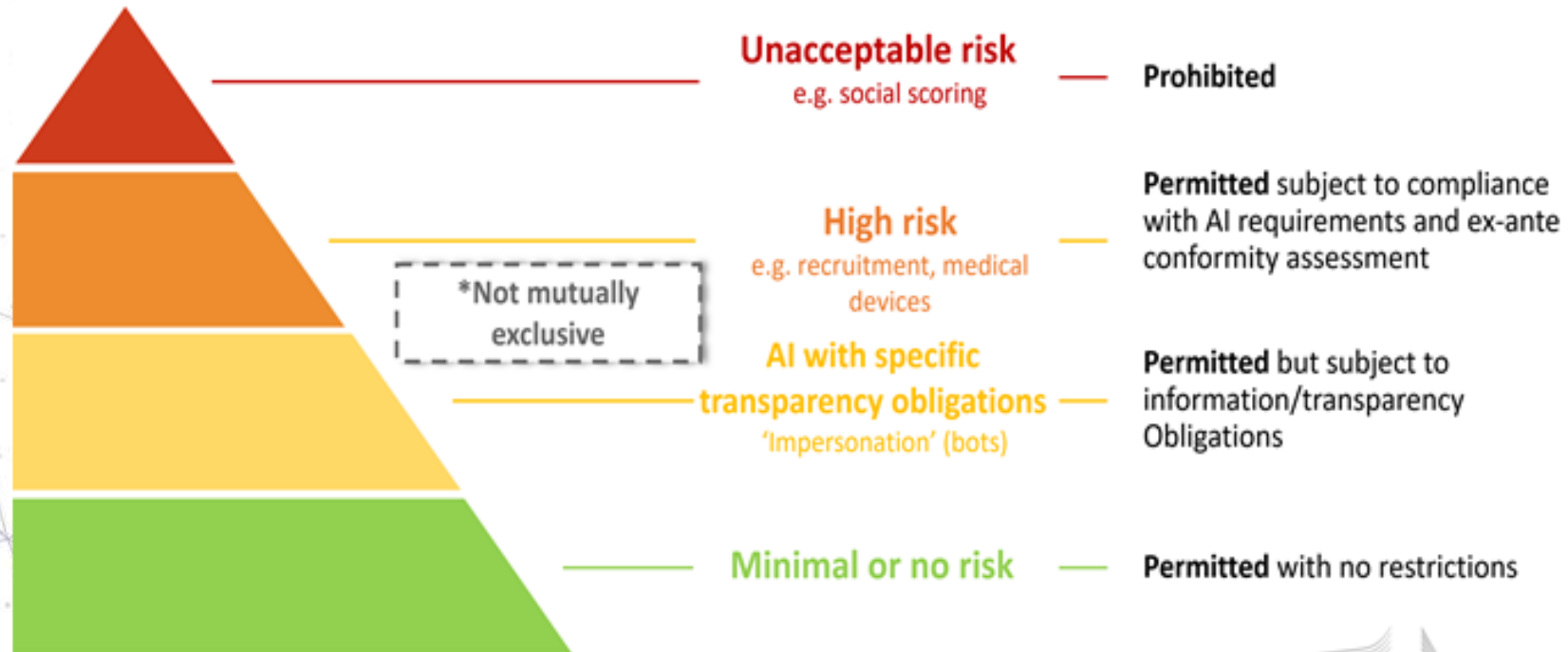
Agenda

**Risk-based Approach
to Technology
Regulation**

**(Cyber-)security
Regulation and the
State of the Art**

A risk-based approach to technology regulation: AI Act Proposal


A risk-based approach to regulation



Title III: „High-risk“ AI Systems - Examples

High Risk AI = AI applications that constitute a high risk for the health and safety or fundamental rights of citizens

AI systems identified as high-risk include AI technology used in:

- **Critical infrastructures** (e.g. transport), that could put the life and health of citizens at risk;
 - **Educational or vocational training**, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
 - **Safety components of products** (e.g. AI application in robot-assisted surgery);
 - **Employment, workers management and access to self-employment** (e.g. CV-sorting software for recruitment procedures);
 - **Essential private and public services** (e.g. credit scoring denying citizens opportunity to obtain a loan);
 - **Law enforcement that may interfere with people's fundamental rights** (e.g. evaluation of the reliability of evidence);
 - **Migration, asylum and border control management** (e.g. verification of authenticity of travel documents);
 - **Administration of justice and democratic processes** (e.g. applying the law to a concrete set of facts).
- 
- **Regulatory "Burdens":** Adequate risk assessment and mitigation systems; Ex-ante conformity assessment

Regulation of NIS under NIS Directive*: Risk-based approach to Cybersecurity

1st step:

Identification of operators of “essential” services

2nd step:

implementation of security measures appropriate to the identified risks

Article 14

Security requirements and incident notification

1. MS shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

* Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

„State of the art“

Art. 9 AI Act Proposal

3. The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

Recital 49 AI Act Proposal

High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art.

The Common Understanding of State of the Art

Cambridge Dictionary:

- *The best and modern of its type*
- *Very modern and using the latest ideas and methods*

Collins Dictionary:

- *If you describe sth as state of the art, you mean that it is the best available because it has been made using the most modern techniques and technology*

Merriam-Webster Dictionary:

- *The level of development (as of a device, procedure, process, technique, or science) reached at any particular time usually as a result of modern methods*

Wikipedia:

- *State of the art (sometimes cutting edge or leading edge) refers to the highest level of general development, as of a device, technique, or scientific field achieved at a particular time. However, in some contexts it can also refer to a level of development reached at any particular time as a result of the common methodologies employed at the time.*

SotA from a Legal Perspective – Three Step Theory

State of science and technology

- Very high level of protection
- requires to take into account the latest scientific knowledge regardless of whether it is technically and economically feasible and available

Subjective element

SotA

Corresponds to at least to the best technique available to the operator in question

- *cost of implementation;*
- *nature, scope, context & purposes of processing; associated risks*

Generally accepted rules of technology

- Technology has stood the test of practice
- Technology is generally accepted amongst the majority of experts, but does not have to be the best technology available
- Rebuttable presumption that technical standards (eg DIN-Norms) amount to generally accepted rules

Take-Aways

- Basic approach to technology regulation: risk-based approach based on the pyramid of criticality with layered enforcement mechanisms
- Compliance is a moving target (dynamic process): state of the art technology depends on context, risk (likelihood and severity) and feasibility (proportionality principle)



Interdisciplinary Centre for Security, Reliability and Trust

Contact:

sandra.schmitz@uni.lu

Connect with us



@SnT_uni_lu



SnT, Interdisciplinary Centre for
Security, Reliability and Trust