

ARTIFICIAL INTELLIGENCE ACT

Proposed by EU Commission

A Tentative Summary (without proof-reading)

中央大学
国際情報学部
学部長・教授・博士 (総合政策)

平野 晋 (*)

(*) 米国弁護士 (NY州)

Presentation @ Cabinet Office of Japan
Council for Social Principle for Human-centric AI
May 12, 2021

What Is the New Proposal

Comparison with my presentation in the 1st meeting of this Council in FY 2020



於：OECD・AI専門家会合@パリ, Sept. 2018.

AI Regulation Proposed by EU Commission

Regulations from Not Only **Private Law** But Also **Public Law**

- My presentation in the 1st Meeting
 - Private Law
 - Torts (不法行為法: *huhō-kōi-hō*)
 - Compensating π 's Injuries
 - Deterrence toward future Δ (Law + Economics)
 - Today's presentation
 - Public Law
 - Administrative Law
 - Stronger interference with freedom / activities



前回発表資料から

42 第一部 不法行為法の概要

図表#2 各種の行為規制の関係

民事・不法行為法

過失責任

care levels

活動の自由: 大

無過失(厳格)責任

activity levels

公法・行政規制

活動の自由: 小

る立場である。(もっとも論者によっては自由に介入して保護主義的に規制を強化すべきという立場もあり得る。) 詳しくは、後掲 第二部、第II章「第四節『パターナリズム』と『自己責任』」内の「1.『選択の自由』と『リバタリアニズム』」対「パターナリズム」以降等を読んで欲しい。

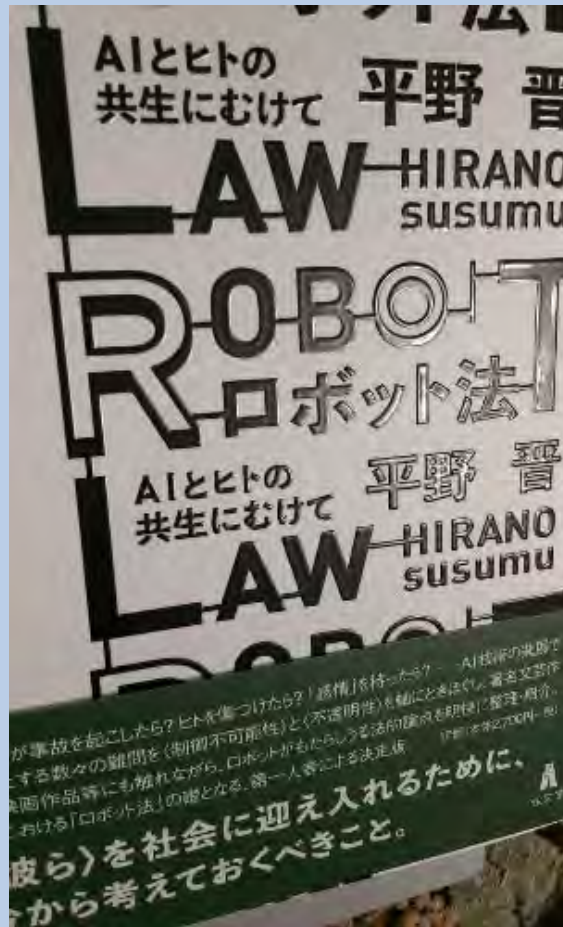
不法行為法に...に述べたように、賠償理由から望ましい...度については、本節...故賠償制度、ニュー...

平野『アメリカ不法行為法』前掲 at 41~42頁 (2006年)

決権という要素以外にも、社会にとって効用のある被告(△)の「非互酬の危険(nonreciprocal risks)な」活動については、禁止したり差止を命じるべきではなく、無過失賠償責任を課すことにより被害者の事故費用を△に転嫁して社会に有用な危険から罪のない被害者を保護すべきであると指摘されている。See, e.g., George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 568-69 (1972). そ



背景



2017年11月 弘文堂



増補版 2019年10月 弘文堂

AI Regulation Proposed by EU Commission

①負の面への対策と、②促進と...

- キーワードは、**health, safety, and fundamental rights**
- 更に、加盟国が区々に法規制することによる流通障害を回避

Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. **Differing national rules may lead to fragmentation of the internal market** and **decrease legal certainty for operators that develop or use AI systems**. A consistent and high level of protection throughout the Union should therefore be ensured, **while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented**, by **laying down uniform obligations for operators** and **guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons** throughout the internal market

Proposal for AI ACT, *infra*, at 17 (Whereas clause (2))(emphasis added).

AI's Dangerous Nature Found by EU

The most recent Conclusions from 21 October 2020 further **called for addressing the opacity**, complexity, **bias**, a certain degree of **unpredictability** and partially **autonomous behaviour** of certain AI systems, to ensure their compatibility with fundamental rights and to facilitate the enforcement of legal rules⁸.

⁸ Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 2020.

European Commission, Proposal for a Regulation of the European Parliament and of the Council: Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Apr. 21, 2021, https://www.plattform-lernende-systeme.de/files/Downloads/Allgemein/Proposal_Artificial_Intelligence_Act.pdf (Apr. 21, 2021)(emphasis added)[herein referred to as “Proposed AI ACT”].

AI's Dangerous Nature Found by EU

The use of AI with its specific characteristics (e.g. **opacity**, **complexity**, **dependency on data**, **autonomous behaviour**) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter').

Proposed AI ACT, *supra*, at 11 (emphasis added).



特徴



**AIGO's 2nd meeting at OECD
in Paris, Nov. 12, 2018**



AI Regulation Proposed by EU Commission

域外（日本）にも適用されるか？

-Yes.

Article 2 *Scope*

1. This Regulation applies to:

- (a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
- (b) users of AI systems located within the Union;
- (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union

Id. at 38 (emphasis added).

代理人—representatives—等の責任

Article 25

Authorised representatives

1. Prior to making their systems available on the Union market, **where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union.**
2. **The authorised representative shall perform the tasks specified in the mandate received from the provider. The mandate shall empower the authorised representative to carry out the following tasks:**
 - (a) **keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities referred to in Article 63(7);**
 - (b) **provide a national competent authority, upon a reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law;**
 - (c) **cooperate with competent national authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.**

Id. at 55 (emphasis added).

尤も、適用[外]は...

Article 2 *Scope*

...

3. **This Regulation shall not apply to AI systems developed or used exclusively for military purposes.**
4. **This Regulation shall not apply to public authorities in a third country nor to international organisations** falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

Id. at 39 (emphasis added).



対象となる “AI systems”

Article 3 *Definitions*

For the purpose of this Regulation, the following definitions apply:

- (1) ‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

Id. at 39 (emphasis added)(AGIは除外か?).

(続き) 対象となる “AI systems”

ANNEX I

ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.


ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS at 1 <https://ec.europa.eu/newsroom/dae/items/709090> (last visited May 9, 2021) [hereinafter referred to as the “ANNEXES”].

(続き) 対象となる AI systems

Article 4

Amendments to Annex I

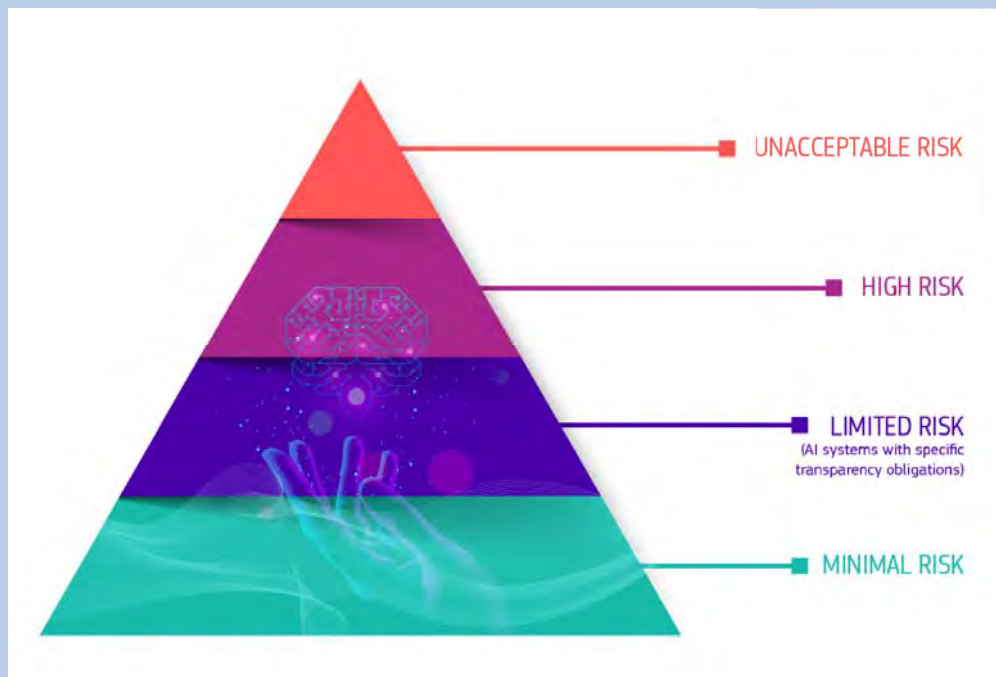
The Commission is empowered to adopt delegated acts in accordance with Article 73 **to amend the list of techniques and approaches listed in Annex I**, in order to **update that list to market and technological developments** on the basis of characteristics that are similar to the techniques and approaches listed therein.



Proposal for AI ACT, *supra*, at 2 (emphasis added).

概ね四層として紹介される  中央大学

Risk-Based Control



European Commission, Excellence and trust in artificial intelligence

<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence#building-trust-through-the-first-ever-legal-framework-on-ai> (last visited May 5, 2021).



AI Regulation Proposed by EU Commission

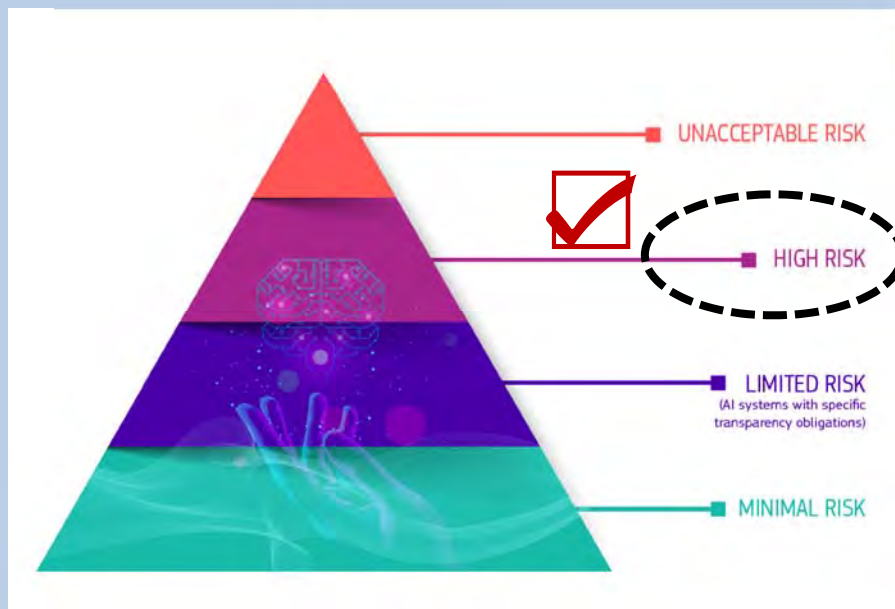
概ね四層として紹介される (続き)

Tiers	Categories	E.g.:	Authorities
Tier 1	Prohibited AI Practices / Un-acceptable risk	<p><i>E.g.:</i></p> <ul style="list-style-type: none"> ✓ subliminal techniques; ✓ an AI system that exploits vulnerabilities to distort materially distort their behaviors ; ✓ AI-based social scoring for general purposes done by public authorities; and ✓ 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement unless certain limited exceptions apply. 	See Title II: Art. 5
Tier 2	High-Risk AI Systems	<p><i>E.g.:</i></p> <ul style="list-style-type: none"> ✓ Safety component of products that are subject to third party ex-ante conformity assessment; or ✓ Stand-alone AI systems, with mainly fundamental rights implications, listed in ANNEX III. 	See Title III
Tier 3	Transparency Obligations for Certain AI Systems / Specific risks of manipulation	Transparency obligations will apply for systems that: <ul style="list-style-type: none"> (i) interact with humans; (ii) are used to detect emotions or determine association with (social) categories based on biometric data; or (iii) generate or manipulate content ('deep fakes'). 	See Title IV
Tier 4	Codes of Conduct	<p>"The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2. . . ." / "Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations."</p>	See Title IX, Art. 69

特に「high-risk AI systems」

は ...

箸の上げ下ろしも指図して
徹底的に管理



AI Regulation Proposed by EU Commission

High-Risk AI Systems

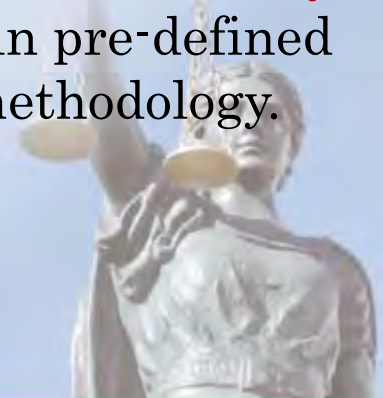


Chapter 1 of Title III sets the classification rules and identifies two main categories of high-risk AI systems:

- AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
- other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III.

This list of high-risk AI systems in **Annex III contains a limited number of AI systems whose risks have already materialised or are likely to materialise in the near future**. To ensure that the regulation can be adjusted to emerging uses and applications of AI, **the Commission may expand the list of high-risk AI systems** used within certain pre-defined areas, by applying a set of criteria and risk assessment methodology.

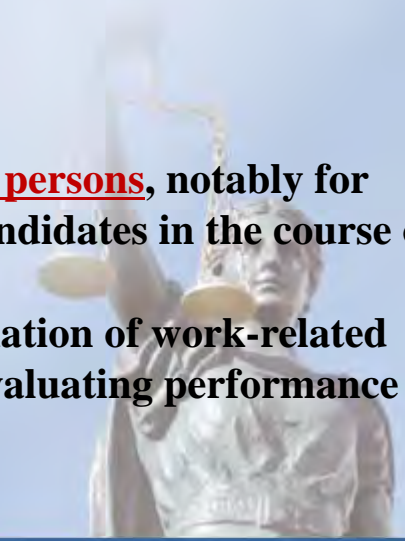
Id. at 13 (emphasis added).



ANNEX III: High-Risk AI Systems



1. **Biometric identification and categorisation of natural persons:**
 - (a) AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons;
2. Management and operation of **critical infrastructure:**
 - (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
3. **Education and vocational training:**
 - (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
 - (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.
4. Employment, workers management and access to self-employment:
 - (a) AI systems intended to be **used for recruitment or selection of natural persons**, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
 - (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.



ANNEXES, *supra*, at 4 (emphasis added).

ANNEX III: High-Risk AI Systems

5. Access to and enjoyment of essential private services and public services and benefits:

- (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
- (b) AI systems intended to be used **to evaluate the creditworthiness of natural persons or establish their credit score**, with the exception of AI systems put into service by small scale providers for their own use;
- (c) AI systems intended to be used to dispatch, or to establish **priority in the dispatching of emergency first response services, including by firefighters and medical aid.**

6. Law enforcement:

- (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
- (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
- (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

Id. at 4-5 (emphasis added).

ANNEX III: High-Risk AI Systems

- (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;**
- (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;**
- (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;**
- (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.**

Id. at 5.

ANNEX III: High-Risk AI Systems



7. Migration, asylum and border control management:

- (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
- (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
- (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
- (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

- (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

Id. at 5 (emphasis added).



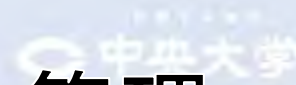
High-Risk AI Systems: 箸の上げ下ろしも指図して徹底的に管理

high-risk AI sysが利用される前に満たすべき要件 E.g. . . .

risk management system	data governance	technical documentation	record keeping
transparency and information to users	human oversight	accuracy, robustness, and cybersecurity	\

See Proposed AI ACT, *supra*, at 46 (Art. 9).

High-Risk AI Systems : (続き)



箸の上げ下ろしも指図して徹底的に管理

high-risk AI sysが満たすべき要件 E.g. . . .

risk management system	Continuous interactive process throughout the entire of life; regular updating; adoption of suitable risk management measures; residual risks to be communicated to users; to be tested to identify most appropriate measures, etc.	Ch. 2, Art. 9
data governance	Meeting quality requirements (re., e.g., annotation, labeling, quality and suitability of the data sets, possible bias , possible data gaps or shortcomings) at the developments based on training, validation, and testing (e.g., data sets must be representative , free of errors, and complete), etc.	Art. 10
technical documentation	Must be drawn up by xxx ___ to demonstrate compliance; must contain items set forth in ANNEX IV; the Commission may amend the ANNEX IV, etc.	Art. 11
Record keeping	Enabling automatic recording events (logs) conformig to stds and common specs, and traceable throughout its lifecycle; biometrics must meet heavier requirements, etc.	Art. 12

cont'd on next page

See Proposed AI ACT, *supra*, at 46-50 (emphasis added).

High-Risk AI Systems : (続き)

箸の上げ下ろしも指図して徹底的に管理

high-risk AI sysが満たすべき要件 E.g. . . .

transparency and information to users

- To enable uses to interpret sys' output appropriately, must ensure transparency; must be accompanied by "instruction for use" which must be concise, complete, correct, and clear.
- The instruction must include: characteristics, capabilities, and **limitation of performance**, **level of accuracy**, robustness, and cybersecurity; known/foreseeable circumstances leading to risks to health, safety, and fundamental rights; when appropriate, input data,; **human oversight measures**; expected lifetime and necessary measures incl. software update; etc.

Ch. 2, Art. 13

cont'd on next page

See Proposed AI ACT, *supra*, at 50 (emphasis added).

High-Risk AI Systems : (続き)

箸の上げ下ろしも指図して徹底的に管理

high-risk AI sysが満たすべき要件 E.g. . . .

human oversight

- Must be designed so that they can be effectively overseen by natural persons; must aim to minimize risks to health, safety, or fundamental rights.
- As appropriate to the circumstances, the natural person must be able to:
 - fully understand the limitations of the sys so that anomalies, dysfunctions, and unexpected performance can be detected;
 - remain aware of possible tendency of automatical reliance/over-reliance on the output (“automation bias”)
 - interpret correctly the output;
 - be able to decide, disregard, override, or reverse the output; [and/or]
 - be able to intervene on the operation of the sys through a “stop” button.
- As to biometrics, at least two (2) natural persons must verify and confirm an identification produced by biometrics before an action is to be taken based on the identification.

Art. 14

cont'd on next page

See Proposed AI ACT, *supra*, at 51-52 (emphasis added).

High-Risk AI Systems : (続き)

箸の上げ下ろしも指図して徹底的に管理

high-risk AI sysが満たすべき要件 E.g. . . .

accuracy,
robustness,
and
cybersecurity

Must be designed to achieve an appropriate level of accuracy robustness and cybersecurity throughout their lifecycle; the **accuracy must be declared in the instruction**; must resilient in errors or faults; in the systems that continue to learn after being placed on the market must be ensure that possibly biased outputs due to outputs used as an input for future operations (“feedback loops”) are duly addressed with appropriate mitigation measures; must include measures to prevent attacks trying to manipulate training data (“data poisoning”) or inputs to cause the model make a mistake (“**adversarial examples**”), etc.

Art. 15

END OF THE TABLE

See Proposed AI ACT, *supra*, at 51-52 (emphasis added).



High-Risk AI Systems : (続き)

“providers”の義務

high-risk AI sysの <u>プロバイダ</u> (*)の義務 E.g. . . .				
quality management system	technical documentation	keeping logs	conformity assessment	registration obligation
corrective actions	information to national competent authorities, notified bodies, et al.	affixing CE marking	demonstrating conformity upon request from nat'l competent authorities	

See Proposal for AI ACT, *supra*, at 52 (Art. 16 (a)-(j)).

(*) The term, “‘provider’ means a natural or legal person, public authority, agency **or other body that develops an AI system or that has an AI system developed** with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge”. *Id.* Art. 3(1).

High-Risk AI Systems : (続き)

providersの義務

high-risk AI syssのプロバイダの義務 E.g. . . .

quality management system	<ul style="list-style-type: none">- Provider shall put into place a quality management sys documented and which must include: examination, test, and validation procedures; technical specs and stds to be applied; sys and procedure for data management; risk management sys; post-mkting monitoring sys; procedures to report serious incidents and malfunctioning; sys and procedure for record keeping; resorce management; accountability framework incl responsibilities of the management and othe staff, etc.- Credit institution is deemed to meet this req by complying with another applicable Directive.	Ch. 2, Art. 17
technical documentation	<ul style="list-style-type: none">- Provider shall draw up the technical documentation in accordance with ANNEX IV.- Credit institute does so in accordance with another applicable Directive.	Art. 18

cont'd on next page

See Proposed AI ACT, *supra*, at 53-54 (emphasis added).

High-Risk AI Systems : (続き)

providersの義務

igh-risk AI sysのプロバイダの義務 E.g. . . .

keeping logs	<ul style="list-style-type: none">- Providers shall keep the logs to the extent such logis are under their control by virtue of a contract arrangementwith the user or by law.- Providers of credit institutes do so under another Directive applied to them.	Ch. 2, Art. 20
conformity assessment	<ul style="list-style-type: none">- Providers shall make their sys <u>undergo conformity assessment procedure before their placing on the market.</u>- Providers shall draw up an <u>EU declaration of conformity</u> and affix <u>the CE marking of conformity.</u>	Arts. 19, 43, 48, 49
registration	<ul style="list-style-type: none">- Before placing on the market the sys, the provider (or, where applicable, the authorised representative) shall register that system in the EU database.	Arts. 51, 60

cont'd on next page

See Proposed AI ACT, *supra*, at 54, 64-65, 67-68, 74 (emphasis added).

High-Risk AI Systems: (続き) providersの義務

high-risk AI sysのプロバイダの義務 E.g. ...

corrective actions	<ul style="list-style-type: none">- Providers who have reason to consider that the sys is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate.- Providers shall share the information with distributors, importers, et al.	Art. 21
information to national competent authorities, notified bodies, et al.	<ul style="list-style-type: none">- Providers shall inform national competent authorities, notified bodies, et al of risks/non-compliance/corrective actions, etc.	Art. 22

cont'd on next page

See Proposed AI ACT, *supra*, at 55 (emphasis added).

High-Risk AI Systems : (続き) providersの義務

high-risk AI sysのプロバイダの義務 E.g. ...

affixing CE marking	<u>The CE marking shall be affixed</u> visibly, legibly, and indelibly [hard to being erased] to the sys, their packaging, or to the accompanying documentation , as appropriate, in accordance with another applicable Directive re CE mark.	Art. 49
demonstrating conformity upon request from nat'l competent authorities	Upon the national competent authorities' request, providers shall provide them with all the information and documentation necessary to demonstrate sys' conformity with the requirements.	Art. 23

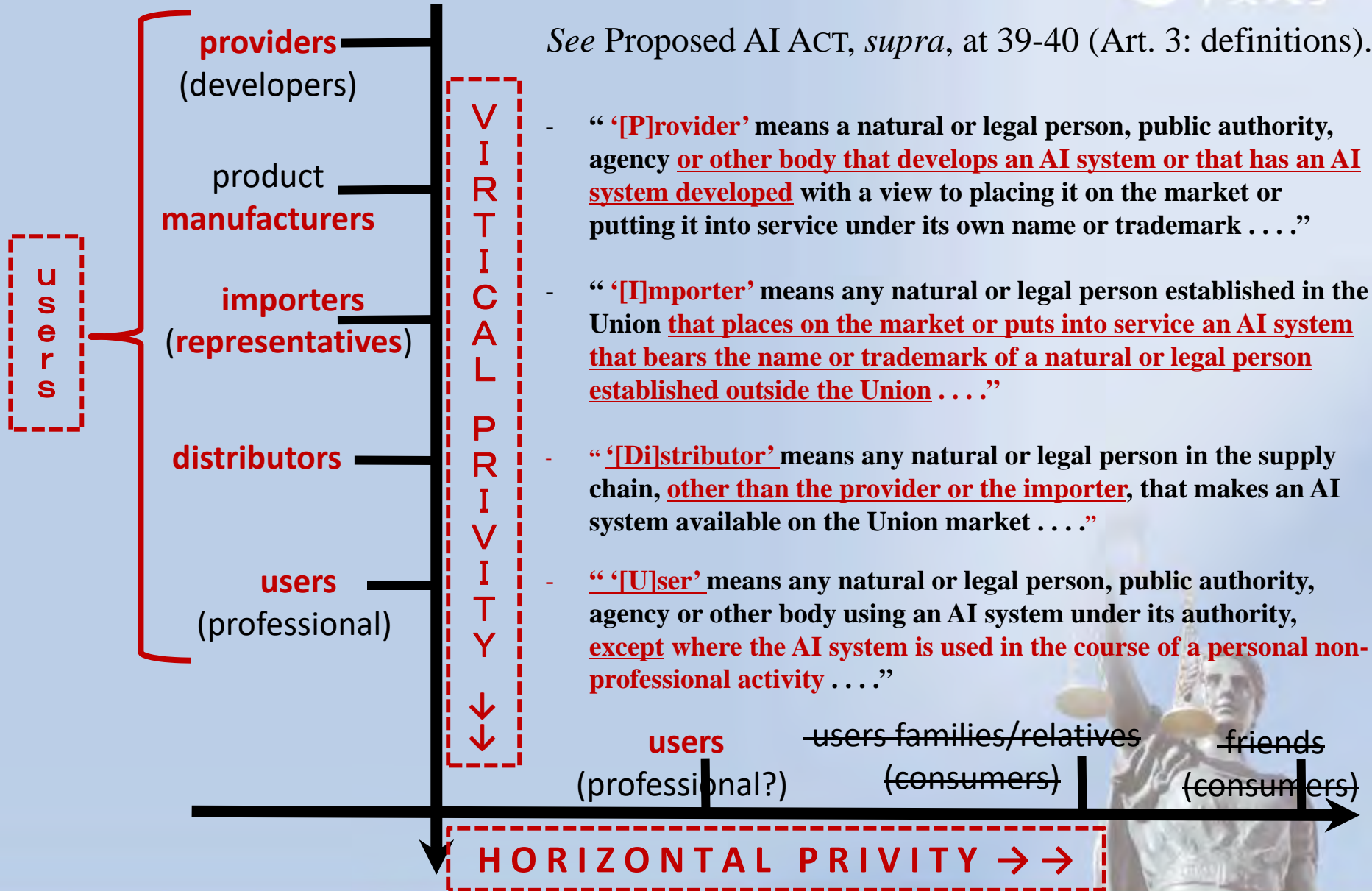
END OF THE TABLE

See Proposed AI ACT, supra, at 68 (emphasis added).



PRIVITY

See Proposed AI ACT, *supra*, at 39-40 (Art. 3: definitions).



High-Risk AI Systems: (続き)

“manufacturers”の義務

high-risk AI sysの製造業者の義務 E.g. . . .

obligations of product manufacturers	The manufacturer of the product, to which ANNEXES II, Sec. A [other applicable Directives/Regulations] applies, <u>shall take the responsibility of the compliance of the AI system with this Regulation</u> and, as far as the AI system is concerned, <u>have the same obligations imposed</u> by the present Regulation <u>on the provider</u> .	Art. 24
---	---	---------

END OF THE TABLE

See Proposal for AI ACT, *supra*, at 55 (Art. 24)(emphasis added).



High-Risk AI Systems: (続き)
“representatives”の義務

See supra slide at 11.



High-Risk AI Systems: (続き)

“distributor”の義務

high-risk AI sysの販売者の義務 E.g. ...

obligations of distributors

Distributor shall verify that:

- the sys bears CE conformity marking;
- it is accompanied by documentation and instruction for use; and
- provider and importer have complied with this Regulation's requirements.

Where a distributor considers the sys does not comply with the requirements, it shall not make the sys available on the market..

Distributors shall ensure that the storage or transport conditions do not jeopardise the sys' compliance with the requirements.

Where a distributor considers the sys which it made available on the market does not comply with the requirements, then, it shall take the corrective actions, withdraw it, recall it, or ensure that the provider, the importer, or any relevant operator as appropriate, takes those corrective actions.

Upon a reasonable request, distributors shall provide the national competent authorities with all necessary information and documentation to demonstrate the conformity. Also, they shall cooperate with those authorities on any action which they take to the sys.

Art. 27

See
Proposal for
AI ACT,
supra, at 57
(emphasis
added).

END OF THE TABLE

High-Risk AI Systems : (続き)

“[those who put their names on the sys / modifiers]”

の義務

high-risk AI sysの表示業者・修正者の義務 E.g. . . .

obligations of anyone who puts his name on the sys or modifies it / providers released from their obligations when someone modified their systems

Any distributor, importer, user, or other third party shall be considered to be the provider when it carries out any one of the followings:
(a) placing the sys on the market under its name or trademark;
(b) modifying the intended purpose of the sys; or
(c) making a substantial modification of the sys.

_____.
In case of the (2) or (3) above, the provider is no longer considered to be the provider.

Art. 28

See Proposal for AI ACT, *supra*, at 57 (emphasis added).

END OF THE TABLE

High-Risk AI Systems: (続き)

“users (professional)”の義務

high-risk AI sysの販売者の義務 E.g. ...

obligations
of users

Users shall use the sys in accordance with its instruction for use.
To the extent the user exercises control over the input data, that **user shall ensure that input data is relevant** in view of the intended purpose of the high-risk AI system.

Users shall monitor the sys' operation based on the instruction for use.

When they have reasons to consider the use might result in a certain risk, then, they shall inform the provider or distributor and suspend the use.

When users identify serious incident or any malfunction, then, they shall inform the provider or distributor, and suspend the use.

Users shall keep the logs to the extent such logs are under their control for an appropriate period of time in light of the intended purpose of the sys and applicable laws.

Credit institutions shall maintain the logs in accordance with another Directive applicable.

Art. 29

See
Proposal for
AI ACT,
supra, at 58
(emphasis
added).

END OF THE TABLE

Conformity Assessment

Proposed AI ACT, *supra*, at 64-65 (emphasis added).

Mainly, there are two (2) tracks as follows:

- 1 For high-risk AI systems listed in point 1 of Annex III [which means **“Biometric identification and categorisation of natural persons”**], where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:
 - (a) the conformity assessment procedure based on **internal control** referred to in **Annex VI**;
 - (b) the conformity assessment procedure based on assessment of **the quality management system** and assessment of the **technical documentation**, with the involvement of a **notified body**, referred to in **Annex VII**.

[continued on next page]

Proposal for AI ACT, *supra*, at para. 1, Article 43 (emphasis added).

Conformity Assessment

1 [continued from the former page]

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in **Annex VII**.

For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

Proposal for AI ACT, *supra*, at para. 1, Article 43 (emphasis added).

Conformity Assessment

Proposed AI ACT, *supra*, at 64-65 (emphasis added).

Annex VI's conformity assessment is, for example, as simple as follows:

ANNEX VI

CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL

1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2 to 4.
2. The **provider verifies** that the established **quality management system** is in **compliance with** the requirements of Article 17.
3. The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2.
4. The **provider also verifies** that **the design and development process** of the AI system and **its post-market monitoring** as referred to in Article 61 **is consistent with** the **technical documentation**.

ANNEXES, *supra*, VI (emphasis added).

Conformity Assessment

Proposed AI ACT, *supra*, at 64-65 (emphasis added).

And, for example, the Annex IV track is used as follows:

2 For high-risk AI systems referred to in points 2 to 8 of Annex III [which means **other than point 1: i.e., “Biometric identification and categorisation of natural persons”**], **providers shall follow** the conformity assessment procedure based on internal control as referred to in **Annex VI, which does not provide for the involvement of a notified body**.

Proposal for AI ACT, *supra*, at para. 2, Article 43 (emphasis added).

However, the Regulation continues as follows:

6 The **Commission is empowered to** adopt delegated acts to **amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof**. The Commission **shall** adopt such delegated acts **taking into account the effectiveness of the conformity assessment procedure based on internal control** referred to in Annex VI **in preventing or minimizing the risks to health and safety and protection of fundamental rights** posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

Id. para. 6 (emphasis added).

Certificate

Article 44 *Certificates*

1. **Certificates issued by notified bodies in accordance with Annex VII** shall be drawn-up in an official Union language determined by the Member State in which the notified body is established or in an official Union language otherwise acceptable to the notified body.
2. Certificates shall be valid for the period they indicate, which **shall not exceed five years**. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures.
3. Where a notified body finds that an AI system no longer meets the requirements . . . it shall . . . suspend or withdraw the certificate issued or impose any restrictions

See Proposed AI ACT, supra, at 65-66 (emphasis added).

EU Declaration of Conformity



Proposed AI ACT, *supra*, at 67-68 (emphasis added).

Article 48

EU declaration of conformity

1. The **provider shall draw up a written EU declaration of conformity for each AI system** and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.
2. The **EU declaration of conformity shall state that the high-risk AI system in question meets the requirements** set out in Chapter 2 of this Title. The EU declaration of conformity **shall contain the information set out in Annex V** and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.
-
5. The **Commission shall be empowered to** adopt delegated acts in accordance with Article 73 for the purpose of **updating the content of the EU declaration of conformity set out in Annex V in order to introduce elements that become necessary in light of technical progress.**



CE Marking of Conformity

Proposed AI ACT, *supra*, at 68 (emphasis added).

Article 49

CE marking of conformity

1. **The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems.** Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to **the packaging or to the accompanying documentation, as appropriate.**
2. The CE marking referred to in paragraph 1 of this Article shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.
3.



Document Retention / Registration



Proposed AI ACT, *supra*, at 68.

Article 50

Document retention

The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

- (a) the technical documentation referred to in Article 11;
- (b) the documentation concerning the quality management system referred to Article 17;
- (c) the documentation concerning the changes approved by notified bodies where applicable;
- (d) the decisions and other documents issued by the notified bodies where applicable;
- (e) the EU declaration of conformity referred to in Article 48.

Article 51

Registration

Before placing on the market or putting into service a high-risk AI system referred to in Article 6(2), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.



EU Database for Stand-Alone High-Risk AI Systems

Proposed AI ACT, *supra*, at 74.

Article 60

EU database for stand-alone high-risk AI systems

1. The **Commission shall, in collaboration with the Member States, set up and maintain a EU database** containing information referred to in paragraph 2 concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Article 51.
2. The data listed in Annex VIII shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.
3. Information contained in the **EU database shall be accessible to the public.**
4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.
5. The Commission shall be the controller of the EU database. It shall also ensure to providers adequate technical and administrative support.

Post-Marketing Monitoring



Proposed AI ACT, *supra*, at 74-75.

Article 61

Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. **Providers shall establish and document a post-market monitoring system** in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.
2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems **throughout their lifetime**, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.
3. The post-market monitoring system shall be based on a post-market monitoring plan. **The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV**. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.
4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.

Incident and Malfunctioning

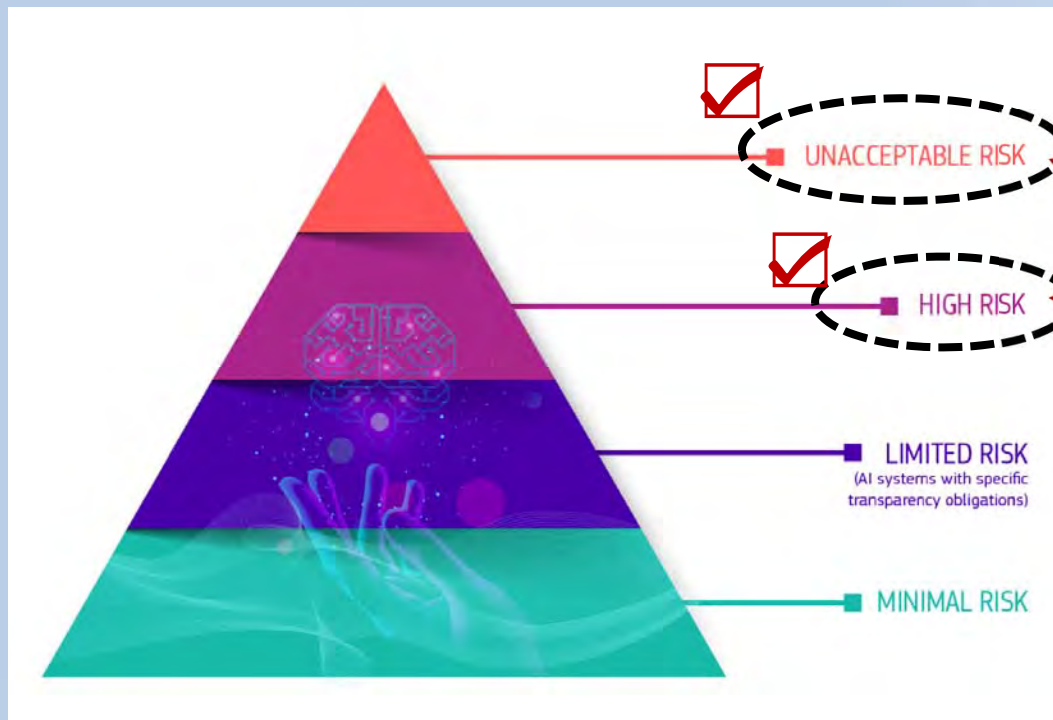
Article 62

Reporting of serious incidents and of malfunctioning

1. **Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning** of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights **to the market surveillance authorities** of the Member States where that incident or breach occurred.
Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.
2. Upon receiving a notification related to a breach of obligations under Union law intended to protect fundamental rights, **the market surveillance authority shall inform the national public authorities or bodies** referred to in Article 64(3). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1. That guidance shall be issued 12 months after the entry into force of this Regulation, at the latest.
3. For high-risk AI systems referred to in point 5(b) of Annex III which are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU and for high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, the notification of serious incidents or malfunctioning shall be limited to those that that constitute a breach of obligations under Union law intended to protect fundamental rights.

禁止 AI sys

生体認証への嫌悪



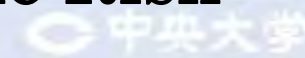
生体認証は、

- ✓ 〈禁止〉又は
- ✓ 〈ハイリスク〉

に分類



Prohibited AI Practices / An Unacceptable Risk



Article 5

1. The following artificial intelligence practices shall be **prohibited**:

- (a) the placing on the market, putting into service or use of **an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour** in a manner **that causes or is likely to cause that person or another person physical or psychological harm**;
- (b) the placing on the market, putting into service or use of an **AI system that exploits** any of the **vulnerabilities of a specific group of persons** due to their age, physical or mental disability, **in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm**;
- (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the **evaluation or classification of the trustworthiness of natural persons** over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with **the social score leading to either or both of the following**:
 - (i) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof in social contexts which are **unrelated to the contexts** in which the data was originally generated or collected;
 - (ii) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof that is **unjustified or disproportionate to** their social behaviour or its gravity;
- (d) the use of **'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives**:
 - (i) **the targeted search for specific potential victims** of crime, including missing children;
 - (ii) **the prevention of a specific, substantial and imminent threat to the life or physical safety** of natural persons **or of a terrorist attack**;
 - (iii) **the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence** referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

Proposal for AI ACT, *supra*, at 43-44 (emphasis added).

Prohibited AI Practices / An Unacceptable Risk

2. The use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in **paragraph 1 point d)** shall take into account the following elements:

- (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
- (b) **the consequences of the use of the system for the rights and freedoms of all persons concerned**, in particular the seriousness, probability and scale of those consequences.

In addition, the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards **paragraphs 1, point (d) and 2**, each individual use for the purpose of law enforcement of a ‘real-time’ remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. **However, in a duly justified situation of urgency**, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the ‘real-time’ remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

Id. at 43-44 (emphasis added).

Transparency Obligations for Certain AI Systems

E.g. . . .

specific risks
of
manipulation

“1 Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.”

“This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.”

“2 Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.”

Title IV,
Art. 52

See
Proposal
for AI ACT,
supra, at
69
(emphasis
added).

cont'd to next page

Transparency Obligations for Certain AI Systems

E.g. . . .

specific risks
of
manipulation

“3 Users of an AI system that generates or manipulates image, . . . that appreciably resembles existing persons, . . . or events and would falsely appear to a person to be authentic or truthful (‘deep fake’), shall disclose that the content has been artificially generated or manipulated.”

“However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.”

Title IV,
Art. 52

See
Proposal
for AI ACT,
supra, at
69
(emphasis
added).

END OF THE TABLE



日本の諸原則・ガイドライン等との類似点も

E.g.:

- human oversight
- “as appropriate to the circumstance” (*E.g.*, Art. 14)
- “remain aware of the possible tendency of **automatically relying or over-relying on the output** produced by a high-risk AI system (**‘automation bias’**), **in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons**” (Art. 14)
- “be able to intervene on the operation of the high-risk AI system or interrupt the system through a “stop” button or a similar procedure” (Art. 14) kill switch SH 論文
- “adversarial attack” (Art. 15)



学ぶべき／研究 & 考慮すべき点も

E.g., human oversight

就活等で既に利活用している例が日本ではあるらしいが、human oversightが必要かも...



Organizations / Governance



European Commission

See, e.g., Proposed AI ACT, supra, at 50, 58-59, 60, 72.

European Artificial Intelligence Board (“Board”)

Head of the Authorities

European Data
Protection Supervisor

National Supervisory Authorities

Head of the Authorities

National Supervisory Authorities

A Member State

National Competent Authorities

National Supervisory Authority

sufficient persons with
professional knowledge

sufficient competent persons

notifying authority (nat'l accreditation body)

market surveillance authority

notified bodies / conformity assessment bodies

Verifying the conformity

providers

AI Regulation Proposed by EU Commission

Thank You

