ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

AI CYBERSECURITY STANDARDISATION AND ITS OVERLAP WITH DSA AND CRA

JUDr. Michal Rampášek

Comenius University, Faculty of Law
Institute of Information Technology Law and Intellectual Property Law
rampasek1@uniba.sk

Abstract: The provision of digital products and digital services has in common that it integrates more and more artificial intelligence (AI) systems and, above all, the so-called foundation models. Using these elements of artificial intelligence brings several cybersecurity challenges. The key element in achieving the cyber security of digital products and digital services is, firstly, the achievement of a high level of standardization of artificial intelligence and subsequent technical standardization. AI cybersecurity is key to achieving trustworthiness of AI and vice versa. The mentioned facts are also reflected in the latest version of the draft Act on artificial intelligence (AI Act). As part of this paper, the focus is on standardization in the field of cyber security of artificial intelligence and the importance of the foundation models. At the same time the relations of the draft AI Act with the Digital Services Act (DSA) and the draft Cyber Resilience Act (CRA) are highlighted.

Keywords: cybersecurity, standardisation, ai, foundation models, ai act, dsa, cra

Introduction

Innovating digital products and services has become a critical component of business success. Artificial intelligence ("AI") is making significant advances in the way products and services are created and what features they offer to consumers. However, along with

commercial success, the security of such new products and services that integrate AI cannot be forgotten. In this paper, we explore how AI standardization in cybersecurity will support the development of trustworthy digital products and services, by extending the analysis to the draft AI Act[1] together with the draft Cyber Resilience Act ("CRA")[2] and the Digital Services Act ("DSA").[3]

1. Cybersecurity of AI

Cybersecurity of AI-featured digital products and services reaches far beyond the usual protection of digital assets. Cybersecurity is also considered instrumental to the correct implementation of trustworthiness features of AI, and vice versa, the correct implementation of trustworthiness features is key to ensuring cybersecurity.[4]

What is the cybersecurity of AI more specifically? Considering various interpretations, in a broader sense it complements protection of the confidentiality, integrity and availability of assets across the life cycle of an AI system, with trustworthiness features such as data quality, oversight, robustness, accuracy, explainability, transparency and traceability.

AI assets include machine learning („ML") models and algorithms, together with training data sets. ML techniques and algorithms are predominant in current AI systems or applications.

The real change of paradigm in building AI systems, or applications, however, came with development of large ML models, known as *foundation* models.

---

[1] In wording of amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), [cit. 4 September 2023] available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

[2] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (12429/22, COM(2022)454 final) known as the Cyber Resilience Act

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[4] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 6. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

2. Foundation models

The Stanford Institute for Human-Centered Artificial Intelligence's Center for Research on Foundation Models introduced the term "foundation model" in 2021.[5] A foundation model is a large ML model that is trained on broad data, generally using self-supervised learning at scale, that can be adapted (fine-tuned) to a wide range of downstream tasks.[6] AI systems with specific intended purpose or general-purpose AI systems can be developed by using a general foundation model at their core, which means that each foundation model can be reused in countless downstream AI systems and products. Indeed, foundation models are fine-tuned to create customer-facing apps. For example, OpenAI's ChatGPT and GPT-4 have become the basis for many chatbots and applications requiring human language understanding.

From a technological point of view, foundation models predate 2021 — they are based on deep neural networks (a class of ML models), self-supervised learning and transfer learning algorithms, and large-scale datasets. Progress in research, engineering and supercomputing, particularly in scaling of these methods to ever larger training datasets and resulting models, led to an inflection point, when these models began to manifest emergent capabilities and became more generally reusable. Their effectiveness across so many tasks stimulates homogenization, with these models serving as the foundation to build upon.

Emergence and homogenization are therefore key traits of foundation models. However, the characteristics of current ML algorithms and of the training data, that are not fully annotated and vetted by humans, also lead to a degree of opacity. A resulting model emerges from the training procedure rather than being explicitly prescribed by the creators. It may exhibit emergent properties and capabilities, both good and bad, that were not anticipated. For example, a model trained on a large natural language dataset may learn to write its own stories without being explicitly programmed to do so, but may also acquire harmful biases or hallucinate false facts. Homogenization means useability across many domains. This allows significant progress, but also introduces the possibility of failure across different applications due to a single deficiency in the underlying model.

[5] Bommasani, R. et al.: On the opportunities and risks of foundation models (2021) [cit. 31 August 2023] available at: https://crfm.stanford.edu/report.html

[6] Ibid

Existing foundation models have been demonstrated to be particularly effective in fields such as Natural language processing and Computer vision with foundation models such as GPT-3 and 4, BERT, PaLM-2, Llama-2, Stable Diffusion, DALL-E 2. Most recent foundation models work with multiple data types. They are multimodal, meaning they can process information in not only text format, but also pictures or even videos. Foundation models can be applied to a wide range of industries, including healthcare, education, translation, social media, law, and more. Use cases that exist in all those industries include content creation, text summarization, translation, answering questions, image generation & classification, etc.[7]

Foundation models are distributed both as proprietary as well as open-source, while they may differ along key dimensions such as cost structure, time-to-market, latency, flexibility and transparency, and security and governance. In respect to the security and governance of large language models and generative models there exist large gaps. Proprietary and open-source models both exhibit risks in different aspects. Proprietary models offer added security and governance capabilities that open-source models lack. Although open-source models lack security and governance capabilities, they can be brought within businesses' security perimeter and securely fine-tuned on local data. That is why many enterprises avoid using or fine-tuning proprietary models.[8]

Despite the widespread deployment of foundation models, more research will be required since we currently lack a clear understanding of how these models work, when they fail, and what they are even capable of due to their emergent properties.[9]

From regulatory perspective, the foundation models are now being strongly focused on in the new draft AI Act.

[7] Dilmegani, C.: Foundation Models: Definition, Applications & Challenges in 2023, last updated 22 December 2022 [cit. 4 September 2023] available at: https://research.aimultiple.com/foundation-models/

[8] Lu. S,: Proprietary vs. Open Source Foundation Models, 15 May 2023, [cit. 5 September 2023] available at: https://tolacapital.com/2023/05/15/foundationmodels/

[9] Bommasani, R. et al.: On the opportunities and risks of foundation models (2021) [cit. 4 September 2023] available at: https://crfm.stanford.edu/report.html

3. AI Act

The draft AI Act states that cybersecurity is an important element of the requirement to ensure that high-risk AI systems are trustworthy and resilient against cyberattacks.

These high-risk systems are subject to a number of requirements, cybersecurity being one of them.[10] It follows that high-risk AI systems shall be designed and developed following the principle of security by design and by default.[11] The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training dataset ("data poisoning"), or pre-trained components used in training ("model poisoning"), inputs designed to cause the model to make a mistake ("adversarial examples" or "model evasion"), confidentiality attacks or model flaws, which could lead to harmful decision- making.

Generally, the draft AI Act permits high-risk AI systems subject to compliance with AI requirements and ex-ante conformity assessment.

The draft AI Act introduces presumption of conformity of AI systems, stating that high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the Cybersecurity Act[12] shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of the AI Act, where applicable, in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.[13]

ENISA stresses the importance of the inclusion of cybersecurity aspects in the risk assessment of high-risk systems in order to determine the cybersecurity risks that are specific to the intended use of each system, as well as the lack of standards related to the cybersecurity of artificial intelligence to cover performing conformity assessments.[14]

---

[10] AI Act , Article 15

[11] AI Act, Article 15 par. 1

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[13] AI Act, article 42 par. 2

[14] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 6. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

Together with the high-risk AI systems, the new draft AI Act expressly defines the foundation models[15] and focuses on obligations of providers of foundation models.[16]

In general, foundation models will not be classed as "high-risk" AI systems – unless they are directly integrated in such a high-risk AI system.[17] The obligations on providers of foundation models would apply regardless of whether the model is provided on a standalone basis or embedded in an AI system or a product. Foundation models would need to be also registered in an EU database.

The draft AI Act considers essential to clarify the legal situation of providers of foundation models. Foundation models should be subject to proportionate and more specific requirements including cybersecurity.

The providers would be obliged to „demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development", as well as draw up "extensive technical documentation and intelligible instructions for use" to help those that build AI systems using the foundation model to meet their own legal obligations.[18] They would further be required to meet obligations around data governance, ensure "appropriate levels" of performance, predictability, safety and cybersecurity, and conform to a range of sustainability standards.

Those providers of foundation models which are used in generative AI would face further obligation relating to transparency over when content has been created by an AI system and not a human and making publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

Stanford researchers evaluated compliance of 10 major foundation model providers with draft AI Act requirements and found that they largely do not comply.[19] Foundation model providers rarely disclose

[15] AI, Act, recitals 60e to 60h, Article 3 par. 1 point 1c

[16] AI Act, Article 28b

[17] Cameron, S., Scanlon, L.: MEPs' EU AI Act proposals focus on 'foundation models' [cit. 4 September 2023] available at: https://www.pinsentmasons.com/out-law/news/meps-eu-ai-act-foundation-models

[18] AI Act, Article 28b

[19] Bommasani, R. et al.: Do Foundation Model Providers Comply with the Draft EU AI Act? [cit. 4 September 2023] available at: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html

adequate information regarding the data, compute, and deployment of their models as well as the key characteristics of the models themselves. In particular, foundation model providers generally do not comply with draft requirements to describe the use of copyrighted training data, the hardware used, and emissions produced in training, and how they evaluate and test models.

Further, insightful is the comparison of different release strategies of foundation models. Open-source releases generally achieve strong scores on resource disclosure requirements (both data and compute), however, make it challenging to monitor or control their deployment. On the other hand, more restricted proprietary releases achieve better scores on deployment-related requirements, but tend to fall behind in resource disclosure. Open-sourcing a model makes it much more difficult to monitor or influence downstream use, whereas APIs or developer-mediated access provide easier means for structured access.[20]

It their conclusions Stanford researchers recommend[21] that foundation model providers should work towards industry standards that will help the overall ecosystem become more transparent and accountable.

4. Standardisation and Cybersecurity of AI

Standardisation should play a key role to provide technical solutions to providers to ensure compliance with the AI Act.

These standards have to be consistent and aimed at ensuring that AI systems or foundation models placed on the market or put into service in the Union meet the relevant requirements.[22]

The high-risk AI systems and foundation models which would be in conformity with such harmonised standards would be presumed to be in conformity with the requirements set in the AI Act.

Indeed, the Commission adopted Implementing decision[23] and requested the European Committee for Standardisation ("CEN") and

[20] Ibid

[21] Ibid

[22] AI Act, article 40 par. 1b

[23] Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence („Implementing decision") [cit. 4 September 2023] available at: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

the European Committee for Electrotechnical Standardisation ("CENELEC") to draft the new European standards or European standardisation deliverables, as listed in Annex I of the Implementing decision. The Implementation decision forms the basis for development of future 10 harmonised European standards:

1. Risk management systems for AI systems
2. Governance and quality of datasets used to build AI systems
3. Record keeping through logging capabilities by AI systems
4. Transparency and information provisions for users of AI
5. Human oversight of AI systems
6. Accuracy specifications for AI systems
7. Robustness specifications for AI systems
8. *Cybersecurity specifications for AI systems*
9. Quality management systems for providers of AI systems, including post-market monitoring processes
10. Conformity assessment for AI systems

The role of cybersecurity is within all sets of requirements that can be considered as referring to the trustworthiness of an AI ecosystem.

The current state in the field of standardisation related to cybersecurity of AI is influenced by the fact that some aspects of cybersecurity are still the subject of research and development, and therefore might not be mature enough to be standardised.

In common, existing general purpose technical and organisational standards (such as ISO-IEC 27001 and ISO-IEC 9001) can contribute to mitigating some of the risks faced by AI.

There are only a few existing specific standards related to the cybersecurity of AI, most of them are still being drafted or are under consideration and planned. One of the most notable is the US National Institute of Standards and Technology ("NIST") AI Risk Management Framework (AI RMF 1.0).[24]

CEN/CENELEC has identified a list of standards from International Organization for Standardization ("ISO") and International Electrotechnical Commission ("IEC"), that are of interest for AI cybersecurity and might be adopted/adapted by CEN-CENELEC based on their technical cooperation agreement. Identified standards include the ISO 27000 series on information security management systems,

[24] US National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). [cit. 31 August 2023] available at: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

which may be complemented by the ISO 15408 series for the development, evaluation and/or procurement of IT products with security functionality, as well as sector-specific guidance.[25]

In addressing the extended scope of cybersecurity of AI, which includes trustworthiness characteristics, data quality, AI governance, AI management systems, etc., following standards has been identified as having direct applicability to the draft AI Act and is being considered for adoption/adaption by CEN/CENELEC:

- ISO/IEC 22989:2022, Artificial intelligence concepts and terminology (published),
- ISO/IEC 23053:2022, Framework for artificial intelligence (AI) systems using machine learning (ML) (published),
- ISO/IEC DIS 42001, AI management system (under development),
- ISO/IEC 23894, Guidance on AI risk management (publication pending),
- ISO/IEC TS 4213, Assessment of machine learning classification performance (published),
- ISO/IEC FDIS 24029-2, Methodology for the use of formal methods (under development),
- ISO/IEC CD 5259 series: Data quality for analytics and ML (under development).[26]

As noted above, it is likely that CEN and CENELEC will transpose standards from ISO and IEC, respectively, to future European standards to ensure compliance with the AI Act.

There are still standardisation gaps, thus we can expect further standards regarding AI systems risk catalogue and risk management, and AI trustworthiness characterisation (e.g., robustness, accuracy, safety, explainability, transparency and traceability). However, it is likely that additional standardisation gaps and needs may become apparent only as the AI technologies advance.

5. AI Act vs. DSA

The high-risk AI systems and foundation models hold growing importance to many downstream applications and systems, having

[25] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 12. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

[26] Ibid, p. 13

direct impact also to digital services and digital products, as such services or products may be classified, composed of, or use high-risk AI systems or foundation models. In other words, regulation and future cybersecurity standardisation of AI systems and foundation models will have a direct impact also on digital services regulated under the DSA, in particular online platforms, as well as on digital products that would be regulated under the CRA.

The DSA establishes harmonised rules for the online environment, aiming to ensure security, predictability, and trust by introducing mechanisms for the protection of the fundamental rights. The act regulates obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content. In particular sales platforms, social networking platforms, very large online platforms ("VLOPs") and very large online search engines ("VLOSEs"). The rules are designed asymmetrically, so that larger intermediary services with significant societal impact (VLOPs and VLOSEs) are subject to stricter rules.

The draft AI Act follows the above-mentioned stricter rules for VLOPs stating that AI systems used by those online platforms in their recommender systems would comply with the requirements laid down under the AI Act, including the technical requirements on data governance, technical documentation and traceability, transparency, human oversight, accuracy and robustness. Compliance with the AI Act should enable such VLOPs to comply with their broader risk assessment and risk-mitigation obligations in Article 34 and 35 of the DSA.[27]

AI systems intended to be used by social media platforms designated as VLOPs, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform are newly expressly included to the high-risk systems category in the draft Annex III of the AI Act.

The DSA imposes transparency reporting obligations for providers of intermediary services (other than micro or small enterprises), in particular to make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period.[28] That includes any use made of automated

[27] AI Act, recital 40b
[28] DSA, Article 15

means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.

VLOPs and VLOSEs are subject to enhanced transparency obligations, including annual independent audits to assess their compliance with their obligations.[29]

In this respect it is worth noting also the Commission's draft delegated regulation laying down rules on the performance of audits for very large online platforms and very large online search engines („Audit rules").[30]

The purpose of the Audit rules is to set out the necessary rules for the procedures, methodology and templates used for the audits of VLOPs and VLOSEs as required under Article 37 of the DSA.

The Audit rules pay attention inter alia to auditing methodologies for algorithmic systems. In its explanatory note the Audit rules stress that algorithmic systems such as *advertising systems*, *content moderation technologies*, *recommender systems* and other functionalities used by online platforms and search engines relying on novel technologies such as generative models (i.e. foundation models) are particularly important elements to analyse when assessing compliance with risk assessment and risk mitigation obligations.

6. AI Act vs. CRA

The draft CRA aims to impose cybersecurity obligations on all products with digital elements (digital products) meaning any software or hardware product and its remote data processing solutions, including software or hardware components if placed on the market separately.[31] The regulation impacts a broad scale of products including critical products such as browsers, password managers, virtual private networks, operating systems, firewalls, IDS/IPS, routers, switches, smart cards, etc. This piece of horizontal legislation introduces

[29] DSA, Article 37

[30] Draft Commission Delegated Regulation (EU) supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines (2023), [cit. 4 September 2023] Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en

[31] Draft CRA, Article 3 par. 1

cybersecurity by design and by default principles and imposes a duty of care for the lifecycle of products. The act also covers AI systems, including the cybersecurity of products with digital elements that are classified as high-risk AI systems.

Manufacturers of digital products would have to ensure that digital products comply with essential cybersecurity requirements and conformity assessment procedures before placing them on the market. Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks, without any known exploitable vulnerabilities.

The Commission's Implementing decision[32] in European standards/standardisation deliverables on Cybersecurity specifications for AI systems expressly mention the draft CRA, stating that *these standards shall take due account of the essential requirements for products with digital elements as listed in Sections 1 and 2 of Annex I to the CRA.*[33]

The CRA introduces the presumption of conformity, stating that products with digital elements classified as high-risk AI systems fulfilling the requirements of the CRA (Annex I), shall be deemed in compliance with the cybersecurity requirements of the AI Act.[34]

Conclusions

Wave of AI in recent years is attributable mainly to the foundation models. Although AI is not just about foundation models, it is their utility that accelerates AI's potential as a general-purpose technology with broad applicability throughout the whole economy. While the potential benefits are enormous, it is important not to overestimate the capability of foundation models.

Firstly, it is inevitable to support international and European standards development work focused on establishing common definitions, specifications for risk management systems, risk

[32] Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence („Implementing decision") available at: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

[33] Ibid, Annex II, point 2.8

[34] Draft CRA, Article 8 par. 1

classification criteria, and other elements of effective cybersecurity of AI. Work on the AI-related standards has already begun, however standards most likely will not be ready before the regulation enters into force.

In the AI regulation a risk and context-based approach remains the most effective strategy to minimize the risks of all AI, including those posed by foundation models. Following the results of the Stanford research cited above, we believe that the AI Act should consider additional critical factors to ensure adequate transparency and accountability of foundation model providers, including the disclosure of usage patterns. Such requirements would mirror transparency reporting for online platforms under the DSA. To avoid overburdening micro and small size companies these requirements should apply only to the foundation model providers that have a significant societal and economic impact.

Bibliography

1. BOMMASANI, R. et al.: *On the opportunities and risks of foundation models* (2021). 5 September 2023. [online], URL: https://crfm.stanford.edu/report.html
2. BOMMASANI, R. et al.: *Do Foundation Model Providers Comply with the Draft EU AI Act?* 5 September 2023. [online], URL: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html
3. CAMERON, S., SCANLON, L.: *MEPs' EU AI Act proposals focus on 'foundation models'.* 4 September 2023. [online], URL: https://www.pinsentmasons.com/out-law/news/meps-eu-ai-act-foundation-models
4. DILMEGANI, C.: *Foundation Models: Definition, Applications & Challenges in 2023*, last updated 22 December 2022. 4 September 2023. [online], URL: https://research.aimultiple.com/foundation-models/
5. European Union Agency for Cybersecurity (ENISA). *Cybersecurity of AI and Standardisation (Report)*. March 2023, 4 September 2023. [online], URL: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport
6. European Union Agency for Cybersecurity (ENISA). *Securing Machine Learning Algorithms* (Report). December 2021, 4 September 2023. [online], URL: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms

7. European Union Agency for Cybersecurity (ENISA). *Standardisation in support of the Cybersecurity Certification*. February 2020, 4 September 2023. [online], URL: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i
8. LU. S,: *Proprietary vs. Open Source Foundation Models*, 15 May 2023. 5 September 2023. [online], URL: https://tolacapital.com/2023/05/15/foundationmodels/
9. Proposal for the Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) in wording of amendments adopted by the European Parliament on 14 June 2023, 4 September 2023. [online], URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html
10. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (12429/22, COM(2022)454 final) (Cyber Resilience Act) 4 September 2023. [online], URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454
11. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
12. Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, 4 September 2023. [online], URL: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en
13. Draft Commission Delegated Regulation (EU) supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines (2023), 4 September 2023. [online], URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en
14. US National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). 31 August 2023. [online], URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf