AI

Main messages

- The EU considers it very important that artificial intelligence is developed, deployed and used in a way that benefits our citizens, societies and economies. We welcome the commitment of Microsoft to responsible AI.
- The benefits of AI will only materialise through uptake, but uptake requires trust.
- Therefore, through our AI package adopted in April 2021, we pursue the twin objective of supporting innovation and excellence and ensuring trust in AI.
- The main pillars of this approach are the revised Coordinated Plan on AI and the first comprehensive horizontal legislative proposal for Artificial Intelligence, the AI Act.
- The AI Act seeks to define the uses of AI technologies that are allowed and the conditions under which they can be deployed on the EU market.
- This Regulation will foster trust, legal certainty for businesses, and a well-functioning single market with uniform rules for AI. Our goal is to support innovation while making sure that people's legitimate concerns about the protection of their safety and fundamental rights are addressed.
- I believe that this goal will be achieved through a proportionate, risk-based approach.
- That is why the AI Act mainly focuses on high-risk systems. This is innovation-friendly because it addresses the real risks of the technology, while shielding systems that do not pose high risks to safety or fundamental rights from diverging national regulations.
- To further support excellence and innovation, the Commission will invest at least EUR 1 billion per year in AI from the Horizon Europe and the Digital Europe programmes in the period 2021–2027.
- The objective is to increase public and private investment in AI gradually to a total of EUR 20 billion per year over the course of this decade.

Defensives

The Commission has been busy adopting regulatory proposals for emerging technologies (AI) and for the digital/data space at large. Is this targeted against big tech companies?

- These rules are grounded in objective, non-discriminatory criteria that will apply regardless of the origin or place of establishment of the companies.
- Our goal is to build trust in emerging technologies, such as AI, by ensuring that risky applications comply with safety requirements and fundamental rights, while maintaining a proportionate approach.
- Trust is key for increasing the wide-scale uptake of AI and will in turn transform into more demand for the products and services of companies operating in the tech sector.
- Last but not least, we need to provide legal certainty for the European market: thus, companies outside the EU can operate in a predictable regulatory environment here.
- It is also about a level playing field and fair rules based competition in the digital space

Background

Microsoft is one of the founding partners of **the Partnership on AI (PAI)** along with many other tech giants. PAI is an open platform for discussion and engagement about AI and its influences on people and society. The **vision of the Partnership on AI** is a future where AI empowers humanity by contributing to a more just, equitable and prosperous world.

Microsoft's stated goal is to amplify human ingenuity through AI, while preserving shared societal values and expectations based on the following **six core principles** that guide their approach to responsible AI:

- Fairness: AI systems should treat all people fairly.
- Reliability & Safety: AI systems must be designed to operate within clear parameters and undergo rigorous testing to ensure that they respond reliably and safely to unanticipated situations and do not evolve in ways that are inconsistent with original expectations. People should play a critical role in making decisions about how and when AI systems are deployed.
- Privacy and security: AI systems must comply with privacy laws that regulate data collection, use and storage, and ensure that personal information is used in accordance with privacy standards and protected from theft.
- Inclusiveness: AI systems should empower everyone and engage people. AI solutions must address a broad range of human needs and experiences through inclusive design practices that anticipate potential barriers in products or environments that can unintentionally exclude people.
- Transparency: AI systems should be understandable. Providing contextual information about how AI systems operate so that people understand how decisions are made and can more easily identify potential bias, errors and unintended outcomes.
- Accountability: People who design and deploy AI systems must be accountable for how their systems operate. Accountability norms for AI should draw on the experience and practices of other areas, such as healthcare and privacy, and be observed both during system design and in an ongoing manner as systems operate in the world.

Microsoft **supports the AI Act's vision and direction** and finds it well balanced. At the same time, in its **written comments** Microsoft suggests *inter alia* that:

- The obligations of different actors should be calibrated. Accountability should be assigned to those closest to the potentially impacted citizens, particularly for high-risk scenarios, and AI suppliers frequently have no visibility as to how customers deploy these services into their own systems.
- They suggest introducing outcome and processed-based requirements for high-risk AI systems. Some of the requirements are seen as prescriptive or focused on specific scenarios, and therefore they may be workable in some cases, but ineffective in others.
- The grounding of the AI Act in the New Legislative Framework and the suggested post-market monitoring regime create some challenges in allocating obligations. The obligations of post-market monitoring of AI systems should be allocated closest to its uses.

Contacts – briefing contribution: [redacted]

Cybersecurity

Main messages

Ransomware

- We need to apply a holistic approach to the global fight against ransomware, allowing law enforcement to jointly investigate ransomware threats, countering illicit finance and the possibility for cyber-criminals to monetise ransoms as well as implementing specific resilience actions for ransomware.
- Moreover, strong internal action should ensure that nations are not cooperative towards cybersecurity criminals, allowing them to operate from their territory.
- On 22 June 2021, U.S. Secretary of Homeland Security Alejandro Mayorkas and Commissioner for Home Affairs Ylva Johansson agreed to create a working group dedicated to ransomware issues focusing on law enforcement. The kick off meeting of took place in November 2021.
- The private sector plays an important role. Public-Private Partnerships (PPPs) to fight cybercrime are essential given the fact that the cyberspace infrastructure is overwhelmingly held by private companies located under different jurisdictions.
- We acknowledge that the private sector needs incentives to improve its own security and to coordinate more effectively with national authorities and with each other. The Commission supports the establishment of PPPs under the Internal Security Fund.

NIS2 – revised Network and Information Security (NIS) Directive:

- Legislative deliberation started in January 2022.
- We are confident that they will go smoothly and can be finalised by mid-2022, with EU legislators aware of the importance of keeping the momentum and of ensuring that an effective and ambitious European cybersecurity framework is in place.
- EU legislators pay particular attention to the alignment between the NIS2 and the Digital Operation Resilience Act (DORA) proposals.

Resilience of critical entities:

- The Commission proposed a Directive on resilience of critical entities in December 2020, which is currently being negotiated between the Council and Parliament.
- The proposal would set up a new framework to ensure that critical entities in key sectors become more resilient against threats such as accidents, terrorist attacks, floods, fire or droughts. They shall be able to continue providing essential services in, and quickly “bounce back” into operations in case of a disruption or an incident.

Cyber Resilience Act (CRA):

- In the second half of this year, the Commission will propose legislation on common standards for digital products under a new European Cyber Resilience Act.
- The Act will set out horizontal cybersecurity requirements for digital products and ancillary services (hardware, but also ‘intangible’, like non-embedded software).

Joint Cyber Unit:

- In June 2021 we launched the process establishing a Joint Cyber Unit ensuring a coordinated response to incidents and cyber-enabled crises across the Union. The Joint Cyber Unit, once operational, could allow European crisis managers and IT experts to structurally cooperate with the US on crisis management.

- Information sharing and cooperation are key to successfully preventing and combating cybersecurity threats. The proposed Joint Cyber Unit would bring together different EU cybersecurity communities, defence, civilian, law enforcement and diplomacy. As we discovered with the COVID-19 pandemic, in order to respond to a cross-border crisis, we need to rely on all available experts, crisis managers and equipment.

Security Operations Centres (SOCs):

- We believe that Security Operations Centres can play a vital role in the constant and comprehensive supervision of cyber-space, the primary way to detect cyber threats and attacks. By relying on artificial intelligence and machine learning techniques, these Centres can detect the signs of a cyber attack early enough to allow proactive action.
- The Commission has proposed to improve the existing Security Operations Centres and create new ones. Linking them in a network, we will establish an EU cyber shield.
- In 2021-2022, EUR 110 million will be dedicated to SOCs.

Cybersecurity Competence Centre and Network:

- In order to better protect ourselves against cyber-attacks, it is also crucial to increase and better target our strategic public and private investments in cybersecurity. This will be the key task of the Cybersecurity Competence Centre in Bucharest.
- The Centre will establish a strategic agenda for technology development, in close collaboration with industry and the academic community.
- In addition, the Centre is responsible for the implementation of the cybersecurity funds of the Digital Europe and Horizon Europe programmes. This should, with the support of the private sector, generate funding of up to EUR 4.5 billion in cybersecurity by 2027.

EU funding in cybersecurity under EU programmes:

- The Commission is aware of the need for ambitious investments. Funding for cybersecurity in the 2021-2027 EU budget is under the Digital Europe Programme, and for cybersecurity research under Horizon Europe. This amounts to close to EUR 2 billion, which will be complemented by Member States and industry investment.
- Investments in the digital technology supply chain should be at least 20% of the Recovery and Resilience Facility, or EUR 134.5 billion out of EUR 672.5 billion.
- The EU is also stepping up its offer to its partners with major investments in infrastructure development through the EU Global Gateway. Between 2021 and 2027, the EU will mobilise up to EUR 300 billion of investments in digital, climate and energy, transport, health, education and research.
- Under NDICI-Global Europe, with an overall budget of EUR 79 billion, investments in building connections are expected to rise significantly. It has a 35% spending target for climate actions and an additional 10% approximately of the total funding will be dedicated to digital actions.

Background

Ransomware

The European police agency (Europol) is supporting ransomware investigations and, with private sector partners, runs the 'No More Ransom' campaign to increase awareness among companies and supply victims with decryption tools.

Increased threats, accompanied by high profile attacks impacting essential sectors across the Union, has led G7 leaders to commit to action on ransomware last year and the EU to launch a joint initiative with the United States.

Contacts – briefing contribution: [redacted]

DSA

Main messages

- The DSA sets rules on content moderation practices of online platforms, and its interaction with freedom of speech and healthy and well-informed public debate.
- It follows three objectives:
  - protect users from illegal goods or content online;
  - better secure their freedom of expression online; and
  - allow companies to emerge and scale in a borderless Internal Market.
- Platforms would have to apply effective measures against misuse of their systems and transparency mechanisms. Users will have the right to be informed about moderation policies and decisions by the platform, to contest them and seek redress.
- These rules should not create a disadvantage to smaller companies. The obligations are proportionate to size and societal reach. Very large platforms need to ensure that those 'public spaces' are open and fair: they will need to assess and address risks their systems pose to freedom of expression and other fundamental rights.
- Finally, the DSA contains a balanced enforcement mechanism:
  - Enforcemenr is primarily a task of national competent authorities, notably the Digital Services Coordinators, supported by the European Board of Digital Services.
  - For very large online platforms, often with significant cross-border impact, the rules provide for enhanced supervision and enforcement, involving the Commission.

Defensives

Why were user-based risk criteria used for determining what is a very large online platform (VLOP)?

- The designation based on user numbers is the most appropriate criterion for determining whether an online platform should be designated as a VLOP.
- Using the number of users as the only criterion for the definition of VLOPs has clear regulatory advantages. It creates a simple, future-proof system where it is easy to determine whether a platform has a significant reach in the single market, which will ensure legal certainty. The current criterion is also objective and non-discriminatory, which is something to which the Commission attaches particular importance.
- Designating a VLOP based on elements of risk might provide less legal certainty than the current criterion, particularly as elements of risk potentially lead to more ambiguity.
- In addition, it may lead to subjectivity and discrimination and risks triggering litigation over many years ahead of designating any platform. Such designation then also comes with reputational impacts on the platform.
- In this context, we believe the criterion that is currently used is a solid proxy for the societal risks platforms pose, while allowing for a smooth and efficient process.

Background

Position Microsoft position – DSA

- Points of support
  - Maintaining the basic principles of the e-Commerce Directive on country of origin, conditional liability and prohibition of general monitoring obligations.

- Overall objective to focus on illegal content and improving safety of online environment.
- Limitation of KYBC rules to marketplaces only; extending this to platforms that indirectly allow for distance contracts would be too great a burden on resources.
- Supporting the rationale of Article 8 (orders to act sent by national authorities to providers concerning unlawful content)

- Points of criticisms / recommendations
  - Lack of clarity about the definition of online platform (e.g. dissemination of information to the public) and qualification of services with ancillary or indirect sharing or editorial functions as well as search engines
  - Differentiation/lighter obligations to act on notices for pure B2B hosting providers, which may be prevented to get access to individual content for technical (encryption), contractual and regulatory (data protection) reasons.
  - Wrong incentives to contest removal decisions triggered by alternative dispue resolution (ADR) systems (Microsoft).
  - No-profiling option for recommender system may be not workable (Microsoft).
  - Search engine should be considered caching services.
  - Amend the definition of “online platforms” to provide greater clarity on the meaning of “disseminates to the public”—in particular, to take into account the overall purpose of the service by recognizing the difference between social media platforms, expressly designed so that content can reach a broad audience, and products with social features.
  - Exemption of liability for intermediaries abiding to orders and clarification of their interaction with possible data protection obligations.
  - More flexibility in organising content of transparency reports (categories may differ depending to national law).
  - User-based very large online platforms (VLOPs) criteria not linked to risk and inconsistent with SME criteria (company based).
  - More flexibility in statement of reasons (in particular possibility to refer to terms and conditions removal only).
  - More flexibility in granting priority to trusted flaggers (risk of conflict with priorities of moderation policies).
  - Consistency of right to refer decisions to internal handling mechanism or ADR with obligations to remove content under orders should be ensured (excluding parallel review of the order and/or no liability for platform complying with order).
  - Need to define better scope of data access obligations, envisage the possibility to refuse/adjust requests for security and confidentiality concerns and clarifications of the use of data and supervision of the access by vetted researchers.
  - Narrowing the list of serious crimes that require notification of suspects.
  - Clarifying and narrowing down the transparency obligations on advertising (high level parameters and less detailed info in repository for VLOPs).

Contact – briefing contribution: [redacted]