EUROSMART
The Voice of the Digital Security Industry

EUROSMART answer to the public consultation on the Draft AI Ethics Guidelines of the High-Level Expert Group on Artificial Intelligence (AI HLEG)

Introduction: Rationale and Foresight of the Guidelines

On the 25th April 2018, the Commission defined in its Communication an European approach for Artificial Intelligence.

This Communication sets out a European initiative based on a triple approach:

1. Boost the EU technological and industrial AI uptake across the economy through investments in research and innovation and better access to data;
2. Prepare for socio-economic changes;
3. Ensure an appropriate ethical and legal framework.

The Draft AI Ethics Guidelines of the High-Level Expert Group on Artificial Intelligence (AI HLEG) contributes to raise the awareness on the close relationship between ethics and technological choices in the digital age. When it comes to the development and implementation of AI, the deep interrelation between ethics and technology modify the way we usually think about technological advances by bringing together deferent disciplines: Ethics, Law, Technology, Industry and Cybersecurity.

Eurosmart welcomes the European Commission initiative and the creation of the High-Level Expert Group on Artificial Intelligence. This initiative plays a key role when defining a common understanding of what the challenges brought by AI are. Organisations, value chain, their related threats and opportunities will be impressively impacted, AI's incidence on the cyber-resilience of our continent must be conscientiously analysed. AI is also challenging both the values and the governance of the European Union.

Definition of AI

Eurosmart supports the provided definition of what the Artificial Intelligence is. This first achievement of the High-level Expert Group on Artificial Intelligence is a milestone to define common rules to make citizens, governments and businesses benefit from trustworthy AI.

> *"Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behavior by analysing how the environment is affected by their previous actions.*

> As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge, *representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems"*

Based on this definition, the European legislator and the industrial and scientific community must nurture an ambitious approach to develop reliable AI based on the European technical know-how and on our common values in reference to the Charter of Fundamental Rights of the European Union.

Can AI be considered as a product placed on the market?

The accompanying document to the Draft AI Ethics Guidelines entitled "A definition for AI" describes what AI is made of. (figure2). Even if the provided elements are a very crude oversimplification of the state of the art, it does have the merit of once highlighting several essential technologies which underlie AI.

- Machine learning is composed by data and their processing.
- Robotics is manly hardware oriented
- Reasoning involved embedder softwares.

From the industrial point of view and regarding the future market evolutions, Eurosmart wonders if **AI could be considered as a product** in the meaning of the EU Single Market related legislations. As a product, the 1985 Product liability Directive 85/374/EEC would apply.

The benefit of this directive lies in its balanced approach between the free movement of goods within the Union, the protection of citizen's safety and the empowerment of the economic actors. For a given product, the full liability is placed on the producer, the importer or the distributor of products. The same approach could apply to AI and thus, with the support of International and European standards.

Chapter I: Respecting Fundamental Rights, Principles and Values - Ethical Purpose

Is AI a Dual use?

Eurosmart underlines that a technology cannot inherently be ethical. It the way the technological application will be developed and implemented which defines its ethical aspect. Considering that this technology could be used at both civilian and military levels, for peaceful and military aims, AI could be a **Dual Use in the sense of the Wassenaar Arrangement**. Deep competences and full mastery of the AI technology is very crucial for the digital sovereignty of our continent. Eurosmart enjoins the High-level Expert Group on Artificial Intelligence and the Commission to further analyse this issue. By the way, the dual use can be also seen from attacker for cyberattacks in the combination of human and computer as well as from the defender of cyberattacks, for example in industry and in governments. Two examples: Intrusion Detection Systems (IDS) with learning function in industry and Chabot's in public services.

Protection of Personal Data is a major ethical aspect

Eurosmart supports the approach adopted by the AI HLEG which is underpinned by the European values and the Charter of Fundamental Rights. These common values have inspired all the data privacy and all the Digital single market legislation. We recommend working on a more comprehensive statement based on the article 8 "Protection of Personal Data". This article allows the citizen to benefit from its personal data as an inalienable freedom and places the respect of this rule of law **under the protection of an independent authority.** We recommend that both ethical and technical aspects should carefully be monitored and guaranteed by an independent and trustworthy Third party. It shall be a key principle while designing and placing on the market any AI solutions.

Chapter II: Realising Trustworthy AI

Standards

The document mentioned technical and non-technical methods to achieve Trustworthy AI. Standards are put forward to ensure that qualitative and trustworthy solutions are indicated to the consumers actors and governments.

Due to the sensitive nature of AI, standards must be carefully handled. The European Union should not enshrine in law any "private" standards or unilaterally business-driven initiatives which could lead to an imbalanced power relationship. It must be considered that AI technologies will fast growing, such an approach would deter innovation. Eurosmart enjoins the AI HLEG to rely on European and International standards to support the AI take-off. European Standardisation Organisations' (ESOs) work should be recognised as the primary reference for a trustworthy AI development. Eurosmart recommends referring to the Mustistakeholder Platform (MSP) for Standardisation while developing priorities for AI in the Annual standardisation rolling-plan. **Both AI HLEG and the European Commission must pay attention to international standards for AI which are under development (ISO/IEC WD 22989) and standards resulting from ongoing work in ISO/IEC JTC 1, SC 42 on Artificial intelligence, as suggested and highlighted by CEN-CENELEC in their response to this consultation.**

Data processing and anonymization

Anonymisation of data must be effective and of non-temporary nature. The anonymisation mechanisms should not be "deconstructed" by AI.

Personal data should be strictly anonymised once they are merged into a large data set. This process should also apply to meta-data, since they are blended with traditional personal records. AI has the capability to de-anonymize the same information based on inferences from other devices. Therefore, voice recognition and facial recognition could potentially compromise anonymity in the public sphere. In this regard, the distinction between personal and non-personal data should be clearly define in the draft guideline and shall comply with the rules enacted in the regulation (EU) 2018/1807 on the free flow of non-personal data when it comes to anonymized and scrubbed data. **The draft AI guideline should provide at least some insights to better understand how to handle data processing with such a requirement level.**

The European Data Protection Board (EDPB) should also issue a concrete contribution through Guidelines on **AI compliance with the GDPR**. Moreover, as foreseen by GDPR, certification schemes for IA should be prepared. It is deemed necessary for producers and importers of AI solutions in the European Union.

Chapter III: Assessing Trustworthy AI

A Cybersecure approach is more than necessary

Assessing Trustworthy AI cannot dispense with the definition of security requirements. The guidelines mentioned mainly safety driven concepts and requirements, which is not enough to protect assets of AI solutions and devices. Cybersecurity is key to prevent from potential attacks and manage the protection of critical assets. AI cannot be assessed against safety concept whose targets of evaluation are static. Therefore, we strongly recommend **penetration tests** by Humans as a fundamental component for assessing AI, to verify and stabilize robustness of the most critical AI applications.

Moreover, **robustness** of IA implies resilience as well as reliability and reproducibility. Eurosmart supports the promotion of a cyber-resilient network in the Union to guarantee security by design and a functional assessment for edge-computing devices.

Third party certification

The international and European standards mentioned in the second chapter can be used to performed 3rd party certification. The European Cybersecurity Certification framework should be mentioned as the primary reference to assess trustworthy AI, the European Commission shall make it a priority in the upcoming Union rolling work programme for cybersecurity certification scheme.

General Comments

Eurosmart strongly supports AI-HLEG's big step forward to define a common understanding for trustworthy AI. This initiative paves the way to AI development in respect of the European values in terms of data protection, privacy and cybersecurity.

Eurosmart highlights the need to mention and to recognise the work on ESOs for a real EU added-value in terms of AI standardisation.

Based on these standards, a real effort shall be made to assess the upcoming AI solutions. The European Union is currently deploying trustworthy certification mechanism through the Cybersecurity Act and the GDPR and should rely on it.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Cabinet Louis Reynaud**, **Fingerprint Cards**, **Gemalto**, **G+S Mobile Security**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS, Bureau Veritas**), laboratories (**Brightsight, CEA-LETI**, **Keolabs**, **SERMA, Trust CB**), research organisations (**Fraunhofer AISEC, ISEN**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com