Global Forum 2022

Report on S3: Designing Ethics for Artificial Intelligence and an Efficient Regulatory, Policy & Governance Framework in a Complex World

by Geneviève Fieux-Castagnet

CONTEXT **1**
RATIONALE **1**
PRESENTATIONS **2**
PANEL 2
GENEVIÈVE FIEUX-CASTAGNET 3
AI Potential and Risks: The Case of SNCF *3*
UNESCO Recommendations *4*
EU Guidelines for Trustworthy AI *4*
US Blueprint for an AI Bill of Rights *5*
Hard Law for AI: The EU Case *5*
RASHA AL-ABDALI (CHAIR) 6
ALESSANDRO GUARINO 7
FAHD BATAYNEY 8
GILLES BABINET 9
SARAH ZHAO 11
DISCUSSION **12**

Context

The 29th edition of the Global Forum, whose main theme was "*Digital Dynamics & Global Societal Challenges: New Realities of Disruption and Resilience*", took place on Monday 17th & Tuesday 18th October 2022 in Muscat, Oman. It was organized by ITEMS International, an international consulting firm based in Paris, IKED, the International Organization For Knowledge Economy and Enterprise Development, based in Sweden, under the High Patronage of the Oman Society for Petroleum Services (OPAL).

On 2nd August 2022, I received an invitation by the Global Forum Organizers to participate as Moderator to the session 3 on "*Designing Ethics for Artificial Intelligence and Effective Governance in a Complex World*" After receiving the consent of my hierarchy, I confirmed my presence and started contacting the prospective speakers and Chair.

Rationale

In order to finetune the agenda of the Global Forum in a spirit of co-creation and collaboration, thematic discussions in form of live webinar sessions were organized between March 2021 and June 2022.

At the invitation of Ms. Sylviane Toporkoff, Founder & Partner ITEMS International, I attended the second webinar on 7th April 2021, where I took part in the conversation about "Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, Blockchain" by giving a PowerPoint presentation on "A European Perspective of Ethics for AI Systems". I also attended the third, fifth and seventh webinars to support the finalization of the draft agenda and continue enriching the rationale for AI Ethics.

It was the first time the Global Forum was addressing Ethics for AI Systems, so the discussions were instructive and enlightening, with various opinions shared by experts from all over the world.

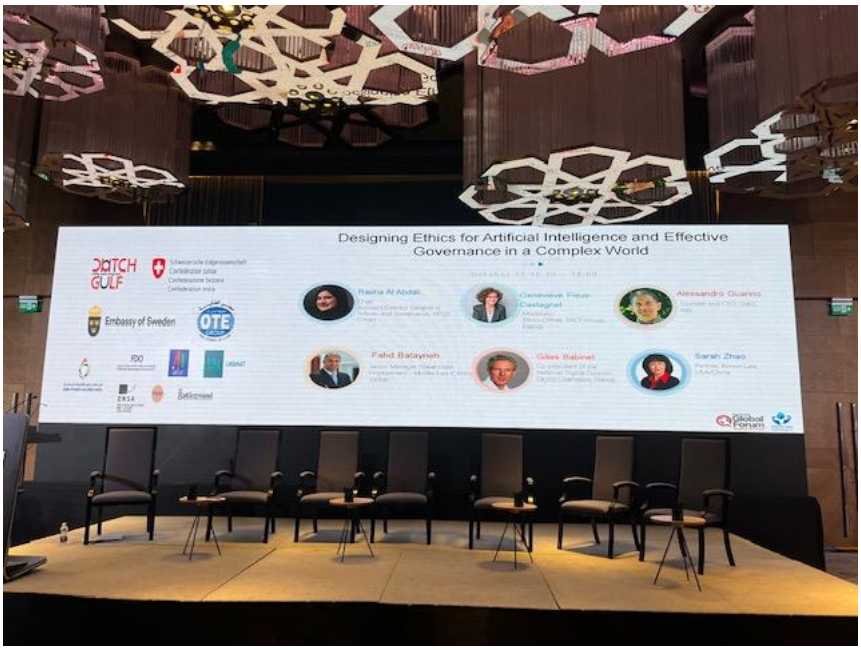
Eventually, it was decided to include "Ethics for AI Systems" within a more general theme concerning Ethics and Regulation, whence the final title of the third session (S3).

During the two weeks before the session, I had several contacts by e-mail with the Chairwoman and the 4 speakers in order to assess progress of the making of the PPTs, check with the experts if they needed more information or guidance, and have sufficient time to prepare questions and ensure a coherent and smooth process of the session.

Presentations

Panel

1. **Rasha Al-Abdali**, Assistant Director General of Policies and Governance, MTCIT, Oman (Chair)
2. **Geneviève Fieux-Castagnet**, Ethics Officer, SNCF Group, France (Moderator)
3. **Alessandro Guarino**, Founder & CEO, StAG, Italy
4. **Fahd Batayney**, Senior Manager Stakeholder Engagement, Middle East, ICANN, Jordan
5. **Gilles Babinet**, Co-President of the National Digital Council; Digital Champion, representing France at the European Commission for digital matters, France
6. **Sarah Zhao**, Partner, Rimôn Law, USA/China



This session, like the others, included the following parts:

- Introduction by the Chair and the Moderator
- Presentation by the panelists
- Discussion among the speakers and with the audience

Geneviève FIEUX-CASTAGNET

With the agreement of the Chair, I introduced the session by focusing the broad theme on Ethics and Regulation for Artificial Intelligence (AI).

AI Potential and Risks: The Case of SNCF

AI has great applications in health, environment, security, mobility, transport, and the identification of human needs and desires, but at the same time, it puts human rights and fundamental freedoms at stake. Facial recognition, for instance, or tracing applications used to fight the pandemic, may also lead to surveillance and a loss of privacy. Therefore, after reminding the paramount potential applications of AI, I sought to draw attention to the main challenges with regards to Human Rights and Fundamental Freedoms:

- Surveillance: Facial Recognition (which enables tracking)
- Discrimination: use of old or uncontrolled data (e.g., for automatic recruitment)
- Privacy, in particular in relation to data collection (e.g., chatbot, autonomous vehicles)
- Free consent and autonomy in an era where prevail merchant sites and social media (risks of profiling)

To raise acceptance of AI and make it a competitive asset, various initiatives for trustworthy AI have been launched – at international, national, and corporate levels (e.g., OECD, UNESCO, EU, CNIL/France, CIFAR/Canada, Beijing AI Principles, but also SNCF, Google AI, or Apple). Inspired by the European guidelines as well as its own code of conduct and values, SNCF follows the Ethics-by-Design approach for AI systems. From the very beginning of any AI project, a multidisciplinary governance team (project manager, developers, ethicists) maps the ethical risks of the project. Then, SNCF identifies remedies and risk mitigations. Monitoring the whole AI system during its entire lifetime is very important. The ideal would be to control the system throughout the whole supply chain. Another important aspect of SNCF's Ethics-by-Design approach for AI systems, is to really ask the right questions. A catalogue of more than 100 questions is used at SNCF to map risks, among those: Which human rights or fundamental freedoms may be concerned? Is the use of AI essential or useful? Can we use a less invasive

system? Can we use less data? Can we anonymize or pseudo-anonymize the personal data? Could we anticipate misuses or double uses? Can we explain the AI system? Is it safe, robust and resilient to attacks? The identification of potential ethical dilemmas is another crucial aspect: Being France's national railway company, SNCF has developed a system to recognize the owners of lost luggage. The most efficient solution would have been to use facial-recognition technology. However, SNCF balanced between efficiency, invasion of privacy and the risk of surveillance, and therefore made the choice of developing a system based on clothes recognition, which is quite efficient, though probably less efficient than facial recognition.

UNESCO Recommendations

UNESCO (193 Member States) is calling: on international and national policies and regulatory frameworks to ensure that AI benefits humanity as a whole; and on a human-centered AI (AI must be for the greater interest of the people, not the other way around.

UNESCO's recommendations on AI Ethics are hence the following:

- Provide a universal framework of values, principles and actions, consistent with international law;
- Guide the actions of individuals, groups, communities, institutions and private sector companies to ensure the embedding of ethics in all stages of the AI system life cycle;
- Protect, promote and respect human rights and fundamental freedoms, human dignity & equality, including gender equality;
- Safeguard the interests of present & future generations; preserve the environment, biodiversity & ecosystems; and respect cultural diversity across the AI system life cycle;
- Foster multi-stakeholder, multidisciplinary and pluralistic dialogue and consensus building about ethical issues relating to AI systems;
- Promote equitable access.

EU Guidelines for Trustworthy AI

Then, I described the EU Ethics Guidelines for Trustworthy AI (the so-called "7 key requirements"), which were published on 8th April 2019 by the High-Level Expert Group on Artificial Intelligence (AI HLEG) set up by the European Commission:

- Human intervention and human control
- Robustness and security
- Privacy and Data Governance
- Transparency
- Diversity, non-discrimination and equity
- Societal and environmental well-being
- Accountability

According to the Guidelines, trustworthy AI should be: lawful (respecting all applicable laws and regulations), ethical (respecting ethical principles and values), and robust (both from a technical perspective while considering its social environment).

The AI HLEG also released on 17th July 2020 an Assessment List for Trustworthy Artificial Intelligence to provide a basis evaluation process for Trustworthy AI self-evaluation. Organizations can therefore draw elements relevant to the particular AI system from ALTAI or add elements to it as they see fit, taking into consideration the sector they operate in.

US Blueprint for an AI Bill of Rights

Recently, the U.S. White House Office of Science and Technology Policy (OSTP) released a Blueprint for an AI Bill of Rights. The document provides an important framework for how government, technology companies, and citizens can work together to ensure more accountable AI.

The Blueprint contains five principles, each of which includes a technical companion that provides guidance for responsible implementation of the principles:

- Safe and Effective Systems: You should be protected from unsafe or ineffective system.
- Algorithmic Discrimination Protections: You should not face discrimination by algorithms and systems should be used and designed in an equitable way.
- Data Privacy: You should be protected from abusive data practices via built-in protections, and you should have agency over how data about you is used.
- Notice and Explanation: You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.
- Alternative Options: You should be able to 'opt out', where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

The Values heralded in the Blueprint are the following:

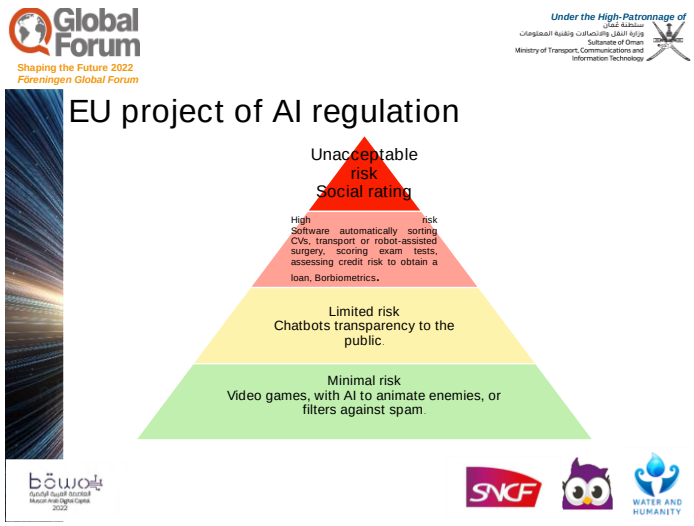
- Civil rights, civil liberties, and privacy, including freedom of speech, voting, and protections from discrimination, excessive punishment, unlawful surveillance, and violations of privacy and other freedoms in both public and private sector contexts.
- Equal opportunities, including equitable access to education, housing, credit, employment, and other programs.
- Access to critical resources or services, such as healthcare, financial services, safety, social services, non-deceptive information about goods and services, and government benefits.

The Blueprint aims to help protect the public from harm. The measures taken to realize the vision set forward in this framework should be proportionate with the extent and nature of the harm, or risk of harm, to people's rights, opportunities, and access.

Hard Law for AI: The EU Case

It is important to distinguish between Ethics and Law – the two concepts are not equivalent. Today there exist several legal texts and initiatives that may support ethics for AI, e.g., the General Data Protection Regulation (GDPR) in the European Union.

As we have seen from A. Guarino's presentation, the EU legal approach is risk-based: risks are qualified according to their degree of potential harm to individuals and groups in terms of the 7 key requirements set out by the European Commission.



Rasha AL-ABDALI (Chair)

The Chair's presentation addressed the issue of « Future Landscape for AI Governance". She reminded the significant anticipated economic effects of AI by 2030:

- $1507 trillion – AI Contribution to the World`s Economy
- $42,7 billion – AI Contribution to National GDP in Egypt
- $13502 – AI Contribution to the national GDP in Saudi Arabia
- ~14% - AI Contribution to the National GDP of UAE

The purpose of AI governance is to encourage using AI technologies in an ethical, fair, and safe manner through a set of rules and regulations designed to consider Human as a main aspect. This includes: societal context and privacy; governing data collection & algorithms development; and global collaboration and international standards.

The key principles of AI governance are the following:

- Inclusiveness
- Human-centered
- Accountability
- Fairness
- Transparency
- Safety

She provided information and data on the Oman context, where focus of work is put on Medicine (Breast Cancer Diagnosing), Power ("Nibras", i.e. the Digital Integrated Asset Management platform of iNNOVATEQ, a leading digital transformation solutions provider), Agriculture (Plant Pollination and Disease Discovery), and Utilities (Smart Water & Electricity Meters).

The foundational governance policies and regulations in Oman, most of them quite recent, are the following:

- Artificial Intelligence Systems Policies, 2021
- Personal Data Protection Law, 2022

- Cybercrime Law, 2011
- E-Transaction Law, 2008
- Government Open Data Policy, 2020
- ICT Services Continuity Policy, 2020
- Guidelines for Classification of Data and Information Security Systems, 2018
- E-Accessibility Policy, 2022

Alessandro GUARINO

The title of the speaker's presentation was: "The European approach to AI regulation and its impact on global cyberspace. Could doing good in fact hurt Europe?"

He claimed that the EU approach is actually a 'gas factory', as illustrated by the slide below:

The European Commission's proposed Artificial Intelligence (AI) Act attempts to regulate a wide range of AI applications, aligning them with EU values and fundamental rights through a risk-based, ethics-inspired and precautionary approach. The scope, instruments and governance framework introduced by the proposal are still being debated and refined by European co-legislators – both the Council of the European Union and the European Parliament have proposed possible amendments to the regulation, with potentially far-reaching impacts on its overall scope and content. An agreement seems possible by 2024, but this will depend on whether the co-legislators converge on key issues such as the definition of AI, the risk classification and associated regulatory remedies, governance arrangements and enforcement rules.

Under this approach, mandatory requirements are applicable to the design and development of AI systems before they are placed on the market.

The risks of such a risk-based approach are manifold:

- EU competitiveness: too high a burden is posed on the industry, especially innovative SMEs;
- EU Relevance in AI: Europe is already lagging behind the USA and China in AI, which is already and will be more in the future, a geopolitical enabler;
- Furthering fragmentation of "cyberspace" even more, when coupled with the emphasis on "digital sovereignty";

- "(Big) Data migration": reluctance of localizing data and information in the European Union;
- Diverging legislation, consequent standards and certification schemes could create a rift for European companies reaching out and also for non-EU companies entering the EU Single Market;
- (Some good news: global standards and mutual recognition of certifications, e.g. SG/FI Cybersecurity labels).

Fahd BATAYNEY

The speaker presented ICANN with one motto: One World, One Internet.

Created in 1988, the Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit, public benefit corporation that helps to keep the Internet secure, stable and interoperable. It serves as the authority on domain names and on a series of Internet-related tasks. The rationale behind the creation of this group was that it was important to establish a central figure which could not only determine but also enforce Internet and Internet domain rules, regulations, and policies. ICANN has played, and continues to play, an essential role in the creation and maintenance of the Internet.

The corporation is managed by a Board of Directors, which is composed of representatives of the Supporting Organizations (SOs), sub-groups that focus on specific sections of the policies under ICANN's realm, independent representatives of the general public interest that are selected through a nominating committee in which all of the constituencies of ICANN are represented; and finally the President and CEO, appointed by the rest of the Board.

There are three Supporting Organizations responsible for developing policy recommendations in the areas they represent:

- The Address Supporting Organization (ASO) that deals with policy on IP addresses.
- The Country Code Names Supporting Organization (ccNSO) that deals with policy regarding country code top-level domains (ccTLD), and
- The Generic Names Supporting Organization (GNSO) that focuses on policy making on generic top top-level domains (gTLDs),

ICANN also relies on 4 advisory committees to balance advice on the interest and needs of stakeholders that do not participate directly with the Supporting Organizations, including:

- The At-Large Advisory Committee (ALAC), comprised of representatives from organizations of individual Internet users from around the world;
- The Government Advisory Committee (GAC), comprised of representatives of a large number of national governments from across the globe;
- The Root Server System Advisory Committee (RSSAC) which provides advice on the operation of the DNS root server system;
- The Security and Stability Advisory Committee (SSAC), comprised of Internet experts who study security issues related to ICANN's mandate.

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to ensure the stable and secure operation of the Internet's unique identifier systems:

- It coordinates the allocation and assignment of names in the root zone of the Domain Name System;

- It coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains (gTLDs);
- It facilitates the coordination of the operation and evolution of the DNS root name server system;
- It coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers;
- It collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations.

ICANN has long regulated the use of top-level domains including .com, .net, and .org and played an integral role in determining the newer TLDs that have been created as of this date. This long and ever-growing list includes TLDs such as .gov (reserved for governmental offices), .info (intended to be used by informational websites), and .mil (reserved for use by military offices). ICANN also regulates country-specific TLDs such as .uk (for the United Kingdom), .us (the United States), .fr (France), and .br (Brazil).

Since 2009 there are Internationalized Domain Names (IDNs), i.e. domain names with non-Latin characters or Latin characters beyond letters (a to z) digits (0 to 9) and hyphens (-), as allowed by relevant protocols.

ICANN is involved in Legislation and Regulation, but not at all, as some people believe, to influence decision-makers. Since the Internet is a "borderless innovation" and the world is pushing hard for "digital transformation", ICANN sees its role as one of ensuring that the Internet doesn't break and remains functional. To achieve this, ICANN shares its technical expertise with legislators, regulators, and intergovernmental agencies in order to assess the potential impact of their initiatives on the functioning of the Internet, and to better understand and define the situations they seek to address.

ICANN calls on politicians "Don't Politicize the Core of the Internet!"

Gilles BABINET

The speaker demonstrated that in Information Technologies, the power of stories is defining the ethical standards. Over the last 60 years, it is interesting to see how much IT technologies went through quite different phases.

At first, there was a community phase, built around the military who invented the Arpanet and the mainframe. Then the hippies came and invented the microcomputer. The army had to deal with coordinating subsidiarity management systems and the hippies were caring for a way to straighten their decentralized communities. It was both an era of cold war and true hope for a better society. It was a true utopian phase and technologies were aiming for greater good.

From the 80's came the business phase of the Internet, it was eased by the Conservative narrative which was pushed by the mercantilism momentum, that was the oxymora of the "conservative revolution". Deregulation was an irresistible policy and most technological companies lobbied for not being regulated.

There was still a very strong sense of Utopia. There was this strong belief that the economy would be fast developing in an inclusive way.

In 2000', the cloud was invented and a new phase of data recentralization allowed it to take control of hundreds of millions of individuals' data.

Soon started some significant crisis: Snowden, Cambridge Analytica, the principle of *captology* (as his inventor JB Fogg defined it), were the most visible faces of that crisis. The digital revolution moved progressively from a utopian to a dystopian era.

In addition, the Platform economy that had created 'never seen before' large-size companies proved not to be inclusive.

- digital shift: with very few high paying jobs, and no social mobility or almost none;
- gig Economy: social rights denied;
- social dumping, due to globalization.

More recently, blockchains took over. It curiously resonates with the narrative of the transhumanism, the libertarian and the neo reactionary movements that were taking shape ever since the mid-nineties, mostly through the Internet and personified through people such as Peter Thiel. It is, forty years after the first phase of it, the new decentralization phase, the era that some call Web3.

One can object that there is at the same time a regulatory wave like never seen before with the Digital Services Act (DSA), Digital Market Act (DMA), Data Governance Act, all adopted in 2022. Not to mention the will of the Congress and the FDA to tighten the US regulation regarding big-tech.

If regulation is certainly important, one can question the importance of common imaginaries.

It is difficult to define the new narrative and the technology that could emerge from it though.

What strikes us is the kaleidoscope of imaginaries. One could call it a new epistemology in the way it desacralized the existing forms of knowledge (medias, intellectuals academies, governments…).

Quantum scientists can talk to their peers in the most efficient way and so will flat-earth believers.

On another aspect, cultural minorities and gender are now able to gather forces and redesign the dominant cultures. You probably heard about the "woke movement", whether we like it or not, it highlights structural inequalities that we must face.

Are we entering a new phase with multiple realities? That would resonate with the quantum computer that can be in several states at the same time.

But the question remains: can there be any common imaginary that would be of the size of the Internet, i.e. almost the entire humanity?

The late Bruno Latour thought that nature could be the narrative that can gather us all. When we look at the monumental challenges we are facing we cannot ignore that it is up to our generation and all generations to collectively find solutions.

Digital has proven to be the only way to catalyze global consciousness to deal with interdependent crisis: environmental, economic, political, societal. But we cannot deal with it

as fragmented and an individualized humanity. We need some technologies that can both deal with our fragmented communities and our Gaia communities. The one that sticks us together.

Victor Hugo once said, “no force is stronger than an idea which time has come”. What is the narrative that will create the technologies that sticks us together to deal with the environmental challenges? Given how contextuality has proven to be a critical driver of new innovations, my true guess is that it is probably here, dormant, just because we need it.

Sarah ZHAO

The speaker presented the new developments of China’s Cybersecurity rules – a very important issue in any discussion on AI ethics from a global perspective.

China has today a comprehensive framework governing cybersecurity, data protection and privacy:

- China Cybersecurity Law (June 2017)
- China Data Security Law (Sept. 2021)
- China Privacy Law, (or Personal Information Protection Law, Nov. 2021)
- Measures for Security Assessment of Cross-Borders Data Transfer (Sept.1, 2022)
- Draft of Amendment to China Cybersecurity Law (Sept. 2022)
- Sectorial implementation regulations, as an example measures for the Administration of Consumer Rights Protection of Banking and Insurance Institutions (Draft issued in May 2022; formal rule is expected to be issued by end of 2022)
- Other related implementation rules and regulations.

China has also implemented measures for Security Assessment of Cross-Borders Data Transfer:

- Based on the Cybersecurity Law and Privacy Law, data collected in China shall be stored in China, unless exceptions apply. For the purpose of being qualified to conduct cross-border data transfers, certain security assessments may be conducted.
- In the past, such security assessments were difficult to be enforced because the security assessments standard did not exist. This confusing situation has been clarified by the new rule, Measures for Security Assessment of Cross-Borders Data Transfer, which became effective last month on September 1, 2022. This new rule has set forth a road map for conducting a security assessment if it is necessary.

Who shall apply the new rule?

- Based on Article 4 of the new rule, a company that handles cross-borders data transfer shall conduct security assessments if they meet any of the following four situations: (i) data handler transfer of critical information out of the country; (ii) Critical Information Infrastructure operators that handle the information of more than one million people; (iii) Since January 1 of the previous year, the data handler has transferred overseas more than 100,000 pieces of personal information, or 10,000 pieces of sensitive personal information; and (vi) Any other required data security assessments by the government.
- The following circumstances are defined as cross-border data transfers: (i) The data handler transfers and stores the data collected and generated in the domestic operation to overseas destinations; (ii) The data is collected and generated within China, and overseas institutions, organizations or individuals may inquire, retrieve, download, or

transfer; (iii) Other data transfers that may be required by the CAC (Cyberspace Administration of China).

How to apply the new rule?

- Data handlers shall apply for security assessments via their local provincial CAC. The submitted materials shall be in both written and electronic versions. After the provincial CAC receives the application materials, it shall complete the review within 5 working days. When the local CAC completes the approval process, it shall forward its report and the application materials to the Central CAC.
- Within 7 working days from the date of receipt of the local approval, the central CAC shall determine whether to accept and notify the data handler in writing.
- If approvals are rejected, the data handlers may require the CAC for re-evaluation within 15 working days of receiving the notification of the assessment result, and the re-evaluation result shall be the final conclusion.

With regard to cross-border transfers about judicial procedures, the requirements are the following:

- The Ministry of Justice issued a notice to clarify the requirements for cross-border data transfer involved in litigations in September, 2022.
- "Hague Service Convention", "Hague Convention on Evidence Collection," and the 38 Sino-foreign bilateral judicial assistance treaties, as well as diplomatic channels.
- Relevant foreign entities shall submit requests for evidence collections to the Ministry of Justice through the channels specified in the treaty, or to the Ministry of Foreign Affairs through diplomatic channels, and the requests shall be executed by the People's Courts after the approvals.
- Based on the Civil Procedure Law of China, evidence collection shall be carried out by the People's Court or by a lawyer with the approval of the People's Court.
- It may be feasible if a party in China voluntarily submits evidence materials located in China directly to a foreign judicial authority.

Discussion

Ethics has a double nature: Etymologically, *ethos* means the place of life, the habits and manners of people trying to live together in a city, a company etc. This very much depends on where you live, what you want to do and what your values are. But, according to Aristotle, ethics also allows to recognize us as members of humanity and of mankind as such. This dialectic seems very appropriate to the ethics for AI systems, too, as AI has no borders and is universally applicable.

AI systems being universal, the panelists agree we should work on a system of international core values that the different stakeholders agree on. The Global Forum might be an opportunity to define a set of core values that could then be shared with the world. I pleaded for consensus building rather than full force hard regulation, except for high-risk AI systems, as advocated by the European Commission in its draft EU AI Act.

Nevertheless, it cannot be ignored that EU's risk-based approach, which involves determining the scale or scope of risks related to a concrete situation and a recognized threat, is challenged by certain groups of stakeholders. They claim a risk-based approach may be useful in technical environments where companies have to evaluate their own operational risks, but it has

companies evaluate their operational risks vs. people's fundamental rights. This is perceived by them a fundamental misconception of what human rights are: They cannot be put in a balance with companies' interests. Companies would also have an interest in downplaying the risks in order to develop products. If human rights are non-negotiable, then they must be respected regardless of a risk level associated with external factors. Therefore, these stakeholders still prefer a rights-based regulation, like the GDPR, as this is the only way to ensure the protection of fundamental rights, instead of a risk-based regulation.

On the other hand, the majority of experts from the public sector, the private sector and international organizations believe that regulation should be seen as a matter of degree. What is required is an approach to AI regulation that takes the middle ground by identifying how much regulation is required, what type of regulation is required, and what coverage domain the regulation addresses. Taking this flexible, pragmatic approach to AI regulation helps society safeguard the common good in cases where the risk is greatest while continuing to support innovation in AI by avoiding extensive regulatory efforts.

It is significant that over the past few years about 30 per cent of the countries in the world have advanced regulations or similar initiatives to keep AI accountable. This is good news, but at the same time the question arises whether, and to what extent, such proliferation of regulations, guidelines etc. could lead to an exacerbation of the fragmentation of technological regimes and governance mechanisms internationally. Efforts should be conducted to ensure greater alignment across countries. International initiatives may be helpful in this respect, in particular UNESCO (November 2021), the World Economic Forum (February & August 2021), the Global partnership on AI (June 2020, and OECD (May 2019). Worth mentioning is also the opening of negotiations for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law (Convention). The Convention may prove to be an important opportunity to complement the European Commission's proposed EU AI Act by strengthening the protection of individuals' fundamental rights, such as the rights to privacy and to the protection of personal data.