G2O BRASIL 2024
BUILDING A JUST WORLD
AND A SUSTAINABLE PLANET

Possible Approaches to Promoting Information Integrity and Trust in the Digital Environment

Integrity of Information and Trust in the Digital Economy

Digital Economy Working Group

Report prepared under the Brazilian Presidency of the G20

Knowledge partner

unesco

Possible Approaches to Promoting Information Integrity and Trust in the Digital Environment

Integrity of Information and Trust in the Digital Economy

Digital Economy Working Group

Report prepared under the Brazilian Presidency of the G20

September 2024

UNESCO is a Knowledge Partner to the Brazilian G20 Presidency to the Digital Economy Working Group, including on artificial intelligence and the integrity of information. This paper focuses on mapping the debate on information integrity and informing the agenda of the G20.

UNESCO is a leader in promoting the safeguarding of information as a public good, as recognized in the Windhoek +30 Declaration. The Government of Brazil has recognized UNESCO's added value in responding to misinformation and disinformation, as well as the relevance of UNESCO's Internet for Trust Initiative.

Acknowledgments

Driving the digital economy: Key points for the G20 to consider

▶ As the COVID-19 pandemic highlighted, **information integrity is essential** for the progress of economies, public health management, and effective governance in the digital era, particularly in times of crisis or disaster. It is also essential if we are to make greater progress towards the Sustainable Development Goals (SDGs).

▶ **Shortfalls in human-rights based governance or self-governance** of digital communication services have contributed to an erosion of human rights and social trust that are essential for a functional modern economy.

▶ The **scale and scope** at which digital services generate and distribute information are raising new concerns about information integrity. Fast-paced innovations have driven down the cost of producing inauthentic information such as with synthetic media and Artificial Intelligence (AI) deep fakes, and this content is then amplified and consumed at scale via social media and search services.

▶ Understanding the **interplay between offline and online information sources**, and the potential of deep fakes to mobilise and create disorder, is particularly important in contexts such as elections and e-commerce.

▶ Among the **governance and self-governance steps** that can be taken in line with international human rights law are: promoting **corporate transparency** and **accountability**; ensuring **access to information and data**; protecting **vulnerable people especially children online**; strengthening **privacy, freedom of expression and access to information**; and advancing **consumer rights** and effective **data governance**.

▶ Other possible measures include: Using **public procurement** as a lever to incentivise changes; **supporting the scientific, cultural and media sectors**; defending **election integrity**; advancing **media and information literacy** and improving **regulatory and policy coordination** and **multistakeholder participation** in information governance.

- Governance interventions for information integrity need to align with **the duty of states to protect freedom of expression** in terms of the International Covenant on Civil and Political Rights. This means that interventions must have a legal basis, be necessary and proportionate, and follow a legitimate purpose. To meet the criterion of predictability, terms such as "disinformation" and "safety" **merit narrow definitions**. Standards call for regulatory interventions to be **independent** of vested interests.

- Information integrity in the digital era hinges on **universal, safe and meaningful Internet access for all**. If digital inequality is not addressed at the same time, actions to counter threats to the integrity of information will have limited social and economic impact.

- Defending information integrity covers more than promoting appropriate content moderation on social media. It needs to be complemented by actions to advance freedom of expression and the provision of **information as a public good** as critical inputs for successful digital economies. This in turn necessitates innovative development and support for a plurality of public interest media and digital infrastructures.

Table of contents

Introduction

Evidence shows that when information integrity is protected, there are concrete benefits for trust, political accountability and sustainable development.[1] By contrast, an information ecosystem that lacks accuracy and reliability, and which is contaminated by hate speech and incitement to violence, works against trust, innovation, digital transformation and sustainable development.

At the same time as addressing the problem of false and potentially dangerous content, attention is also merited for the other side of the coin, namely the need for policies to promote and protect that kind of content which counts as "information as a public good"[2]. Success on both fronts – decreasing potentially harmful content *and* elevating accurate and reliable information for universal access – is a precondition for information integrity. Taking cognisance of common parameters within several existing definitions of "information integrity, the G20 is invited to consider the points below.

---

1. For example, accurate and ubiquitous information is the currency of competitive markets, economic investments and consumer choice. Within this, independent journalism adds special value by bringing transparency to public processes and reducing corruption. Open government and effective access to information regimes are also key components for information to play a positive role in the digital economy.

2. An elaboration of "information as a public good" appears in the companion report to this document. The criteria of pure "public goods" are that they are non-rivalrous and non-excludable. Free-to-air public broadcasting is an example of a pure public good. A person listening to the radio does not diminish the use of it by others, and it is non-excludable in the sense that in principle no-one can be excluded from listening. There are also public goods characteristics of media that are available only to paid subscribers, which are known as "merit goods" in that these are non-rivalrous but excludable. Most governmental information is availed as a public good. A balance of public and merit goods in relation to other content helps ensure information integrity within the wider information ecosystem. This why media and public information have historically been governed for public interest objectives of universality, plurality, equity and quality – principles key for information integrity.

Revisiting regulatory, co-regulatory and self-regulatory configurations (a call for a new governance system): Ensuring policy dynamism, coherence with international law and co-ordination for information integrity

Governance that concerns information integrity needs to be cognisant of risks and opportunities for human rights and fundamental freedoms – which are both overarching and underlying as regards digital economies. In this context, the evolving intersections between regulation systems for media, digital platforms and new AI systems have profound implications for each G20 country's information governance landscape.

These changes make it appropriate to revisit the policy and institutional settings of current governance and self-governance frameworks. For example, the Global AI law and policy tracker covering 24 jurisdictions notes numerous authorities of relevance to digital developments. These include ministries, planning departments, national securities commissions, access to Information agencies, e-safety commissions, competition and consumer commissions, data protection agencies, national science and technology councils, research institutes, specialised AI advisory councils and task forces, and statistics bodies. Copyright offices, election management bodies, advertising standards regulators, and a range of other institutions can be added to this landscape, depending on the digital service and/or informational issue at stake. Existing

regulators dealing with issues that are germane to information integrity (from audiovisual to electoral regulators, from consumer protection to privacy or telecom regulators) are being complemented by new ones, particularly in regard to AI.

Co-ordination of a distributed governance scenario can help tackle the protection and promotion of information integrity that aligns with international human rights law. This calls for regulatory linkups and structured multistakeholder involvement in rule-making, oversight, monitoring and redress. Co-ordination amongst regulatory, co-regulatory and self-regulatory systems depends on the existence of coherent umbrella policies which draw on the full range of relevant interests and expertise. This should precede any laws and regulations, as well as enforcement thereof. Good practice involves a systematic monitoring and evaluation feedback loop, especially given rapid changes in digital services. Nuance is called for throughout so that regulations do not reinforce the most powerful digital services who can afford to meet defined standards, while disadvantaging start-ups and SMEs seeking to compete.

As advocated in UNESCO's Guidelines for the Governance of Digital Platforms, international principles on freedom of expression call for independence in regulation insofar as content is concerned. This is to prevent capture by commercial, political or other forces. In addition, the different layers of the "tech stack" as regards information should be respected, to avoid regulatory overreach that, for example, might hold connectivity providers liable for content conveyed via their services. However, attention is merited in regard to governance of the data layer, in order to address bias and exclusions which flow "downstream" into applications and information use cases.

In the interests of information integrity, digital standards can be promoted for independent stress-testing and "red-teaming", thereby contributing to "safety-by-design". To avoid falling into catch-up mode, some jurisdictions like Singapore create or authorise "regulatory sandboxes" for controlled testing of AI, for example. Others such as the US and UK have created AI safety institutes and consortia for research and testing of safeguards.

Promoting digital inclusion:
Policies to ensure meaningful and safe connectivity

An enabling policy environment is fundamental to addressing inequalities. There are continued inequalities in accessing affordable, quality connectivity, and arguably even greater challenges in addressing skills and resource deficits that have major bearing on information's role in the digital economy. Attempts to address these inequalities include steps to foster competition in order to benefit underserved people, and also to make markets more open to new informational players, including micro- and community actors with business models that could support the expansion of digital public infrastructures including in local languages. Even for users who are connected, problems like technology-facilitated gender-based violence, including gendered disinformation, contribute to increasing the gender digital divide and create unsafe digital spaces for women and girls.

Protection of human rights and fundamental freedoms:
Policies to secure protection of groups in situations of vulnerability

There is universal consensus that children in particular merit additional protection online, with an elaboration in the General Comment by the UN Human Rights Committee on the Convention of the Rights of the Child. The G20 has produced a Toolkit on Cyber Education and Cyber Awareness of Children and Youth. Several G20 members are considering requirements for age-appropriate design of services and better implementation of company policies in this area. Numerous UN and other international resolutions also call for the protection of women online[3], as well as for journalists[4] and human rights defenders. These people collectively and individually face online harm that may also feed offline violations. Dealing with discrimination and intimidation in the digital environment, particularly for women in the information space, requires rigorous application online of laws developed for offline cases, with possible updates such as to account for cases like non-consensual sexual imagery. Digital platforms and providers can be guided to do more to protect users and ensure that those abusing the rights of others cannot do so with impunity. Digital inclusion depends on metrics for assuring safety, including safety from e-commerce and online scams, as key for an effective digital economy.

G20 members may consider advocating for greater application of the UN Guiding Principles for Business and Human Rights by digital platform owners. Undertaking impact studies (see for example, UNESCO's tool for AI ethical risk assessments) can enable stakeholders to address potential content harms before these reach scale.

---

3. See for example: https://www.unwomen.org/sites/default/files/2022-10/A-77-302-SG-report-EVAWG-en.pdf

4. See relevant international commitments here: https://www.unesco.org/en/safety-journalists/basic-texts?hub=687

Information integrity and the Sustainable Development Goals:
Policies to support the 2030 agenda

Dangers resulting from the integrity of information being compromised have been rated as top global risks. The importance of access to accurate and reliable information so evident in the COVID-19 pandemic, is further relevant to the wider Sustainable Development Goals. To take just one example, this can be seen with the challenge of combating climate change in the face of disinformation aimed at denial and delay and high risks to truth-tellers. The informational problem has been recognised by the Intergovernmental Panel on Climate Change, which is concerned that the urgency of action is being questioned and the scientific consensus being discredited. The Climate Action Against Disinformation Coalition (CAAD) has been working to stop adverts and monetisation where content contradicts climate science. This provides a practical example of a mechanism to mitigate risks resulting from platform advertising models. States can also positively contribute to promoting the hard-won consensus on climate change by communicating on the basis of expert advice. They can protect journalists and scientists under attack, and support awards for high-quality information on climate communication. Leaders can further consider the example of the UN joint statement about the intersection of freedom of expression, countering disinformation and the right to a clean, healthy and sustainable environment.

Advancing transparency and research access:
Policies to enable informed interventions

A major challenge for authorities is to avoid taking steps on information integrity that may be arbitrary, fragmented, unilateral, unrealistic and even counterproductive. To this end, evidence is essential for informed and effective governance. To secure this evidence, steps can be taken to increase the transparency of digital service providers, particularly in relation to AI systems that are used in informational content generation, recommender systems and content moderation (with regard to automated identification and actioning).[5] A primary intervention is to require systematic (and graduated) disclosures by digital service providers as pertains to information.[6] On the radar of the G20 could be interventions such as Algorithmic Impact Assessments and advocacy for disclosure about the data sets used to train AI systems. States also have a key role to play in transparency, open government and making information and data available, not least about their own use of digital services that impact on information integrity.

As is also happening in some places, governance aiming at accountability within a given jurisdiction may include requiring digital companies to conduct human rights due diligence, and to make this exercise open in various degrees as well as subject to independent auditing. The introduction of requirements for transparency reporting as well as for authorised regulatory agencies to have data access (with due respect to the anonymity of personal information and data) can also enhance information integrity. There is value in independent researchers, fact checkers and journalists having access to categories of data held by digital service providers, thereby widening the evidence pool needed for effective governance. Criteria and systems for vetting those who may receive different

---

5. Examples of the challenges are low levels of transparency in the foundation models of the major AI companies, (although improvements are noted between October 2023 and May 2024), and the transparency of 14 digital companies being assessed as below a pass-mark.

6. As regards digital advertising, there is the issue of access to data on ad targeting, where ads appear ("brand safety"), who purchases them, and how prices are set. Ranking Digital Rights further urges reporting on ad policy enforcement data and compliance with various legal requirements related to advertising (including political advertising). The EU's Media Freedom Act calls for transparent and harmonised metrics for competition in digital advertising markets.

degrees of access (for defined public interest purposes) would need to be independent and non-discriminatory. Principles and guidelines for transparency regulation and proposals for data access have been elaborated by UNESCO and by the European Union (EU). Any measures should recognise cost burdens and legitimate commercial confidentiality amongst different tiers of service providers, and avoid stifling innovation in emerging technology sectors.

G20 members can also promote knowledge networks inclusive of G20 and non-G20 countries by creating multi-stakeholder advisory groups and task teams to engage with counterparts across jurisdictions. In addition, the G20 can consider institutionalising roles in digital governance for academics and civil society, and further supporting research capacities, access to data, "compute," and the development of high-level skills through joint research initiatives. Transparently-provided support for civil society fact-checking, and media verification and monitoring of the effects of information integrity measures, could also be considered.

Privacy and consumer protection, data governance and procurement possibilities:
Policies to incentivise support for information integrity

Applying existing informational rules to the online realm can address phenomena such as online racism, gender-based violence, and threats to people's safety. However, in some cases, current legal provisions merit revision in order to ensure these are applicable, predictable, enforceable and aligned to standards of legality, proportionality, and legitimate purpose as per international human rights law. Adherence by states to the rule of law means that digital services should not be required to restrict lawful content.

Within the bigger picture of information integrity, content-specific approaches that are aligned to international human rights law can be complemented by measures in other areas that can have a significant bearing on the diversity, viability and accuracy of information sources while not intruding on freedom of expression. These are areas that intersect directly with information integrity and have substantive relevance to the subject.

Using existing regulation to deal with anti-competitive practices in information markets is one such area where action can help to increase information pluralism and diversity. At the same time, this area may not be practical where smaller states lack jurisdiction over global players that are not domiciled within their countries. However, there are further areas for consideration that can help advance information integrity. These may include material support for local content developers and digital startups to provide alternative infrastructures and content in local languages. Likewise, there can be steps to strengthen media enterprises, public service broadcasting and non-profit digital platforms.

Promoting national and regional integration of data and digital markets could further contribute to the development and maintenance of viable information economies. Fostering data portability amongst digital services enhances user choice, while regional level co-operation can help create the economies of scale and scope needed for competitive integration into the global market [7]. By expanding the breadth of the information ecosystem, such measures reduce the opportunity for disinformation actors (whether state or non-state actors[8]) to reach mass audiences by exploiting a handful of dominant channels.

Rights to privacy, freedom of expression, and access to information are implicated in the business models using advanced data-driven technologies such as machine-learning and AI. Governance to protect of these rights can also have the benefit of helping to safeguard information integrity within economic and technical configurations. For example, data protection laws have been passed and, in some cases, authorities have been established, especially in the wake of the EU's General Data Protection Regulation (GDPR). Yet in many parts of the world the necessary enabling frameworks and human and financial resources required for effective implementation are insufficient. Addressing these gaps can help incentivise services to favour information integrity by reducing how disinformation and misinformation can benefit from data-driven targeting of content and advertising. Strengthening individual online privacy choices to be freer and more informed can nourish resilience against potentially harmful digital content.

Further, instituting transparency for data markets, including of data-brokers and data flows, can help guide policy decisions on possible guardrails relevant to information integrity. Another area of potential action within the informational scope is enforcing consumer protection law in the digital communications space, drawing possible lessons from G20/OECD work on financial consumer protection. This realm of work can support the right to redress, especially when digital services fall short of honouring their terms of service concerning users' rights and their safety. Such steps can lead to improved customer services in local languages and to the hiring of software engineers and content moderators who have the necessary linguistic and national knowledge to guide their operations and strengthen information integrity.

---

7. See European Union Data Act, Digital Services Act and AI Act and the African Union Digital Transformation Strategy for the development of a single digital market in Africa.

8. As noted in the UN General Assembly resolution 76/227 "Countering disinformation for the promotion and protection of human rights and fundamental freedoms".

A further area where states can act beyond, or instead of, a content-specific focus, is in the public procurement of digital services, including data services. Here, authorities can require suppliers to meet transparency, consumer and data safety standards which directly contribute to information integrity. While procurement policy, like copyright, is a matter in its own right, these two areas can be profitably conceptualised and elaborated in terms of a scope that recognises how they can have meaningful significance for information integrity in the digital economy.

Support for accurate and reliable content:
Policies that promote news, science, culture and open government information

Journalists, scientists, artists and culture professionals have major roles in contributing to information integrity. News media that operate – online and offline – with journalistic standards, clear provenance of content and legal liability for quality control are especially key contributors. Independent self-regulatory mechanisms for accountability in the media can serve as an objective and transparent basis for awarding financial support and deciding on tax exemptions. Digital services could be encouraged to contract media councils to provide comprehensive appeal systems for the high volume of complaints against moderation decisions that are currently not considered.

Policy can encourage scientific communication that follows principles of transparency, inclusivity, integrity, accountability, freedom and autonomy, and timeliness. Journalists and cultural professionals contribute to information integrity by often "speaking truth to power", debunking falsehoods and enhancing human awareness and agency to protect and promote human rights.

Supporting all these groups is governance that enables free expression, media freedom, academic freedom and artistic freedom. Also important are policy measures to support scientific endeavour, cultural output, digital transformation and the economic viability of media businesses. Related measures may include special attention to public service and community media, as well as to the protection of journalists, scientists, artists and cultural professionals through timely actions against criminal attacks on these persons. Support can be extended to media development as per the OECD's Development Cooperation Principles on Relevant and Effective Support to Media and the Information Environment, as well as initiatives such as the International Fund for Public Interest Media and local counterparts. UNESCO's Convention on the Protection

and Promotion of the Diversity of Cultural Expressions, which observes that cultural diversity depends on freedom of expression, sets out a frame for governmental measures to promote and protect this social and economic asset.

In addition to all this, in order to help build societal trust, states themselves can give attention to UNESCO's 2023 policy guidelines on the right to information and make authoritative information and data available to citizens. As per UN positions, governments should avoid communicating disinformation. Public communications should pre-empt information gaps and consider open government practises as well as the Good Practice Principles for Public Communication Responses to Mis- and Disinformation proposed by OECD. Government funding of information integrity efforts that are transparent in principle can avoid "boomerang" effects on credibility if covert subsidies come to light.

Cultural and copyright protections: Policies that preserve pluralism and diversity as a condition of information integrity

Growing numbers of countries are seeking to address digital services' economic impact on the domestic media and cultural industries which are significant factors in regard to information production, circulation and consumption. This covers issues around data-scraping, revenues for content creators, and the impact of AI-generated content. To address these, content producers advocate the principles of consent, credit and compensation. Regulatory arrangements (such as by competition authorities) might be more coordinated internationally so that accords reached with digital services in one country might extend more easily to other jurisdictions. In order to maintain cultural and media diversity, smaller entities in content production should not be left off the radar in any such arrangements. It is the case that some digital companies may push back against bargaining codes, copyright fees or levies on digital advertising by excluding news content from their services. Here, consideration can be given to private-sector providers (of a certain size and which play a public role) to disclose relevant data as well as apply labels (eg. to signal AI-generated content) or follow "must carry" provisions (akin to broadcast, cable[9] and internet regulation in many jurisdictions). Ensuring data access can help resolve debates around revenue sharing between digital and other economic sectors, such as through objectively assessing contributions to, and detractions from, information integrity, and helping to achieve a better balance across the ecosystem.

---

9. See for example the US's Cable Carriage of Broadcast Stations.

G20 – Possible Approaches to Promoting Information Integrity and Trust in the Digital Environment

Building competencies:
Policies to empower the public to value information integrity

Digital, media and information literacies, covering and intersecting with a wide set of competencies and skills, are essential if there is to be meaningful digital inclusion and societal resilience to disinformation and misinformation. Policies can especially ensure such competencies are furnished within programmes of formal and informal education and lifelong learning. Developing the societal capacity to devise, roll out, and monitor appropriate programmes requires dedicated interventions, including dynamic curriculum development and the training of trainers.

Comprehensive competencies to deal with information integrity are more effective than piecemeal skills. This means initiatives that include, but also go beyond technical skills and digital security practices, for example by extending into critical thinking, research and evaluation, and into the skills for recognising content credibility signals. Learning about ethics and human rights is a vital component, not least for innovators, software designers and data developers. Capacities to be strengthened in the interests of information integrity can therefore profitably encompass rights such as privacy and freedom of expression, as well as consumer rights. Understanding of the political economy of digital services and the human rights obligations of the private sector is important. Further key ingredients of the package are understanding of: digital inequalities; data biases; epistemological limits of large language models; and how data and algorithms can be used to nudge people's behaviours. Knowledge about intellectual property (and environmental dimensions of digital technologies) is equally significant.

Special attention is merited for building the knowledge base of parliamentarians, policymakers, and regulators about digital services and changing governance issues. This is particularly significant for global cooperation and governance to be able realise national public interest objectives in information integrity.

Platforms often already provide briefings to leading decision-makers, and these can be structured to include debate and multistakeholder engagements so that they are kept distinct from lobbying actions.

Complementing the building of literacies on the consumer side, are actions on the provider side by digital companies. The services of these businesses can be encouraged to provide user empowerment tools such as flags and labels (such as for AI-generated content). Countries can further join UNESCO efforts to foster national and international networks around media and information literacy and engage with related work to develop international standards for measuring digital competencies and assessing the impact of related interventions.

Elections: Policies to update and build capacity to protect information integrity for democratic processes

Information integrity during elections is of particular importance, given how polls are determinative moments in the life of a nation and have significant influence on economies, peace and security. Important in electoral contexts is attention to the interplay between increasingly popular online information sources such as messaging services and the use of digital fakes. This applies particularly audio and visual fakes which are difficult to detect even to those aware of their use to mobilise and create electoral disorder. Independent monitoring of online disinformation patterns is a key part of addressing this issue. In addition, Election Management Bodies (EMBs) can benefit from having contemporary principles and guidelines, such as those adopted by the African Association of Electoral Authorities. Experiences of partnerships with civil society and tech companies can be adapted as complementary initiatives to an EMB's own rules and activities. Tracking trends in online content during election periods can be supported by EMBs engaging neutral researchers and participating in multistakeholder mechanisms.

International cooperation:
Sharing practices to leverage information integrity experiences worldwide

Jurisdictional differences and authority over multinational actors vary greatly in the G20, compounding efforts to achieve more aligned international approaches. However, progress is possible at the level of norms and sharing of knowledge as seen in the most universal institutions addressing digital governance, namely the UN system. While much diversity can be expected to persist, reflecting different national contexts, bridges can be built for a greater understanding of the challenges and the range of responses to them. The basic agreed layer of international human rights and commitment to the Sustainable Development Goals can be reinforced as common ground. In this context, UNESCO's Internet for Trust process, along with its Recommendation on the ethics of AI, provides more specific guidance for G20 actors, as does the OECD's Hub on Information Integrity which builds on the report Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity.

Conclusion and recommendations

Information integrity is a sought-after outcome of an information ecosystem that is increasingly globalised, digitalised and platformised – although also articulated to significant analogue communications channels. This ecosystem is highly uneven not only in terms of the impact of harms but also economic opportunities. G20 members could commit to cooperation in the common interest where this advances the general conditions conducive to comprehensive information integrity.

To deepen evidence-based governance and collaboration to promote information integrity, the G20 can provide leadership and principled commitments. This would entail active measures to support inclusive, viable, sustainable and diverse local and regional information systems that align with international human rights law, as well as refraining from steps that jeopardise human rights and fundamental freedoms. This positive perspective can help inform ongoing national, regional and multilateral discussions and multistakeholder consultations about aspects of digital governance that impact the information environment. On the basis of such commitments, G20 members can:

▶ Comprehensively act on digital inequality which excludes half of the world's population from the digital economy and society and undermines the foundations of information integrity.

▶ Build all-of-society and all-of-government approaches, focusing on regulatory and self-regulation coordination, multistakeholder processes and independence of regulatory mechanisms.

▶ Refrain from disinformation while also, as per open government and freedom of information standards, providing optimum information and data.

▶ Foster transparency and data access frameworks within digital platform and AI service providers, as well as fair terms of access by these entities as regards content produced by the media, science and cultural sectors.

▶ As a critical input for the digital economy, especially support provision for that category of information and infrastructures that count as public goods.

▶ Intensify strategies and implementation for digital, media and information literacies.

▶ Engage with the UN and other international and regional opportunities in this area, building on existing global agreements and current initiatives.

For more information on UNESCO's work:

Guilherme Canela

Chief, Freedom of Expression and Safety of Journalists Section

Communication and Information Sector

g.godoi@unesco.org